Universiteit
Leiden
The Netherlands

Privacy en politiegegevens. Over geautomatiseerde normatieve informatie-uitwisseling

Koelewijn, Wouter Immánuël

Citation
Koelewijn, W. I. (2009). Privacy en politiegegevens. Over geautomatiseerde normatieve informatie-uitwisseling. Retrieved from https://hdl.handle.net/1887/21364

Version: Not Applicable (or Unknown)
License:
Downloaded from: https://hdl.handle.net/1887/21364

Note: To cite this publication please use the final published version (if applicable).

E.M. MEIJERS INSTITUUT
INSTITUUT VOOR RECHTSWETENSCHAPPELIJK ONDERZOEK

Privacy en politiegegevens

Over geautomatiseerde normatieve informatie-uitwisseling

W.I. Koelewijn

LEIDEN UNIVERSITY PRESS

Privacy en politiegegevens

Over geautomatiseerde normatieve informatie-uitwisseling

Leiden University Press

Voor Marloes, Nine en Lotte

Privacy en politiegegevens

Over geautomatiseerde normatieve informatie-uitwisseling

PROEFSCHRIFT

ter verkrijging van de graad van Doctor
aan de Universiteit Leiden, op gezag van
de Rector Magnificus prof. mr. P.F. van der Heijden,
volgens besluit van het College voor Promoties
te verdedigen op woensdag 4 november 2009
klokke 16.15 uur

door

Wouter Immánuël Koelewijn

Geboren te Baarn in 1979

Promotiecommissie

Promotoren:	prof. dr. H.J. van den Herik prof. mr. A.H.J. Schmidt
Co-promotor:	dr. L. Mommers
Overige leden:	prof. mr. Y. Buruma (Radboud Universiteit Nijmegen) prof. mr. H. Franken prof. dr. J-J. Meyer (Universiteit Utrecht) prof. dr. mr. E.R. Muller prof. dr. W. Voermans

Nederlandse Organisatie voor Wetenschappelijk Onderzoek.
Dit onderzoek is onderdeel van het ANITA-project dat is mogelijk gemaakt door NWO binnen het ToKeN-programma onder projectnummer: 634.000.017.

E.M. Meijers Instituut voor Rechtswetenschappelijk onderzoek.
Dit onderzoek is tot stand gekomen binnen het onderzoeksprogramma 'Criminal Justice: Legitimacy, Accountability, and Effectivity' van de Universiteit Leiden.

SIKS dissertation series no. 2009-35
The research reported in this thesis had been carried out under the auspices of SIKS, the Dutch Research School for Information and Knowledge Systems.

Lay-out: AlphaZet prepress, Waddinxveen

© W.I. Koelewijn / Leiden University Press, 2009
ISBN 978 90 8728 070 3
e-ISBN 978 90 4851 138 9

Behoudens de in of krachtens de Auteurswet van 1912 gestelde uitzonderingen mag niets uit deze uitgave worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand, of openbaar gemaakt, in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of enige andere manier, zonder voorafgaande schriftelijke toestemming van de uitgever.

Voorzover het maken van reprografische verveelvoudigingen uit deze uitgave is toegestaan op grond van artikel 16h Auteurswet 1912 dient men de daarvoor wettelijk verschuldigde vergoedingen te voldoen aan de Stichting Reprorecht (Postbus 3060, 2130 KB Hoofddorp, www.reprorecht.nl). Voor het overnemen van (een) gedeelte(n) uit deze uitgave in bloemlezingen, readers en andere compilatiewerken (art. 16 Auteurswet 1912) kan men zich wenden tot de Stichting PRO (Stichting Publicatie- en Reproductierechten Organisatie, Postbus 3060, 2130 KB Hoofddorp).

No part of this book may be reproduced in any form, by print, photoprint, microfilm or any other means without written permission from the publisher.

Voorwoord

De Franse socioloog Jacques Ellul (1912 – 1994) signaleerde tijdens zijn leven dat de westerse cultuur sinds de renaissance in toenemende mate op een rationeel gestroomlijnde leest werd geschoeid. Volgens hem is de techniek daarbij een alles bepalende factor geworden. Uiteindelijk zullen de technologische ontwikkelingen volgens Ellul tot gevolg hebben dat de vrijheid van mensen om hun eigen leven vorm te geven steeds verder wordt uitgehold. Wanneer het gaat om technologische ontwikkelingen aangaande de opsporing van strafbare feiten zoals de verwerking van politiegegevens, zal de techniek er volgens Ellul uiteindelijk voor kunnen zorgen dat het gedrag van ieder individu kenbaar is bij de politiële autoriteiten. In zo'n samenleving bestaat geen privacy en geen vrijheid.

Hoewel ik diverse vraagtekens plaats bij deze signaleringen en voorspellingen van Ellul, hebben zijn soms wat absurdistische ideeën en toekomstvisies mijn onderzoek wel een vruchtbare denkpiste verschaft. Het uitgangspunt voor het onderzoek was namelijk dat het recht op privacy, ondanks de enorme technologische ontwikkelingen, op adequate wijze gewaarborgd dient te blijven. Bij de verwerking van politiegegevens worden technologische ontwikkelingen vaak gezien als een bedreiging van de privacy en daarmee van de vrijheid van individuele burgers. Binnen het interdisciplinaire onderzoek, waar mijn proefschrift een onderdeel van vormt, ligt de focus op de elektronische uitwisseling van politiegegevens. Door vele gesprekken met collega-onderzoekers werd mijn beeld over de gevaren van computers voor het recht op privacy aanmerkelijk genuanceerd en groeide het inzicht dat software juist ook een waardevol instrument kan zijn bij de waarborging van het recht op privacy. In het politiedomein wordt weinig aandacht besteed aan deze ideeën. De ontwikkeling van nieuwe informatiesystemen, zoeksystemen en analysesystemen zijn vooral vraaggestuurd. Systemen moeten slimme verbanden kunnen leggen die de politie zelf niet kan leggen. Er is daarbij niet of nauwelijks aandacht voor het inbouwen en ontwikkelen van normatieve beperkingen in het belang van de privacy. Dat is naar mijn mening echter wel noodzakelijk teneinde het recht op privacy ook in de toekomst te waarborgen. Er dient daarom meer aandacht te komen voor de wijze waarop informatiesystemen worden ontwikkeld. Met dit proefschrift wil ik een bijdrage leveren aan het wetenschappelijk, en wellicht ook maatschappelijk debat over dit onderbelichte onderwerp.

Graag wil ik op deze plek de Nederlandse Organisatie voor Wetenschappelijk Onderzoek danken voor de financiering van mijn onderzoek. Het E.M. Meijers Instituut voor Rechtswetenschappelijk Onderzoek, eLaw@Leiden,

centrum voor recht in de informatiemaatschappij van de Universiteit Leiden en de Nederlandse Onderzoeksschool voor Informatie- en Kennissystemen SIKS, dank ik voor het faciliteren van mijn onderzoek. Mijn gezin, Marloes, Nine en Lotte bedank ik voor de allesomvattende steun.

Wouter Koelewijn
Haarlem, juli 2009

Inhoudsopgave

VOORWOORD 5

INHOUDSOPGAVE 7

LIJST VAN GEBRUIKTE AFKORTINGEN 11

1 INTRODUCTIE
- 1.1 Maatschappelijke achtergrond 13
- 1.2 Aanleiding tot het onderzoek 16
- 1.3 Het anita-project 20
- 1.4 Probleemstelling en vier onderzoeksvragen 22
- 1.5 Het technologiedebat 25
- 1.6 Afbakening onderzoeksdomein 27
- 1.7 Methodologie van het onderzoek 28
  - 1.7.1 Literatuuronderzoek 30
  - 1.7.2 Veldwerk 31
  - 1.7.3 Analyse 32
  - 1.7.4 Discussie en oplossingsrichtingen 32
- 1.8 Structuur van het proefschrift 33

2 MOGELIJKHEDEN SOFTWAREAGENTEN 35
- 2.1 Artificiële intelligentie 35
- 2.2 Het concept *softwareagent* 39
  - 2.2.1 Autonomie 41
  - 2.2.2 Reactiviteit en adaptief gedrag 42
  - 2.2.3 Communicatie 42
- 2.3 Multi-agentsystemen 43
  - 2.3.1 Emergent gedrag 44
  - 2.3.2 Normatieve systemen 45
- 2.4 Resultaten ANITA-project 46
  - 2.4.1 Teepe 47
  - 2.4.2 Aldewereld 49
  - 2.4.3 Dijkstra 52
- 2.5 Beantwoording eerste onderzoeksvraag 53

3 HET JURIDISCH KADER 55
- 3.1 Historische achtergrond 55
  - 3.1.1 Periode van 1955 tot 1970 55
  - 3.1.2 Periode van 1971 tot 1991 56
  - 3.1.3 Periode van 1992 tot heden 58

3.2 Internationale normen 60
3.2.1 Het EVRM en het IVBPR 60
3.2.2 Het Europees Databeschermingsverdrag 62
3.2.3 Aanbevelingen van de Raad van Europa 63
3.3 Nationale normen: begrip, beheer, en doel 63
3.3.1 Het begrip 'politieregister' 64
3.3.2 Het beheer van politieregisters en databases 66
3.3.3 Doel register en goede uitvoering van politietaak 67
3.4 Nationale normen: algemene opnamecriteria en gevoelige gegevens 68
3.4.1 Algemene opnamecriteria 68
3.4.2 Gevoelige gegevens 71
3.5 Registers en verwerkingscriteria 72
3.5.1 Het voorlopig register 73
3.5.2 Het register zware criminaliteit 74
3.6 Wettelijk verstrekkingsregime 78
3.6.1 Het begrip 'verstrekken' 79
3.6.2 Algemene gesloten verstrekkingenregime 80
3.6.3 Het bijzonder verstrekkingenregime 82
3.6.4 Protocolplicht 82
3.6.5 De weigeringsgrond 83
3.6.6 Verstrekkingenregime in de Wpolg (2008) 84
3.7 Beantwoording tweede onderzoeksvraag 88
3.7.1 Vijf leidende rechtsbeginselen 89
3.7.2 Normatieve beperkingen en de privacy 90

4 DE CRIMINELE INLICHTINGENEENHEDEN 93
4.1 Historische ontwikkeling van de CIE 93
4.1.1 Van CID tot CIE 94
4.1.2 De informatie- en registratiesystemen 100
4.2 Taken van de CIE 103
4.2.1 Inwinnen van informatie 104
4.2.2 Veredelen en analyseren van informatie 106
4.3 Verstrekken van informatie 107
4.3.1 Verstrekking bij proces-verbaal 107
4.3.2 Verstrekking via informatierapport 108
4.3.3 Elektronische verstrekking 111
4.3.4 Mondelinge verstrekking 113
4.4 Tussenconclusies 114

5 KNELPUNTENINVENTARISATIE 115
5.1 Onderzoeken naar informatie-uitwisseling 115
5.1.1 Onderzoek 1996: Wpolr en Bpolr 116
5.1.2 Onderzoek 1998: Uitwisseling recherche-informatie 117
5.1.3 Onderzoek 2002: Uitwisseling van opsporings-informatie 118

5.1.4 Onderzoek 2004: Uitwisseling politie-informatie 121
5.1.5 Onderzoek 2005: Evaluatie Wet bijzondere politieregisters 124
5.2 Onderzoek 2005-2006: Eigen veldwerk 126
5.3 Tussenconclusies 129

6 ORGANISATIEANALYSE 131
6.1 CommonKads-methode 131
6.2 Organisatiemodel 135
6.2.1 Organisatiemodel 1: Knelpunten en oplossingen 136
6.2.2 Organisatiemodel 2: Beschrijving van organisatorische aspecten 139
6.2.3 Organisatiemodel 3: Bedrijfsproces informatie-uitwisseling 143
6.2.4 Organisatiemodel 4: Benodigde kennis 146
6.3 Taakmodellen 148
6.3.1 Taakmodel 1: Controle informatiegerechtigde 149
6.3.2 Taakmodel 2: Vaststellen doel 150
6.3.3 Taakmodel 3: Beoordeling afbreukrisico's 152
6.4 Beantwoording derde onderzoeksvraag 153

7 CONCEPTUELE ANALYSE 157
7.1 Theoretische basis 157
7.2 Normatieve softwareagenten in het CIE-domein 160
7.2.1 Indexeringsagent 162
7.2.2 Autorisatieagent 165
7.2.3 Zoekagent 167
7.2.4 Transactieagent 169
7.2.5 Poortwachteragent 170
7.2.6 Surveillanceagent 172
7.3 Conceptuele uitwerking 173
7.3.1 Centrale beheersindex 174
7.3.2 Autorisatie en doelstellingscontrole 177
7.3.3 Informatietransacties 180
7.3.4 Surveillancetoepassing 183
7.4 Verantwoording en discussie 185
7.5 Beantwoording vierde onderzoeksvraag 188

8 CONCLUSIES EN AANBEVELINGEN 191
8.1 Softwareagenten en multi-agenttechnieken 191
8.2 Juridisch kader 194
8.3 Organisatie en knelpunten 196
8.4 Conceptuele toepassing softwareagenten 199
8.5 Beantwoording probleemstelling 200
8.5.1 Rechtsbescherming 200
8.5.2 Technologische regulering 203

8.5.3 Discussie 206
8.6 Aanbevelingen 208
8.6.1 Aan de wetgever 208
8.6.2 Aan Politie en Justitie 210
8.6.3 Aan het Cbp 211
8.7 Slotbeschouwing 211

SAMENVATTING 213

SUMMARY 219

REFERENTIES 225

CURRICULUM VITAE 235

SIKS DISSERTATIEREEKS 237

VERSCHENEN IN DE MEIJERS-REEKS 243

Lijst van gebruikte afkortingen

ABRIO	Aanpak Bedrijfvoering Recherche Informatiehuishouding en Opleidingen
ACL	*Agent Communication Language*
AMvB	Algemene Maatregel van Bestuur
AI	Artificiële Intelligentie
AIVD	Algemene inlichtingen- en veiligheidsdienst
ANITA	*Administrative Normative Information Transaction Agents*
BOD	Bijzondere Opsporingsdienst
BOB	Bijzondere opsporingsbevoegdheden
Bpolg	Besluit politiegegevens
Bpolr	Besluit politieregisters
BPS	Bedrijfsprocessensysteem
Cbp	College bescherming persoonsgegevens
CIA	*Central Intelligence Agency*
CID	Criminele inlichtingendienst
CIE	Criminele inlichtingeneenheid
CRI	Centrale Recherche Informatiedienst
DNRI	Dienst Nationale Recherche Informatie
ECD	Economische Controledienst
EG	Europese Gemeenschap
EU	Europese Unie
EVRM	Europees verdrag voor de rechten van de mens
FBI	*Federal Bureau of Investigation*
FIOD	Fiscale Inlichtingen- en Opsporingsdienst
GBA	Gemeentelijke Basisadministratie
HKS	Herkenningdienstsysteem
HR	Hoge Raad
IAO	*Information Awareness Office*
ICT	Informatie- en Communicatietechnologie
IRT	Interregionaal Rechercheteam
IVBPR	Internationaal Verdrag inzake Burgerrechten en Politieke Rechten
KLPD	Korps Landelijke Politiediensten
MAS	Multi-agentsysteem
MOT	Meldpunt Ongebruikelijke Transacties
MRO	Melding Recherche Onderzoeken
MvA	Memorie van Antwoord
MvT	Memorie van Toelichting
NI	Unit Nationaal Inzicht

NRI	Nationale Recherche Informatie
OM	Openbaar Ministerie
OvJ	Officier van Justitie
OV	Onderzoeksvraag
PAA	*Protect America Act*
PEC	Parlementaire enquêtecommissie
PS	Probleemstelling
PSO	Politie Suite Opsporing
PZU	Platform zwacri-uitwisseling
RBS	Recherche Basissysteem
RCIE	Regionale Criminele Inlichtingeneenheid
RHC	Raad van Hoofdcommissarissen
RID	Regionale inlichtingendienst
RIO	Regionale Informatie Organisatie
SIOD	Sociale Inlichtingen en Opsporingsdienst
UCITA	*Uniform Computer Information Transactions Act*
UETA	*Uniform Electronic Transaction Act*
VROS	Verwijsindex Rechercheonderzoeken en Subjecten
Wbp	Wet bescherming persoonsgegevens
Wpolg	Wet Politiegegevens
Wpolr	Wet Politieregisters
WPR	Wet persoonsregistraties

1 Introductie

In dit proefschrift onderzoeken wij de mogelijkheden om de informatie-uitwisseling binnen de politieorganisatie te ondersteunen door ICT-toepassingen. De informatie-uitwisseling wordt grotendeels beheerst door twee conflicterende belangen, namelijk de goede uitvoering van de politietaak enerzijds en de bescherming van de persoonlijke levenssfeer anderzijds. In dit onderzoek wordt nagegaan (1) in hoeverre informatie-uitwisseling kan worden ondersteund door ICT-toepassingen met normatieve beperkingen waardoor een normconforme uitwisseling van politiële informatie tot stand kan worden gebracht, (2) welke juridische problemen er kleven aan het reguleren van de informatie-uitwisseling met behulp van software in het politiedomein en (3) in welke richting voor deze problemen oplossingen kunnen worden gezocht.

In sectie 1.1 zetten wij de maatschappelijke achtergrond van het onderzoek uiteen. Direct daarna, in sectie 1.2, gaan wij in op de aanleiding tot het onderzoek. In sectie 1.3 geven wij een toelichting op het ANITA-project, waarvan ons onderzoek een onderdeel vormt. Vervolgens formuleren wij in sectie 1.4 onze probleemstelling en vier daarbij behorende onderzoeksvragen. In sectie 1.5 plaatsen wij het onderzoek in de context van het wetenschappelijk debat over de mate waarin technologische ontwikkelingen stuurbaar zijn. Vervolgens wordt in sectie 1.6 het onderzoeksdomein verder afgebakend. Sectie 1.7 geeft inzicht in de onderzoeksmethoden. In sectie 1.8 beschrijven wij de structuur van dit proefschrift.

1.1 Maatschappelijke achtergrond

Na de aanslagen van 11 september 2001 werd in de Verenigde Staten de hoogste prioriteit gegeven aan terrorismebestrijding. Een van de eerste onduidelijkheden waarmee de Amerikaanse regering zich na de aanslagen geconfronteerd zag, betrof de vraag hoe het mogelijk was dat de voorbereiding voor een dergelijke aanslag voor de overheid onopgemerkt was gebleven. De FBI, CIA en andere betrokken veiligheidsdiensten bleken achteraf ieder afzonderlijk over veel bruikbare inlichtingen te beschikken.[1] Zo waren zij op de hoogte van het idee om vliegtuigen in te zetten als wapen, en beschikten de diensten over lijsten met terroristen en potentiële terroristen.

1 National Commission on Terrorist Attacks Upon the United States, Final Report on 9/11 Commission Recommendations, December 2005, <www.9-11pdp.org>.

Daarnaast bestonden er verdenkingen tegen enkele buitenlandse studenten die op Amerikaanse vliegscholen lessen hadden genomen en waren er gegevens beschikbaar van verdachte financiële transacties. Elk van deze gegevens afzonderlijk vormde geen duidelijke aanwijzing voor een aanslag, de combinatie daarvan mogelijk wel. Een belangrijke oorzaak in het ontbreken van integrale informatie vormde de gebrekkige communicatiemogelijkheden van de informatiesystemen van de verschillende bij het onderzoek betrokken veiligheidsdiensten. Elke organisatie beschikte over eigen systemen met eigen datamodellen en standaarden waardoor uitwisseling van informatie werd belemmerd en integrale veiligheidsinformatie bleek te ontbreken. Een citaat uit het rapport van de *National Commission on Terrorist Attacks Upon the United States* maakt dit duidelijk.

> "Information was not shared, sometimes inadvertently or because of legal misunderstandings. Analysis was not pooled. Effective operations were not launched. Often the handoffs of information were lost across the divide separating the foreign and domestic agencies of the government."[2]

De Amerikaanse overheid heeft aan dit probleem grote prioriteit gegeven en de informatie-uitwisseling tussen politiediensten en veiligheidsdiensten is een belangrijk middel geworden ter voorkoming van terroristische aanslagen.[3] Daartoe is onder meer de USA Patriot Act[4] ingevoerd en werd het zogeheten Information Awareness Office[5] opgericht. Binnen het IAO werd een Total Information Awareness Program ontwikkeld. Het doel van dit ontwikkelingsprogramma was om grote hoeveelheden (ruwe) informatie met behulp van geavanceerde software technologieën te verzamelen uit politiedatabases, databestanden van de veiligheidsdiensten en allerlei openbare bronnen zoals Internet. Daarnaast werden door het IAO technieken ontwikkeld om deze grote hoeveelheden informatie te analyseren teneinde daaruit potentiële terroristische dreigingen vroegtijdig te adresseren. Vanwege politieke onrust over de vergaande inbreuken die het IAO maakte op de persoonlijke levenssfeer werd na drie maanden al de naam van het programma veranderd in het Terrorism Information Awareness Program. Dat bleek echter niet voldoende om het programma te voorzien van voldoende democratisch draagvlak. In 2004 werd door de Senaat en het Huis van Afgevaardigden de financiering van het programma stopgezet. Slechts onderdelen van het programma werden verder ontwikkeld met als doel het verbeteren van

2 National Commission on Terrorist Attacks Upon the United States, The 9/11 Commission Report, Washington, July 2004, p. 353.

3 Statement of Robert J. Jordan, Information Sharing Initiatives, 17 April 2002.

4 USA Patriot Act of 2001, H.R. 3162, *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001*.

5 Het Information Awareness Office is in September 2003 opgehouden te bestaan toen de financiering werd ingetrokken, zie: Conference Report on H.R. 2658, Department of Defence Appropriations Act 2004, House Report 108-283.

de informatiepositie van de verschillende veiligheidsdiensten en het verbeteren van de uitwisseling van informatie.

Naast deze organisatorische maatregelen zijn ook verschillende maatregelen genomen om de bevoegdheden tot informatievergaring uit te breiden. Een voorbeeld daarvan is de op 5 augustus 2007 in werking getreden Protect America Act (PAA) die het voor de Amerikaanse veiligheidsdiensten mogelijk maakt om zonder voorafgaande rechterlijke machtiging, Internet- en telefoonverkeer af te luisteren buiten de Verenigde Staten. Het eerder aangehaalde citaat uit het onderzoeksrapport naar de aanslagen van 11 september 2001 toont aan dat een uitbreiding van de bevoegdheden tot informatievergaring niet los kan worden gezien van een effectieve uitwisseling van informatie.

Het Amerikaanse voorbeeld illustreert het belang van informatie-uitwisseling tussen politiediensten en veiligheidsdiensten voor de opsporing van (mogelijke) dreigingen. Het opsporingsbelang moet in dit licht worden gezien als een onderdeel van het veiligheidsbelang van burgers. De uitwisseling van grote hoeveelheden informatie tussen veiligheidsdiensten en/of politiediensten onderling heeft evenwel ook een keerzijde die meer in zijn algemeenheid geldt voor ieder beleid dat ziet op de bestrijding van terrorisme en criminaliteit. De Amerikaanse rechtsfilosoof Ignatieff (2002) beschrijft deze keerzijde als een *democratisch dilemma*. Dit dilemma wordt veroorzaakt door het spanningsveld tussen veiligheid van de meerderheid enerzijds en de inperking van de vrijheid van de minderheid of het individu anderzijds. Veel burgers menen dat genoemde verwerking van persoonsgegevens geen probleem is zolang je als burger niets te verbergen hebt. Deze burgers ervaren de verwerking van persoonsgegevens niet als een inbreuk op hun vrijheid of privacy. Een dergelijke houding wordt ons inziens vooral ingegeven door het feit dat de gevolgen van gegevensverwerking niet direct zichtbaar zijn voor de individuele burgers. Dit leidt in veel gevallen tot een onderschatting van de mogelijke gevolgen van een onbegrensd inzicht van de overheid in het privéleven van haar onderdanen. Het staat evenwel vast dat een dergelijk inzicht een vergaande inbreuk vormt op de persoonlijke levenssfeer en meer specifiek op de informationele privacy (Van Gunsteren, 2004). De directe gevolgen zijn wellicht onzichtbaar, maar dat geldt niet voor de consequenties op de lange termijn. Van Gunsteren (2004) wijst als één van de velen op de nadelige gevolgen en waarschuwt ervoor dat dergelijke vergaande inbreuken op lange termijn zouden kunnen leiden tot zelfdisciplinerend gedrag van burgers. En zo merkt hij op, juist dat tast de rechtsstatelijke vrijheid van het handelen van die burgers aan.

In Nederland zijn soortgelijke problemen gesignaleerd als in de Verenigde Staten waar het gaat om de uitwisseling van informatie tussen (1) politiediensten onderling, (2) veiligheidsdiensten onderling en (3) politiediensten en veiligheidsdiensten. Illustratief is de constatering van de Algemene

Rekenkamer in 2003 dat de verzameling en uitwisseling van informatie tussen politiekorpsen, inlichtingendiensten, en bijzondere opsporingsdiensten tekortkomingen vertoont.[6] Eenzelfde conclusie[7] is getrokken met betrekking tot het verzamelen en uitwisselen van informatie over (potentiële) criminele activiteiten tussen de politieregio's[8] onderling. Sinds 1985 heeft de Algemene Rekenkamer verschillende malen de politiële informatie-uitwisseling onderzocht, en telkens is geconcludeerd dat de uitwisseling onvoldoende van de grond is gekomen. Meermalen is geconstateerd dat de belangrijkste oorzaak daarvoor gezocht moet worden in de verticale scheiding van informatie binnen de politieorganisatie (Koolen en Moonen, 2004). Verticaal scheiden wil zeggen dat informatie per dossier, per specialisme, of per regio wordt opgeslagen met als gevolg dat er onvoldoende samenhang bestaat tussen de verschillende informatiestromen. Het voorbeeld van de Verenigde Staten laat zien dat juist de samenhang tussen delen van informatie van belang kan zijn omdat alleen de combinatie daarvan een goed en volledig inzicht kan geven. In Nederland zijn evenals in de Verenigde Staten ook verschillende maatregelen genomen ter verbetering van de informatie-uitwisseling op nationaal en regionaal niveau.[9] Dit neemt niet weg dat er nog steeds sprake is van knelpunten. In hoofdstuk 5 van dit proefschrift worden deze knelpunten uitgebreid geïnventariseerd.

1.2 Aanleiding tot het onderzoek

Een bijzondere categorie politiële informatie wordt gevormd door de zogenaamde criminele inlichtingen.[10] Het gaat dan vooral om tips en aanwijzingen van informanten met betrekking tot uiteenlopende vormen van zware criminaliteit. Voor de uitvoering van de politietaak[11] zijn criminele inlichtingen om twee redenen van belang. De eerste reden is dat zij in de pro-actieve

6 *Kamerstukken II*, 2002/03, 28 845, nrs. 1-2, p. 33.

7 *Kamerstukken II* 2002/03, 28 845, nr. 2.

8 De Nederlandse politieorganisatie is ingevolge art. 21 Politiewet 1993, opgedeeld in 25 verschillende politieregio's en een korps landelijke politiediensten.

9 Hierbij kan worden gedacht aan het ontwikkelen van het landelijke Verwijsindex Recherchеonderzoeken Systeem (VROS), maar ook verschillende maatregelen uit het actieplan terrorismebestrijding (*Kamerstukken II* 2001/02, 27925, nr. 10) zoals het onderzoek dat is gedaan naar de wettelijke belemmeringen van informatie-uitwisseling bij terrorismebestrijding. In hoofdstuk 4 wordt daarop uitgebreider ingegaan.

10 Criminele inlichtingen worden in art. 1 sub e CIE-regeling omschreven als gegevens die in aanmerking komen voor registratie in het register zware criminaliteit. De opnamecriteria voor deze gegevens zijn neergelegd in art. 13a lid 1 sub a t/m d Wet Politieregisters (Wpolr).

11 De politietaak valt ingevolge art. 2 politiewet 1993 uiteen in twee deeltaken, de daadwerkelijke handhaving van de rechtsorde en het verlenen van hulp aan hen die deze behoeven. Het gebruik van criminele inlichtingen is met name van belang bij de uitoefening van de eerste deeltaak waaronder ook de opsporing en voorkoming van strafbare feiten valt.

fase van de opsporing een belangrijke rol kunnen spelen bij (1) de voorkoming van misdrijven en (2) het opstarten van strafrechtelijke onderzoeken. De tweede reden is dat deze inlichtingen tevens een waardevolle rol kunnen spelen in de actieve fase van de opsporing omdat zij richting kunnen geven aan rechercheonderzoeken.[12]

Ieder regionaal politiekorps heeft een zogenaamde Criminele Inlichtingen Eenheid, kortweg aangeduid als de CIE. Deze eenheid is verantwoordelijk is voor het verzamelen, opslaan, verwerken en uitwisselen van inlichtingen die grotendeels afkomstig zijn van politie-informanten. De waarde van deze inlichtingen is groot, maar dat geldt ook voor de afbreukrisico's. Het domein waarin CIE-en hun werk doen is in meerdere opzichten buitengewoon complex en vraagt meestal per individueel geval een afweging tussen (1) het opsporingsbelang en (2) het belang van de informantenbescherming en privacy van derden. CIE-en hebben te maken met complexe wet- en regelgeving voor de verzameling, opslag, verwerking, en uitwisseling van criminele inlichtingen.[13]

De regels met betrekking tot de uitwisseling zijn gedetailleerd aangezien nauwkeurig in de wetgeving is vastgelegd aan welke personen en instanties informatie verstrekt mag worden. Toch laat de wetgeving binnen zekere marges ook beoordelingsruimte aan de CIE-en zelf om informatie al dan niet te verstrekken. Dit komt tot uitdrukking in het verplichtend karakter van de verstrekking van informatie binnen de politieorganisatie[14] en de mogelijkheden voor CIE-en om de uitwisseling van informatie te weigeren in het belang van de politiële taakuitvoering.[15] De wetgever acht het, ondanks de ruimte die zij laat voor weigering van verstrekkingen, van groot belang dat een vrije informatie-uitwisseling plaatsvindt binnen de politiegelederen. Dit blijkt ook uit de Memorie van Toelichting waarin expliciet wordt benadrukt dat de mogelijke aantasting van de persoonlijke levenssfeer niet gebruikt mag worden als weigeringsgrond bij de *interne* verstrekking, dat wil zeggen verstrekkingen binnen de politieorganisatie.[16] Dit betekent overigens niet dat de bescherming van de privacy helemaal geen rol speelt bij gegevensverwerking en uitwisseling door de politie. Privacyregels normeren de verwerking en uitwisseling door regels die zien op een zorgvuldig gegevensbeheer.

---

12 In dit proefschrift gebruiken wij de termen *politiële informatie* en *criminele inlichtingen* door elkaar. Wij doelen daarmee echter steeds op het wettelijke begrip *politiegegevens* zoals vastgelegd in art. 1 van de Wet Politiegegevens.

13 De inzet van burgerinformanten bij de verzameling is de Wet Bijzondere Opsporingsbevoegdheden (Wet BOB). Regels met betrekking tot de opslag verwerking, en uitwisseling zijn neergelegd in de Wet Politiegegevens, het Besluit Politiegegevens en de CIE-regeling.

14 Art. 14 Wpolr en art. 6 CIE-regeling.

15 Art. 13a lid 3 Wpolr juncto art. 11lid 1 Bpolr.

16 *Kamerstukken II* 1996/97, 25398, nr. 3, p. 4.

Het gaat dan onder meer om de beperking van bewaartermijnen en de geslotenheid van het verstrekkingenregime.

Verschillende uitkomsten van onderzoeken wijzen er echter op dat de uitwisseling van informatie te wensen over laat. De oorzaak daarvan moet naar onze mening worden gezocht in drie verschillende soorten barrières (juridisch, bestuurlijk, en technisch) die onderling sterk met elkaar samenhangen. De barrières worden op hun beurt veroorzaakt door uiteenlopende knelpunten die uitgebreid geïnventariseerd en geanalyseerd worden in hoofdstuk 5. Hieronder gaan we kort in op de genoemde barrières.

Ten eerste onderscheiden wij de juridische barrière. Deze barrière is niet direct het gevolg van een bepaalde wettelijke regel, maar meer het gevolg van de structuur van de toepasselijke wetgeving als geheel. Deze structuur gaat uit van regionaal georganiseerde informatiehuishoudingen met bijbehorende verantwoordelijkheden en bevoegdheden. Als gevolg daarvan heeft de politieorganisatie een sterk op de regio gerichte ontwikkeling doorgemaakt waarbij informatie in beginsel alleen voor regionaal rechercheonderzoek wordt gebruikt. Dat heeft bijgedragen aan een politiecultuur waarin het niet vanzelfsprekend was en voor een deel nog altijd niet vanzelfsprekend is, dat bijvoorbeeld criminele inlichtingen worden gedeeld met andere regio's.[17] De wettelijke ruimte voor beleidsontwikkeling op regionaal niveau lijkt mede de oorzaak van tekortkomingen in de informatie-uitwisseling. De ruim geformuleerde norm met betrekking tot de weigering van een verstrekking geeft deze beleidsruimte. De wetgever heeft evenwel beoogd tegemoet te komen aan de politiepraktijk en ruimte te willen laten voor een belangenafweging. Tegelijkertijd leiden open normen echter ook tot onduidelijkheid over de precieze bedoeling van de wetgever. In de politiepraktijk zijn voorbeelden bekend van situaties waarin deze onduidelijkheid leidde tot het ten onrechte weigeren van een informatieverstrekking (Schreuders e.a., 2005, p. 124).

Ten tweede onderscheiden wij de bestuurlijke barrière. Deze barrière speelt zich vooral op centraal niveau af. De barrière kan worden afgeleid uit het feit dat de Algemene Rekenkamer de regering al meer dan vijftien jaar wijst op de tekortkoming in de politiële informatie-uitwisseling zonder dat dit heeft geleid tot een adequate oplossing van het probleem.[18] Wij menen dat de oorzaak daarvan voor een belangrijk deel kan worden teruggevoerd op (1) de inrichting van de politieorganisatie en (2) de relatief grote autonomie van de regiokorpsen. Hierdoor is het bijzonder lastig om een centraal beleid te ontwikkelen dat bijvoorbeeld gericht is op het aanpakken van problemen in de

17 *Kamerstukken II* 2002/03, 28 845, nrs. 1-2.
18 *Kamerstukken I* 2002/03, 28 845, nrs. 1-2.

informatiehuishouding van de verschillende korpsen.[19] Mede daardoor heeft er ook binnen de CIE-afdelingen van de regiokorpsen vanaf het begin van de jaren negentig een cultuur kunnen groeien waarin de verzamelde inlichtingen eerst en vooral voor de regionale rechercheonderzoeken werden gebruikt (Aalbersberg, Barendregt en De Wit, 1993). Met het oog op onder meer deze problematiek zijn door de regering voorstellen gedaan om te komen tot een herziening van het politiestelsel.[20] In de Memorie van Toelichting op dat wetsvoorstel stelt de wetgever het volgende.

> "Het huidige bestel geeft ruimte voor en leidt tot grote verschillen tussen de politiekorpsen en een gebrek aan eenheid in taakuitvoering en in beheersmatige aangelegenheden, zoals ICT-beleid, personeelsbeleid en financieel beleid. Er is een gebrek aan strategische flexibiliteit bij de politie en daardoor komen noodzakelijke landelijke veranderingen maar langzaam tot stand."[21]

De Raad van State is echter van oordeel dat er geen dringende redenen zijn om het politiestelsel te herzien. Zij meent dat de huidige Politiewet 1993 voldoende mogelijkheden biedt aan de ministers van Justitie en Binnenlandse Zaken om aan de politie eisen te stellen.[22] Het wetsvoorstel is na dit advies en een wisseling van kabinetten ingetrokken.

Ten derde onderscheiden wij een technische barrière. Deze barrière hangt eveneens sterk samen met de regionaal georganiseerde informatiehuishoudingen. Er worden in het politiedomein verschillende informatiesystemen gebruikt en er is onvoldoende afstemming tussen de regio's over de wijze waarop gegevensbeheer is vormgegeven.[23] Dit betekent dat inlichtingen in allerlei vormen en op allerlei manieren worden opgeslagen, variërend van Word-documenten op lokale pc's tot geautomatiseerde registers die via een landelijk netwerk kunnen worden geraadpleegd. Deze diversiteit aan systemen veroorzaakt verschillende knelpunten in de informatie-uitwisseling (zie hoofdstuk 4).

---

19 Kenmerkend in dit verband is het feit dat op het moment van het schrijven van dit proefschrift vanuit het ministerie van Binnenlandse Zaken al meer dan 10 jaar zonder succes wordt gewerkt aan een centraal gecoördineerde gemeenschappelijke informatiehuishouding voor de politieorganisatie, de zogenaamde Politie Suite Opsporing (PSO). Dit project is in 2000 opgevolgd door PSO II dat in 2005 weer is stopgezet.

20 *Kamerstukken II* 2006/07, 30 880, nr. 1 en 2.

21 *Kamerstukken II* 2006/07, 30 880, nr. 1 en 2.

22 *Kamerstukken II* 2006/07, 30 880, nr. 3.

23 Rapport van de commissie Criminaliteit en Technologie o.v.v. P. Winsemius, *Technologie en misdaad, kansen en bedreigingen van technologie bij de beheersing van criminaliteit*, Den Haag, januari 2005.

De drie barrières vormen de belangrijkste aanleiding tot het doen van onderzoek naar de mogelijkheden die nieuwe softwaretechnieken bieden bij het verbeteren van de informatie-uitwisseling. Het onderzoek richt zich daarbij op (1) het in kaart brengen van de knelpunten en (2) het zoeken van een oplossing voor die knelpunten in een technologische richting.

1.3 Het ANITA-project

In 2002 is het ANITA-project[24] gestart waarin interdisciplinair onderzoek wordt gedaan naar de mogelijkheden van normatieve multi-agenttechnieken in het domein van de politiële gegevensuitwisseling. De doelstelling van het project is het ontwikkelen van juridisch verantwoorde regulering van de elektronische uitwisseling van politiegegevens met behulp van agenttechnieken. Binnen het ANITA-project wordt daartoe samengewerkt door onderzoekers van twee disciplines, de rechtswetenschap en de artificiële intelligentie (AI). De toepassing van normatieve multi-agenttechnieken houdt kort gezegd in dat verschillende soorten softwareagenten worden ontwikkeld die ieder aan de hand van hun eigen normatieve kennis een bepaalde rol vervullen bij de uitwisseling van politiegegevens (Jones en Carmo, 2001). In hoofdstuk 2 gaan wij uitgebreider in op het concept softwareagent maar wij achten het van belang om dit begrip op deze plaats in het proefschrift reeds enigszins te duiden. Daarvoor voor maken wij gebruik van de definitie van Shoham (1997) die softwareagenten als volgt omschrijft.

> "a software entity which functions continuously and autonomously in a particular environment, often inhabited by other agents and processes."

In deze definitie komen twee van de belangrijkste onderscheidende eigenschappen van softwareagenten naar voren, namelijk dat zij (a) *voortdurend* en (b) *autonoom* kunnen functioneren. Voortdurend wil zeggen dat de softwareagenten permanent beschikbaar zijn voor de uitvoering van hun specifieke taak. Zij behoeven in tegenstelling tot reguliere softwareprogramma's niet steeds (handmatig) opgestart te worden alvorens het programma zijn taak kan uitvoeren. Deze eigenschap is nauw verbonden met de zelfstandigheid van een softwareagent. Zelfstandig betekent in deze context zonder menselijke tussenkomst. Daarin schuilt het andere onderscheidende karakter met reguliere softwareprogramma's: bij reguliere programma's is menselijk handelen een noodzakelijk onderdeel, bij agent-gestuurde programma's is dit niet het geval. In hoofdstuk 2 worden de verschillende eigenschappen en mogelijkheden van softwareagenten nader uitgewerkt.

---

24 ANITA in de afkorting voor: Administrative Normative Information Transaction Agents, een project dat is gefinancierd door het ToKeN-programma van NWO onder nummer 634.000.017.

Enige toelichting op het begrip autonoom is hier echter wel op zijn plaats, omdat de samenwerking in interdisciplinair onderzoek als het ANITA-project heeft geleerd dat dergelijke begrippen vaak leiden tot een spraakverwarring tussen informatici en juristen. In een juridische context wordt met autonomie gedoeld op de onafhankelijkheid van de menselijke wil en de mogelijkheid voor mensen om voor zichzelf in vrijheid beslissingen te nemen. In de definitie van Shoham (1997) wordt daarentegen vooral gedoeld op de technische capaciteit van softwareagenten om zelfstandig te handelen, en niet zozeer op de vrijheid of onafhankelijkheid waarin dat handelen plaatsvindt. Daarnaast zijn er verschillende gradaties in de mate van zelfstandigheid die samenhangen met de technische inrichting van het multi-agent systeem (MAS). Ook hier komen wij in hoofdstuk 2 uitvoerig op terug.

Binnen het ANITA-project ligt de focus vooral op de mogelijke inzet van informatie-agenten zoals onderscheiden door Klusch (2001), omdat juist dit type softwareagenten, veel beter dan mensen, in staat zou zijn om grote hoeveelheden informatie te doorzoeken, te verwerken, en uit te wisselen. In concreto zou de toepassing van zo'n systeem moeten betekenen dat ambtenaren van CIE-en met behulp van softwareagenten in staat zijn criminele inlichtingen op grotere schaal uit te wisselen en te raadplegen dan nu vanwege de verschillende barrières het geval is. Een belangrijk element binnen het ANITA-project is het normatieve kader waarbinnen de softwareagenten handelen. Dit kader beoogt dat de uitwisseling van inlichtingen rechtmatig verloopt doordat de softwareagenten zich gedragen in overeenstemming met het normatief kader.

In het ANITA-project onderscheiden we vijf deelonderzoeken. Het eerste deelonderzoek (AI) is uitgevoerd door Teepe (2006) aan Rijksuniversiteit Groningen (RU). De resultaten van zijn onderzoek beogen technische oplossingsrichtingen te bieden voor het spanningsveld dat bestaat tussen het geheimhouden van informatie tegenover het delen van informatie.

Het tweede deelonderzoek (AI) is uitgevoerd aan de Universiteit Utrecht (UU) door Aldewereld (2007). Aldewereld gaat in op de technische mogelijkheden voor de normhandhaving in een multi-agent omgeving en onderzoekt twee methoden. Ten eerste beschouwt hij de *normering* van het gedrag van softwareagenten door de instelling van vooraf vastgestelde protocollen. Ten tweede ziet hij op het *controleren* van het gedrag van de softwareagenten en het toedienen van 'straffen' wanneer regels worden overtreden. Met deze twee methoden (normeren en controleren) beoogt hij een balans te vinden tussen de (technische) autonomie en het gewenste normconforme gedrag van softwareagenten.

Het derde deelonderzoek (AI) wordt uitgevoerd door Dijkstra (2007), eveneens aan Rijksuniversiteit Groningen. Zijn deelonderzoek richt zich op elektronische informatietransacties die tot stand komen op basis van onder-

handelingen tussen softwareagenten. Hierbij richt hij zich met name op de ontwikkeling van communicatieprotocollen voor softwareagenten. Dit onderzoek loopt nog.

Het vierde deelonderzoek (juridisch) wordt uitgevoerd door Kielman (2009) aan de Universiteit Leiden (UL). Hij brengt in kaart welke veranderingen de wetgever heeft aangebracht in het normatief kader voor de politiële gegevensverwerking en welke gevolgen dat heeft voor de bescherming van de privacybescherming van belanghebbenden.

Het vijfde deelonderzoek (juridisch/AI) is het onderhavige onderzoek. Daarin worden de resultaten van de AI-deelonderzoeken samengebracht met de resultaten van het juridische onderzoek door (1) de knelpunten in de praktijk van informatie-uitwisseling in kaart te brengen en (2) na te gaan waar de AI-technieken mogelijkheden bieden om deze knelpunten te verminderen of op te lossen. De resultaten van de AI-onderzoeken binnen het ANITA-project worden besproken in hoofdstuk 2.

1.4 Probleemstelling en vier onderzoeksvragen

Vooral na de aanslagen van New York (2001) en Madrid (2004) is in Nederland sprake van een toenemend (politiek) bewustzijn van het belang van uitwisseling van informatie voor de bestrijding en voorkoming van terrorisme en criminaliteit. Dit bewustzijn gaat echter gepaard met de constatering dat er barrières bestaan die een effectieve uitwisseling belemmeren. Ons onderzoek richt zich, zoals eerder aangegeven, op drie barrières (juridisch, bestuurlijk en technisch) en in samenhang daarmee (1) op het in kaart brengen van de knelpunten in de uitwisseling van inlichtingen en (2) op de mogelijkheden om oplossingen te bieden met behulp van multi-agenttechnieken. We beogen met het onderzoek een stap voorwaarts te maken bij het slechten van de geconstateerde barrières.

Technologische ontwikkelingen als fax, mobiele telefonie en Internet hebben, in combinatie met een toegenomen mobiliteit van personen, geleid tot internationalisering van de zware criminaliteit. Samenwerking en goede uitwisseling van inlichtingen op regionaal niveau maar ook op nationaal en internationaal niveau wordt daarom steeds belangrijker (zie: Verbeek, 2004). Ons onderzoek beperkt zich niettemin tot de uitwisseling van politiële inlichtingen op regionaal en nationaal niveau. Wij hangen in dit geval het natuurlijke groeimodel aan, en wel als volgt: van regionale uitwisseling via nationale uitwisseling naar internationale uitwisseling. In het algemeen menen wij dat een op normatieve kennis gebaseerd MAS kan bijdragen aan een oplossing van de knelpunten in de informatie-uitwisseling. Dit brengt ons tot de volgende probleemstelling (PS).

PS: *In hoeverre kan de inzet van softwareagenten en normatieve multi-agenttechnieken bijdragen aan de verbetering en de regulering van de elektronische uitwisseling van politiegegevens?*

De probleemstelling leidt tot vier onderzoeksvragen (OV). De eerste onderzoeksvraag ziet op de mogelijkheden van AI-technieken in zijn algemeenheid en de mogelijkheden van softwareagenten in het bijzonder. In de Artificiële Intelligentie (AI) worden verschillende veelbelovende eigenschappen en mogelijkheden toegeschreven aan multi-agenttechnieken. In dit onderzoek gaan wij allereerst na welke mogelijkheden dat zijn. De eerste onderzoeksvraag luidt als volgt.

OV 1: *Wat zijn de (theoretische) mogelijkheden van softwareagenten en multi-agenttechnieken?*

De tweede onderzoeksvraag ziet op de wijze waarop de uitwisseling van politiegegevens en de bescherming van de informationele privacy is vormgegeven. Het juridisch kader vormt het vertrekpunt voor de vraag op welke wijze AI-technieken ingezet zouden kunnen worden om het proces van informatie-uitwisseling te verbeteren, zowel vanuit het perspectief van de rechtshandhaving (de adequate uitvoering van de politietaak[25]) als vanuit het perspectief van de rechtsbescherming (bescherming van privacy). De tweede onderzoeksvraag luidt als volgt.

OV 2: *Op welke wijze heeft de wetgever de uitwisseling van criminele inlichtingen genormeerd?*

Het juridisch kader wordt gevormd door (1) formeel-wettelijke normen en (2) door materiële wettelijke normen en lokale invullingen daarvan. Op formeel-wettelijk niveau is gedurende het onderzoek sprake van een belangrijke rechtsontwikkeling. De voormalige Wet Politieregisters (Wpolr) is in de loop van de onderzoeksperiode vervangen door de Wet Politiegegevens, namelijk op 1 januari 2008. Deze aanpassing in het wettelijk regime heeft vanzelfsprekend consequenties voor het antwoord op deze onderzoeksvraag. In het proefschrift wordt daarom aandacht besteed aan zowel het voormalige als het 'nieuwe' formeel-wettelijk kader.

Bij de beantwoording van deze onderzoeksvraag rijzen verder interpretatieproblemen die voortvloeien uit het gebruik van open normen en van vage normen omdat zij uitwisseling van informatie reguleren.[26] De oorzaak voor

25 De Wet Politiegegevens spreekt overigens consequent van verwerking van gegevens voor de 'goede' uitvoering van de politietaak waarmee de wetgever heeft benadrukt dat een adequate gegevensverwerking van belang is voor uitvoering van de politietaak. Een adequate uitvoering van de politietaak is op zijn beurt weer van belang voor een effectieve rechtshandhaving.

26 Bijvoorbeeld art. 13a lid 3 Wpolr (oud), verstrekking van informatie kan worden geweigerd indien dit noodzakelijk is voor de goede uitvoering van de politietaak. De open norm is hier gelegen in het woord 'kan', deze laat ruimte voor nadere invulling in de praktijk. De vage norm is de 'goede uitvoering van de politietaak'.

het gebruik van dergelijke normen is dat het in zijn algemeenheid vaak onvermijdelijk is. In de juridische taal is onbepaaldheid en vaagheid vaak ingebakken. Daarnaast heeft de wetgever bewust voor deze vormen gekozen om, in casu de CIE, ruimte te geven rekening te kunnen houden met relevante omstandigheden en belangen. In de CIE-praktijk wordt op verschillende wijze invulling gegeven aan die normen en zijn deze vertaald in bepaalde technische en/of organisatorische maatregelen. Ons onderzoek richt zich op (1) de beoordeling van de huidige praktijk, (2) de ruimte die daarin ligt voor verbetering, en (3) de mogelijkheden die normatieve multi-agenttechnieken bieden om deze verbetering tot stand te brengen. Dat brengt ons tot de derde onderzoeksvraag.

OV 3: *Op welke wijze is de huidige uitwisseling van criminele inlichtingen ingericht en wat zijn daarin de (juridische) knelpunten?*

Om antwoord te kunnen geven op de probleemstelling is het van belang de huidige praktijk van uitwisseling van criminele inlichtingen in kaart te brengen en daarin de belangrijkste (juridische) knelpunten te identificeren. Zoals eerder opgemerkt is de uitwisseling van politiegegevens sinds het midden van de jaren tachtig regelmatig onderwerp van onderzoek geweest. Wij hebben voor het in kaart brengen van de gegevensuitwisseling en het inventariseren van de meest in het oog springende (juridische) knelpunten deze onderzoeken geanalyseerd. Hierbij is de focus gericht op het domein van de criminele inlichtingen. Het betreft onder andere onderzoeken in het kader van de wetsevaluaties van de Wet politieregisters en de Wet bijzondere politieregisters, alsmede empirische onderzoeken door de Algemene Rekenkamer en de Inspectie Openbare Orde en Veiligheid (Inspectie OOV) naar de bestaande praktijk van de gegevensuitwisseling. De analyse is uitgevoerd met behulp van de CommonKads methode (Schreiber e.a., 2000). CommonKads is een methode om gestructureerd na te gaan waar binnen een organisatie mogelijkheden liggen om handelingen te automatiseren. Wij hebben gedeelten van deze methode gebruikt om de organisatie rond de informatie-uitwisseling binnen de politieorganisatie en specifiek de CIE inzichtelijk te maken. Wij voeren twee analyses uit, te weten een organisatieanalyse en een knelpuntenanalyse.

De organisatie- en knelpuntenanalyse vormen het uitgangspunt voor de vierde onderzoeksvraag en deze luidt als volgt.

OV 4: *Op welke wijze kunnen softwareagenten en multi-agenttechnieken worden ingezet ten behoeve van de verbetering van het proces van informatie-uitwisseling vanuit het perspectief van de rechtshandhaving en de rechtsbescherming?*

Aan de hand van het geïnventariseerde overzicht van diverse mogelijkheden wordt in dit deel van het onderzoek nagegaan welke van deze mogelijkheden kunnen bijdragen aan de oplossing van de knelpunten die in het kader

van het antwoord op de derde onderzoeksvraag zijn gesignaleerd. Deze conceptuele analyse resulteert uiteindelijk in een antwoord op de probleemstelling.

1.5 Het technologiedebat

In de wetenschappelijke disciplines die zich bezighouden met de ontwikkeling van nieuwe technologieën of met de bestudering daarvan, wordt gediscussieerd over de mate waarin technologische ontwikkelingen stuurbaar zijn. In dit zogenaamde technologiedebat staan de aanhangers van het technologisch determinisme tegenover de aanhangers van het technologisch sociaal constructivisme. De technologisch deterministen gaan er vanuit dat de technologie als autonome kracht richting geeft aan sociale veranderingen. Dit betekent dat er van stuurbaarheid van die ontwikkelingen nauwelijks sprake kan zijn omdat technologie zich volgens hen ontwikkelt langs de autonome wetten van de techniek. Deze wetten komen er kort samengevat op neer dat efficiëntie altijd gaat voor moraliteit en dat de techniek een zo breed mogelijk werkingsgebied zoekt. Daarnaast stellen technologisch deterministen dat alles wat technisch mogelijk is uiteindelijk zal gebeuren. Een duidelijke exponent van deze benadering is Van den Herik (1983) die in zijn dissertatie stelde dat computers uiteindelijk een partij schaak zouden kunnen winnen van de mens. Deze voorspelling stuitte aanvankelijk op veel ongeloof en onbegrip maar veertien jaar later kreeg hij zijn gelijk toen Kasparov in 1997 een match van zes partijen verloor van de schaakcomputer Deep Blue (Campbell, Hoane en Hsu, 2001). Een zelfde soort voorspelling deed Van den Herik (1991) in zijn Leidse inaugurele rede toen hij stelde dat computers in 2080 zouden kunnen rechtspreken. Dergelijke voorspellingen vloeien voort uit een benadering die nadrukkelijk uitgaat van de autonomie van de technologische ontwikkelingen. Naast de 'positieve' voorspellingen van Van den Herik zijn er onder de technologische deterministen ook pessimistische geluiden hoorbaar. Een voorbeeld van een onderzoeker die pessimistische geluiden voortbrengt is de Franse socioloog Ellul (1964) die al in de jaren zestig grote vraagtekens zette bij de risico's die menselijke waarden lopen tegenover de overmacht van de technologie. Met name voor de rechtshandhaving door de politie schetst hij een donker scenario.

> "The techniques of the police, which are developing at an extremely rapid tempo, have as their necessary end the transformation of the entire nation into a concentration camp. This is no perverse decision on the part of some party of government. To be sure of apprehending criminals, it is necessary that everyone be supervised. It is necessary to know exactly what every citizen is up to, to know his relations, his amusements etc. This does not imply a reign of terror or of arbitrary arrests. The best technique is one which makes itself felt the least and which represents the least burden. But every citizen must be thoroughly known to the police and must live under conditions of discrete surveillance. All this results from the perfection of technical methods." (Ellul, 1964).

Hoewel de sombere voorspellingen van Ellul nog altijd niet zijn uitgekomen vormt technologie inmiddels wel een belangrijk middel in de surveillancemethoden door de politie. Schermer (2007) heeft in zijn dissertatie in dat verband de houdbaarheid van het juridisch kader onderzocht in het licht van de zich snel ontwikkelende surveillance met behulp van softwareagenten. Hij komt in de lijn van Ellul tot de conclusie dat deze technologische ontwikkeling de vrijheid en privacy van de geobserveerden hoe langer hoe meer onder druk zal zetten. In het verlengde daarvan stelt Schermer dat het huidige juridische kader voor de bescherming van de vrijheid en de privacy, dat met name geconcentreerd is rond het privacybegrip, in de toekomst niet langer afdoende zal blijken. Om die reden doet hij een aantal voorstellen tot aanpassing van het juridisch kader zodat daarmee de technologische ontwikkelingen op het terrein van surveillance met softwareagenten kan worden gereguleerd. Met deze voorstellen betreedt Schermer het domein van de technologisch sociaal constructivisten. Zij stellen in tegenstelling tot de technologisch deterministen dat juist sociale en culturele krachten bepalend zijn voor ontwikkelingen in de techniek. Volgens de Amerikaanse sociaal constructivist Fukuyama (2002) ontwikkelt technologie zich niet autonoom, maar zijn het uiteindelijk de mensen die de (gevolgen) van technologie naar hun hand kunnen zetten. Mumford (1963) was daar bijna veertig jaar eerder ook al van overtuigd, al vergt het volgens hem wel een sterke wil en krachtig ingrijpen. Maar zo stelt hij, techniek heeft de mens in ieder geval één ding geleerd namelijk dat niets onmogelijk is.

Zoals vaker voorkomt in wetenschappelijke discussies wordt er tussen twee uiterste benaderingen ook een middenpositie ingenomen. In het technologiedebat wordt dat gedaan door Hughes (1994) die tussen het technologisch determinisme en sociaal constructivisme de theorie van het technologisch momentum plaatst. Hij stelt dat sociale ontwikkeling en technologie elkaar wederkerig beïnvloeden en dat het evenwicht verschuift naar mate de technologie zich meer vestigt. Hoe omvattender en complexer de technologie wordt des te meer deze verweven raakt met verschillende sectoren in de samenleving, en des te groter het 'momentum' (determinerend vermogen) wordt. Dat gaat dan tevens gepaard met een geringere gevoeligheid voor de invloed die mensen of maatschappelijke groeperingen kunnen uitoefenen op de technologische ontwikkeling. Slechts hele intense of brede maatschappelijke veranderingen kunnen een technologie nog sturen. Als voorbeeld noemt Hughes de Amerikaanse auto-industrie die onder druk van de oliecrisis in 1973 en een groeiend milieubewustzijn compactere en zuinigere auto's ging produceren. Volgens hem zijn dus met name jonge technologische ontwikkelingen nog stuurbaar en daar zou dan ook de benadering van sociaal constructivisten kunnen werken. Oudere en gevestigde technologieën ontwikkelen zich veel meer volgens de wetten zoals die door de technologisch deterministen zijn vastgesteld.

In dit proefschrift staat de relatief 'jonge' technologische ontwikkeling van softwareagenten centraal. Het is opvallend dat in het debat rondom de inzet van deze technologie veel wordt gewezen op de gevaren voor de privacy (zie o.a. Borking, Van Eck en Siepel, 1999). Volgens technologisch deterministen zou het ook onontkoombaar zijn dat deze gevaren zich uiteindelijk manifesteren. Het onderhavige onderzoek ligt echter meer in de lijn van de benadering van het technologisch 'momentum' van Hughes. Wij menen dat het niet te laat is om invloed uit te oefenen op de richting waarin multi-agenttechnologie zich ontwikkelt. De techniek is relatief jong en daarom is het determinerend vermogen nog gering. In ons onderzoek wordt derhalve bewust niet het veelal pessimistische perspectief gekozen waarbij vooral gewezen wordt op de gevaren van softwareagenten. Wij beschouwen multi-agenttechnieken als een uitdaging om juist de belangen van rechtshandhaving en rechtsbescherming te dienen. Daarmee kiezen wij de zijde van Hughes en trachten wij met dit onderzoek de technologische ontwikkeling rondom multi-agenttechnieken te sturen in een richting die waardevol is en juist geen bedreiging vormt voor de privacy.

1.6 Afbakening onderzoeksdomein

De centrale doelstelling van het ANITA-project richt zich op de mogelijkheden voor regulering van de uitwisseling van politiegegevens met behulp van multi-agenttechnieken. Vanzelfsprekend brengt deze doelstelling beperkingen met zich mee ten aanzien van de richting waarin oplossingen worden gezocht voor bestaande knelpunten. In ons onderzoek ligt de nadruk op technologische oplossingsrichtingen binnen de CIE-organisatie en worden mogelijke alternatieve oplossingen met betrekking tot veranderingen in de organisatiestructuur, de coördinatie van de uitwisseling en de bedrijfscultuur buiten beschouwing gelaten. Datzelfde geldt voor de politieke dimensies en de eventuele gevolgen die aanpassingen in de politiëke informatiesystemen kunnen hebben, of zouden moeten hebben, voor de (hiërarchische) verhouding tussen de politie en het openbaar ministerie.

Het domein van de verwerking van politiegegevens is breed en er zijn zowel binnen als buiten de politieorganisatie veel verschillende instanties bij betrokken. Deze zogenaamde horizontale uitwisseling kan echter niet losgekoppeld worden van de verticale uitwisseling en om die reden is dan ook de verticale informatiestroom onderwerp van onderzoek geweest. Binnen het ANITA-project is sprake van beperking tot het domein van criminele inlichtingen. Dat heeft vanzelfsprekend gevolgen voor de genoemde onderwerpen in dit proefschrift. Er zijn twee redenen voor deze beperking. De eerste reden is gelegen in het feit dat uit verschillende onderzoeken naar voren is gekomen dat CIE-ambtenaren de van toepassing zijnde wet- en regelgeving vaak als lastig en complex ervaren (Cozijn e.a., 1996, Gunther Moor e.a., 1997,

Scheuders e.a., 2005). Dit vormt op zichzelf reeds aanleiding om aan te nemen dat er mogelijkheden aanwezig zijn voor de inzet van normatieve multi-agenttechnieken die de verwerking en uitwisseling van inlichtingen ondersteunen. De tweede reden hangt daarmee samen en heeft betrekking op de complexiteit van de belangen in dit domein. De regionale opsporingsbelangen enerzijds en de informationele privacybelangen van betrokkenen anderzijds, maken informatie-uitwisseling tot een interessant onderzoeksdomein voor juristen en AI-onderzoekers.

Een verdere beperking van onderzoek tot de CIE-praktijk is gelegen in de tijd. Wij beschrijven de periode 2005-2008. Zoals eerder opgemerkt zijn er volop ontwikkelingen gaande die uiteenlopen van het ontwikkelen en invoeren van nieuwe informatiesystemen tot een vergaande reorganisatie van de CIE-en. Omdat het onderzoek echter in tijd gebonden is en wij in deze periode een aantal (7) gesprekken hebben gevoerd met politieambtenaren uit de CIE-praktijk (zie hoofdstuk 5) is de organisatie in die periode 2005-2008 als uitgangspunt genomen. Wij hebben de praktijk beoordeeld aan de hand van het juridisch kader en de aansluiting op de doelstellingen van de wetgever. Daarvoor kiezen wij nadrukkelijk voor een normatief perspectief, omdat wij uitgaan van de vooronderstelling dat multi-agenttechnieken in het domein van de uitwisseling van criminele inlichtingen een effectieve bijdrage kunnen leveren aan de handhaving van het normatief kader. Zodoende introduceren wij in dit proefschrift multi-agenttechnieken als *waarborgingsmechanisme*.

1.7 Methodologie van het onderzoek

In de rechtswetenschap is al enige jaren een debat gaande over de vraag wat het betekent dat de rechtswetenschap een wetenschap is en welke consequenties dit heeft voor de methoden van onderzoek (zie bijvoorbeeld: Stolker, 2003). Twee op elkaar aansluitende vragen zijn in dit opzicht relevant.

(1) Dient een rechtswetenschappelijk onderzoeker zich bij het doen van onderzoek te beperken tot het in kaart brengen van verschillende posities van verschillende groepen ten aanzien van een bepaalde rechtsvraag?

(2) Moet het onderzoek gericht zijn op het zoveel mogelijk vaststellen van wat de *communis opinio* is, die dan als de 'objectieve waarheid' voor die specifieke kwestie moet worden beschouwd?

Afgezien van de beantwoording van deze twee vragen merken we op dat in de rechtsgeleerdheid er vrijwel altijd verschillende conclusies mogelijk zijn ten aanzien van rechtsvragen. Dat roept dan logischerwijs de nieuwe vraag op of het wel mogelijk is om te komen tot één juist antwoord of één objectieve waarheid. Dit is een immer terugkerend punt. Stolker (2003) lijkt zich in

het debat op te stellen als een exponent van het relativisme en gaat ervan uit dat het eenvoudigweg niet mogelijk is om 'ware' antwoorden te vinden op zulke kwesties, omdat deze afhankelijk zijn van wat in een gemeenschap als waar, goed en rechtvaardig wordt gezien. Gemeenschappen zijn veranderlijk en daarom zijn de antwoorden die gevonden worden per definitie relationeel, dat wil zeggen afhankelijk van argumenten en tegenargumenten (Smith, 1998). Een objectief waarheidbegrip dient vanuit dit perspectief dan ook te worden verworpen.

Een tweede immer terugkerend punt in deze discussie is de trend dat rechtswetenschappelijk onderzoek zich steeds meer richt op het recht zoals het zou moeten zijn. Rechtsgeleerdheid is daarmee in hoge mate een normatieve wetenschap waarin moraal en inzichten over de inrichting van onze nationale en internationale samenleving doorklinken in de uitkomsten van de onderzoeker. Het is de vraag of dat wenselijk is. Voor de methoden van rechtswetenschappelijk onderzoek zou dat kunnen betekenen dat juridische onderzoekers zich in belangrijke mate zouden moeten beperken tot het aanreiken van oplossingsrichtingen en mogelijke scenario's zonder daarin een echte keuze te maken. De 'echte' keuzes zouden moeten worden overgelaten aan de wetgever of de rechter. Stolker (2003) betoont zich voorstander van die terughoudendheid en wijst er in dat verband op dat de meeste juridische onderzoekers bovendien onvoldoende zijn toegerust om een analyse te maken van de doelmatigheid van een oplossing en deze vervolgens af te wegen tegen andere perspectieven.

Wij voelen echter voor de opvatting van Wendt (2005, 2008). Hij meent dat de rechtswetenschap vooral gezien moet worden als een 'technologie' waarmee hij wil uitdrukken dat de rechtswetenschap primair gericht zou moeten zijn op het zoeken naar 'beter recht', dus recht zoals het zou moeten zijn. In deze opvatting kunnen twee methoden van onderzoek worden onderscheiden.

De eerste methode is de methode van de systeemkritiek waarin het niet alleen gaat om kritiek op het systeem maar juist ook om opbouw en het geheel aan argumentatie dat daarmee gepaard gaat (Wendt 2008). Dit geldt evenzeer voor het formuleren van systeemkritiek op (technologische) toepassingen binnen juridische domeinen. In het verleden hebben we gezien dat Albert (1976, p. 187) uitgaat van een rechtswetenschappelijk onderzoeker die werkt vanuit bepaalde hypothetisch vooropgestelde gezichtspunten naar de formulering van een interpretatie van de in het geldende recht erkende normatieve stellingen. Maar, zo betoogt Albert, de onderzoeker kan ook voorstellen doen tot invoering van nieuwe wettelijke normen. Het is volgens Albert aan de bevoegde instituties in het rechtsstelsel om deze inzichten al dan niet over te nemen en een plaats te geven in het geldende recht. Op deze manier ontstaat een op de praktijk gerichte rechtswetenschap zonder dat deze een te sterk normatief karakter draagt.

De tweede methode is de methode van het empirisch onderzoek. Immers, empirisch onderzoek kan bijdragen tot een beter zicht op de vraag of de doelstellingen van wetgeving en andere vormen van juridische sturing daadwerkelijk bereikt worden (Wendt, 2005). Bovendien kan het empirisch onderzoek bijdragen aan inzichten in neveneffecten of ongewenste effecten van juridisch handelen die weer kunnen leiden tot inzichten met betrekking tot oplossingsrichtingen.

In ons onderzoek kiezen wij als rechtswetenschappelijke onderzoeksmethode voor de systeemkritische benadering (de eerste methode) waarin wij op kleine schaal veldwerk hebben verricht (dus iets van de tweede methode). Het veldwerk was uitsluitend bedoeld om inzicht te krijgen in de CIE-praktijk en wij benadrukken dat wij daarmee geen wetenschappelijk verantwoord empirisch onderzoek beoogden te doen. Het 'rechtssysteem' (in de zin van: Fuller, 1964) dat centraal staat in deze studie is de uitwisseling van criminele inlichtingen.

Onze onderzoeksmethodologie ziet er kort gezegd als volgt uit. De bestaande praktijk wordt in kaart gebracht met behulp van *literatuuronderzoek* (subsectie 1.7.1) en *veldwerk* (subsectie 1.7.2). Vervolgens wordt met behulp van *analyse* van de resultaten onderzocht welke knelpunten er in dit systeem zitten en hoe technologische aanpassingen in het systeem tot een verbetering kunnen leiden (subsectie 1.7.3). Wij menen met dit onderzoek geen 'waar' antwoord te vinden op de probleemstelling, maar beogen een op de praktijkgericht rechtswetenschappelijk onderzoek uit te voeren waarin we beleidsmakers in de praktijk *voorzien van inzichten* hoe multi-agenttechnieken bijdragen aan een verbetering van de handhaving van juridische normen in het systeem van informatie-uitwisseling. Op dit punt sluiten wij ons via een omweg aan bij de opvattingen van Stolker (2003). Een rechtswetenschappelijk onderzoeker past ons inziens terughoudendheid toe ten aanzien van een *validatie* van de mogelijke technologische oplossingen. De validatie valt buiten het bereik van dit onderzoek en wij beperken ons (zoals het een rechtswetenschappelijk onderzoeker betaamt) tot het aanreiken van oplossingsrichtingen (subsectie 1.7.4).

1.7.1 Literatuuronderzoek

Ons onderzoek is begonnen met een literatuurstudie om het juridisch kader van de verwerking, en specifiek de uitwisseling van politiegegevens vast te leggen. Zo'n juridische kader is richtinggevend voor normen waarbinnen softwareagenten (1) de uitwisseling van de gegevens vormgeven en (2) de beslissingen omtrent de uitwisseling ondersteunen. Wij hebben verder in het bijzonder aandacht besteed aan *twee* evaluatieonderzoeken (Cozijn e.a., 1996 en Schreuder e.a., 2005) van het juridisch kader en *drie* empirische onderzoe-

ken[27] naar de bestaande praktijk van gegevensuitwisseling. Op basis van dit literatuuronderzoek zijn de achtergronden, taken, bevoegdheden, werkwijzen, en organisatie van de CIE nagegaan. Tijdens het onderzoek bleek dat er weinig literatuur beschikbaar was over de CIE, met name waar het gaat om een actuele beschrijving van de gang van zaken. Op basis van uitsluitend literatuuronderzoek zou het beeld derhalve onvolledig blijven. Om die reden hebben wij door middel van eigen interviews aanvullend onderzoek gedaan in de CIE-praktijk. De uitkomsten van het literatuuronderzoek en het veldwerk zijn vervolgens gebruikt voor het ontwerpen van een conceptueel model voor de gegevensuitwisseling met behulp van softwareagenten.

1.7.2 Veldwerk

In de periode van februari 2005 tot en met december 2005 hebben wij (Kielman en Koelewijn, zie hieronder) in totaal 15 regionale hoofden van de CIE telefonisch benaderd met het verzoek om een interview te houden met politieambtenaren die werkzaam zijn bij de CIE. Van de 15 CIE-hoofden hebben er 7 positief gereageerd en konden vervolgafspraken worden gemaakt. Daarop zijn in de loop van de onderzoeksperiode in zeven politieregio's[28] interviews gehouden. De interviews zijn door Kielman en Koelewijn gezamenlijk afgenomen. Vanwege de gevoeligheid rondom het CIE-werk werd door de geïnterviewden geen toestemming gegeven om bandopnamen of videoopnamen van de gesprekken te maken. Wel zijn tijdens het interview aantekeningen gemaakt die direct na afloop van het interview door een van de onderzoekers zijn uitgewerkt. Het gespreksverslag is vervolgens ter verificatie voorgelegd aan de andere onderzoeker. De knelpunten- en organisatieanalyse die tot stand is gekomen op basis van de gehouden interviews en de resultaten van ons onderzoek zijn tenslotte ter nadere validatie voorgelegd aan een (politie)organisatiedeskundige, de heer Johan Oostveen.

In de 7 gesprekken hebben wij in het totaal gesproken met 12 CIE-ambtenaren van wie 5 ten tijde van het interview een leidinggevende functie (CIE-hoofden) bekleedden; en verder 2 runners[29], 1 informatierechercheur, 1 administrateur, en 3 groepschefs. Daarnaast is gesproken met een privacyadviseur van de politieacademie, een CIE-Officier van Justitie, en een informatiespecialist van het Concern Informatiemanagement Politie (CIP).

---

27 Algemene Rekenkamer 1998 en 2003, en de Inspectie OOV 2004.

28 Wij hebben zoveel mogelijk gestreefd naar een geografische spreiding zodat zowel regio's uit de randstad, als het noorden, midden, en zuiden van Nederland zijn bezocht.

29 Een runner is een politieambtenaar die als de contactpersoon functioneert van (criminele) informanten. Het onderhouden van deze contacten wordt binnen CIE aangeduid als het 'runnen' van informanten en zodoende wordt de politieambtenaar die belast is met deze taak een 'runner' genoemd.

1.7.3 Analyse

Na ieder interview zijn de resultaten uitgewerkt en geanalyseerd waardoor de gelegenheid werd gecreëerd om in het volgende interview de nieuwe bevindingen te verifiëren en onduidelijkheden nader uit te diepen. Het ging ons er tenslotte om op *exploratieve* wijze meer kennis over het domein te vergaren. Uiteindelijk is in de loop van de interviews een consistent beeld ontstaan over de wijze waarop aan informatie-uitwisseling in de praktijk is vormgegeven. Wij benadrukken nogmaals dat het niet onze bedoeling was om kwalitatief empirisch onderzoek te verrichten en vervolgens op basis van de resultaten van dat onderzoek normatieve uitspraken te doen over de CIE-praktijk.

Met behulp van de CommonKads methode (Schreiber e.a., 2000) hebben we vervolgens de in het literatuuronderzoek en veldwerk vergaarde kennis rondom de informatie-uitwisseling gestructureerd in kaart gebracht en geanalyseerd. Door deze analyse werd het mogelijk om na te gaan waar er mogelijkheden liggen om taken in het proces van de informatie-uitwisseling verder te automatiseren en te 'intelligentiseren'. De CommonKads methode is ontwikkeld voor het bouwen van kennissystemen, maar leent zich wat de organisatieanalyse betreft ook voor de ontwikkeling van multi-agentsystemen. Het ontwikkelingstraject wordt in deze methode opgedeeld in verschillende fasen met bijbehorende modellen. CommonKads voorziet in een volledige ontwikkelingscyclus van probleemdefinitie tot de daadwerkelijke oplevering en onderhoud van het systeem. In het kader van onderhavig onderzoek hebben wij CommonKads gebruikt als analysemethode voor het uitvoeren van een identificatieonderzoek, dat wil zeggen, er wordt nagegaan welke knelpunten zich voordoen in het proces van uitwisselen van informatie. Wij hebben in ons onderzoek gekeken in hoeverre de verschillende taken in het proces van de informatie-uitwisseling verder konden worden geautomatiseerd en 'geïntelligentiseerd'.

1.7.4 Discussie en oplossingsrichtingen

De uitgevoerde analyse resulteerde in een overzicht van (juridische) knelpunten die op zijn beurt het vertrekpunt vormde voor het zoeken naar oplossingen in het domein van de multi-agenttechnologie. De mogelijkheden die op het gebied van de multi-agenttechnologie voor handen zijn destilleren wij uit de literatuur. Op basis van de geconstateerde knelpunten en de technologische mogelijkheden om deze knelpunten op te lossen, doen wij enkele (conceptuele) voorstellen voor de toepassing van deze multi-agenttechnieken ter ondersteuning van de informatie-uitwisseling in het politiedomein.

Omdat wij in dit onderzoek, zoals gezegd, menen geen 'waar' antwoord te kunnen vinden op de probleemstelling analyseren wij verschillende discussiepunten ten aanzien van de door ons voorgestelde oplossingsrichtingen. Die discussiepunten bespreken wij aan de hand van de twee invalshoeken, te weten (1) de rechtshandhaving waarbij het meer specifiek gaat om de adequate uitvoering van de politietaak en (2) de rechtsbescherming ten aanzien van de informationele privacy. Vervolgens wordt in deze conceptuele analyse ook nagegaan welke nieuwe juridische vraagstukken de implementatie van softwareagenten met zich brengt en welke oplossingsrichtingen daarvoor mogelijk zijn.

De conceptuele analyse dient tenslotte te resulteren in enkele conclusies ten aanzien van de probleemstelling. Op basis daarvan zullen wij in staat zijn aanbevelingen te formuleren aan verschillende betrokken instituties in de rechtspraktijk (wetgever, politie en justitie en het Cbp).

1.8 Structuur van het proefschrift

Hieronder volgt een beschrijving van de structuur van het proefschrift. In hoofdstuk 1 geven wij een korte inleiding op het probleemgebied en vermelden wij de probleemstelling alsmede de vier onderzoeksvragen. Verder zetten wij de methode van onderzoek uiteen.

In hoofdstuk 2 beschrijven wij de mogelijkheden van agenttechnologie. Dat gebeurt aan de hand van de verschillende eigenschappen en mogelijkheden die in de literatuur aan softwareagenten worden toegeschreven. Vervolgens bespreken wij de resultaten van drie AI-deelonderzoeken binnen het ANITA-project. Deze resultaten geven inzicht in de mogelijkheden van normatieve agenttechnieken toegespitst op het politiedomein. Hoofdstuk 2 geeft daarmee een antwoord op de eerste onderzoeksvraag.

Hoofdstuk 3 beschrijft het juridisch kader waarbinnen de gegevensuitwisseling dient plaats te vinden en gaat in op de actuele rechtsontwikkelingen (de vervanging van de Wpolr door de Wpolg), en de gevolgen die dat heeft voor de uitwisseling van criminele inlichtingen. Het juridisch kader vormt in het onderzoek het uitgangspunt om (1) de huidige praktijk van uitwisselen te beoordelen en (2) na te gaan in hoeverre daarin ruimte wordt gelaten om de uitwisseling vorm te geven met behulp van softwareagenten. Het hoofdstuk geeft antwoord op de tweede onderzoeksvraag.

In hoofdstuk 4 geven wij een algemene beschrijving van de context van het onderzoeksdomein waarbij aandacht wordt besteed aan het ontstaan en de ontwikkeling van Criminele Inlichtingeneenheden en het gebruik van registratie- en communicatiesystemen. Verder beschrijft het hoofdstuk de huidige

CIE-praktijk, de taken en de bevoegdheden, en behandelt het de verschillende wijzen waarop de informatie-uitwisseling rondom deze politiële eenheden is vormgegeven. Wij besluiten het hoofdstuk met het formuleren van enkele tussenconclusies.

In hoofdstuk 5 inventariseren wij de belangrijkste knelpunten met betrekking tot het uitwisselen van politiegegevens (onderdeel van de derde onderzoeksvraag). Deze inventarisatie geschiedt aan de hand van vijf onderzoeken waaruit wij de belangrijkste hoofdknelpunten in kaart brengen. Deze hoofdknelpunten vormen vervolgens het vertrekpunt voor de organisatieanalyse.

In hoofdstuk 6 wordt met behulp van CommonKads de organisatorische context en het proces van informatie-uitwisseling in kaart gebracht. Een belangrijk deel van de kennis met betrekking tot de wijze waarop de CIE-organisatie is opgebouwd putten wij uit ons eigen veldwerk. Dat is noodzakelijk omdat over de CIE-organisatie omtrent de gegevensuitwisseling relatief weinig literatuur beschikbaar is en voor zover die er is gaat het om relatief oude bronnen. Uit ons eigen veldonderzoek is naar voren gekomen dat er verschillende regionale organisatievormen kunnen worden onderscheiden. Deze vormen worden uitgewerkt met behulp van de CommonKads methode. Hoofdstuk 6 geeft daarmee antwoord op de derde onderzoeksvraag.

In hoofdstuk 7 wordt met het oog op de in hoofdstuk 2 onderscheiden mogelijkheden nagegaan welke taken in het proces van de uitwisseling van inlichtingen (hoofdstuk 6) kunnen worden ondersteund door softwareagenten. Met behulp van een conceptuele analyse wordt vervolgens gekeken in hoeverre agenttechnologie bijdraagt aan een oplossing van de geconstateerde knelpunten in de uitwisseling van criminele inlichtingen. Dat doen wij aan de hand van twee invalshoeken. De eerste invalshoek betreft de rechtshandhaving waarbij de nadruk ligt op de mogelijkheden die de inzet van softwareagenten biedt bij het beter waarborgen van de goede uitvoering van de politietaak. De tweede invalshoek betreft de rechtsbescherming. Daarbij wordt gekeken hoe de inzet van softwareagenten kan bijdragen aan de bescherming van de informationele privacy. Tevens wordt in dit hoofdstuk ingegaan op de juridische vragen die samenhangen met de normering van handelen via computersystemen in dit specifieke domein. Daarbij zal aandacht worden besteed aan de 'Code as Law'-discussie (Lessig, 1999) en legitimeringsvraagstukken die samenhangen met *regulating by architecture* (Dommering en Asscher, 2006). Hoofdstuk 7 geeft daarmee een antwoord op de vierde onderzoeksvraag.

In hoofdstuk 8 geven wij tenslotte antwoord op de probleemstelling. Dit resulteert in een aantal conclusies en aanbevelingen over de toepassing van multi-agenttechnologie in het politiedomein.

2 Mogelijkheden softwareagenten

In dit hoofdstuk behandelen wij de eerste onderzoeksvraag (OV 1): wat zijn de theoretische mogelijkheden van softwareagenten en multi-agenttechnieken? Daartoe beschrijven wij het concept *softwareagent* aan de hand van een aantal eigenschappen en mogelijkheden. Wij beogen allereerst de lezer meer inzicht te geven in de technologische ontwikkeling. Dit inzicht is nodig omdat wij in hoofdstuk 7 voortborduren op deze kennis. Wij zullen daar immers aangeven wat softwareagenten in het proces van informatie-uitwisseling ons inziens kunnen bijdragen aan het optimaliseren van de rechtshandhaving en rechtsbescherming.

In sectie 2.1 geven wij een toelichting op het concept *Artificiële Intelligentie* (AI). Het is de wetenschap die zich bezighoudt met de technische ontwikkeling van softwareagenten. Vervolgens gaan wij in sectie 2.2 dieper in op het concept *softwareagent*. In sectie 2.3 behandelen wij de theoretische achtergronden van multi-agentsystemen. Daarna geven wij in sectie 2.4 een overzicht van enkele bestaande domeintoepassingen. Vervolgens, in sectie 2.5, worden de mogelijkheden besproken die binnen het ANITA-project zijn ontwikkeld. In sectie 2.6 formuleren wij tenslotte een antwoord op OV 1.

2.1 Artificiële intelligentie

Voor ons onderzoek is een goed begrip van AI van belang omdat het aangeeft in welke richting computers zich ontwikkelen. We merken op dat agenttechnologie een onderdeel is van de AI. Om enig inzicht te krijgen in de mogelijkheden van softwareagenten en multi-agenttechnieken is het daarom nodig om globaal de achtergronden te kennen van de wetenschap die zich bezighoudt met de ontwikkeling van deze technieken. In dat verband wordt vaak de omschrijving van Kurzweil (1990) aangehaald die de AI heeft gedefinieerd als:

> "The art of creating machines that perform functions that require intelligence when performed by people."

Het onderzoek binnen de AI richt zich derhalve op het ontwikkelen van machines die taken kunnen uitvoeren waarvoor een bepaalde mate van menselijke intelligentie nodig is. Dat roept vervolgens de vraag op wat onder intelligentie moet worden verstaan. Daarover kan veel worden gezegd, maar het wetenschappelijk debat over intelligentie valt buiten het bereik van dit proefschrift. Wij volgen hier Postma (2003) die in zijn oratie aansluiting zoekt

bij elementen van intelligentie die door Wechsler (1958) zijn onderscheiden. Wechsler stelt dat intelligentie het vermogen is (1) tot zinvol handelen, (2) tot rationeel denken, en (3) om effectief om te gaan met de omgeving.

Om inzicht te krijgen in de ontwikkelingen en mogelijke trends behandelen wij hier in chronologische volgorde vanaf 1950 enkele van de belangrijkste ontwikkelingen en successen die binnen de AI zijn geboekt.

Turing (1950) was de eerste wetenschappelijk onderzoeker die zich de vraag stelde of machines zouden kunnen denken en wanneer gesproken zou kunnen worden van intelligentie bij machines. In zijn artikel *Computing Machinery and Intelligence* ontwikkelde hij een test aan de hand waarvan kan worden vastgesteld of een machine menselijke intelligentie vertoont. In deze test communiceert een proefpersoon met een mens en een computer. De twee gesprekken vinden plaats via een toetsenbord. Wanneer de proefpersoon niet consistent kan aangeven of hij met een mens of een computer communiceert, kan de betreffende computer volgens Turing intelligent worden genoemd.

Het onderzoek binnen de AI heeft zich vanaf de jaren vijftig van de vorige eeuw gericht op de mogelijkheden van de computer. In de beginperiode ging het daarbij om het representeren van kennis in feiten en regels. De gedachte die aan deze benadering ten grondslag lag was (1) dat ook de menselijke cognitie is gebaseerd op het manipuleren van symbolen en (2) de grote gelijkenis die cognitief redeneren (schaken, puzzels oplossen, vertalen) vertoont met de werking van een computer. In een computer worden reeksen enen en nullen gemanipuleerd en in het menselijke brein vindt iets soortgelijks plaats door een combinatie van actieve en inactieve hersencellen (cf. Postma, 2003). De moeilijkheid is echter gelegen in het feit dat voor de uitvoering van bepaalde taken andersoortige kennis moet worden vastgelegd. Met name voor complexe taakuitvoeringen moet veel impliciete of onderbewuste kennis worden vastgelegd. Om een computer vervolgens zo'n complexe taak te kunnen laten uitvoeren moet al deze impliciete kennis worden geformaliseerd. Het formaliseren van kennis in feiten en regels en het vervolgens toepassen daarvan wordt binnen de AI aangeduid als *rule-based reasoning*. In de praktijk blijkt dit eigenlijk alleen maar goed mogelijk op bepaalde deelgebieden waarin de impliciete kennis in de omgeving overzichtelijk is en expliciet gemaakt kan worden. Naarmate de complexiteit en omvang van de impliciete kennis toeneemt wordt het moeilijker deze te formaliseren.

Vanaf de jaren tachtig van de vorige eeuw is deze klassieke AI-benadering van het formaliseren van kennis in feiten en regels echter hoe langer hoe meer losgelaten en ontwikkelde zich een nieuwe benadering binnen de AI die wordt aangeduid als *case-based reasoning* (of zelfs *data-driven decision making*). Daarbij zijn niet langer regels en feiten het voornaamste uitgangs-

punt voor het 'redeneren' door een computer maar redeneert de computer kort gezegd aan de hand van resultaten van eerdere casus over een nieuwe casus. Recentelijk heeft Hamburg (2006) deze *case-based reasoning* technieken toegepast in zijn onderzoek naar de mogelijkheden van een computermodel voor euthanasiebeslissingen. Hij laat zien dat de computer op basis van ervaringen uit het verleden kan leren redeneren over toekomstige gevallen. Daarbij redeneert de computer over verschillende deelvragen van een casus verder aan de hand van eerdere uitkomsten. De uiteindelijke beslissing die een computer neemt is zodoende opgebouwd uit verschillende deelprocessen. Deze benadering is gebaseerd op het werk van Minsky (1988) die zich in zijn onderzoek richtte op het menselijk verstand. In zijn boek, *Society of the Mind,* stelt hij het verstand voor als een enorme gemeenschap van individueel eenvoudige niet-intelligente processen die hij 'agents' noemt. Hij vat zijn theorie als volgt samen.

> "What magical trick makes us intelligent? The trick is that there is no trick. The power of intelligence stems from our vast diversity, not from any single, perfect principle." (Minsky, 1988, p. 308).

Brooks (1991) werd geïnspireerd door deze theorie en stelde dat een hoger niveau van artificiële intelligentie daarom niet meer rechtstreeks in een machine geprogrammeerd zou moeten worden. De intelligentie, zo veronderstelt Brooks, komt als het ware vanzelf tevoorschijn uit de interactie van de verschillende modules met de fysieke wereld. Door deze interactie kunnen er complexe taken worden uitgevoerd die tezamen een intelligente actie genoemd kunnen worden. Met behulp van sensoren en communicatieprotocollen kan de interactie van de verschillende modules met de omgeving worden gerealiseerd. Zodoende is het niet noodzakelijk om de gehele omgeving waarbinnen de agenten werken in symbolen te representeren.

Wooldridge (2002) koppelt deze theorie aan software-omgevingen en stelt dat intelligentie daarin kan voortvloeien uit de interactie van op zichzelf eenvoudige processen tussen softwareprogrammaatjes, die ook wel worden aangeduid als softwareagenten. Wooldridge plaatst deze relatief nieuwe ontwikkeling rond softwareagenten in een bredere historische ontwikkeling rond het gebruik van computers. Hij onderscheidt daarin onder meer de volgende twee trends (1) *intelligence* en (2) *situation awareness*. Binnen het kader van dit proefschrift zijn deze twee trends van belang omdat zij aangeven in welke richting de mogelijkheden van computers zich ontwikkelen. Deze ontwikkeling zal op termijn ook gevolgen hebben voor het gebruik van informatiesystemen binnen de politieorganisatie.

(1) Wij duiden, zoals gezegd, de eerste trend van Wooldridge (2002) kort aan met het begrip *intelligence*. Computersystemen kunnen steeds ingewikkelder taken uitvoeren als ondersteuning voor de mens. Werd de computer aanvankelijk alleen maar gebruikt voor rekentaken, tegenwoordig worden

computers ingezet om complexe taken bij onbemande vluchten in de lucht- en ruimtevaart uit te voeren. Een toenemende inzet van *intelligentie* in computersystemen zien we ook terug in de politieorganisatie. Wij noemen als voorbeeld de inzet van *intelligente* camera's die in combinatie met detectiesoftware bepaalde surveillancetaken voor de politie kunnen uitvoeren. Met betrekking tot het gebruik van informatiesystemen verwachten wij dat informatiesystemen in de toekomst steeds intelligenter zullen omgaan met de daarin opgeslagen informatie. In combinatie met de toenemende opslagcapaciteit en de verruiming van de wettelijke mogelijkheden tot het verzamelen van politiegegevens, verwachten wij dat met name de technieken voor *data-driven decision making* zich vergaand zullen ontwikkelen. Daarbij moet niet alleen gedacht worden aan *profiling* op basis van de geregistreerde informatie maar ook aan de mogelijkheid dat een computer aangeeft of een persoon als verdachte moet worden aangemerkt.

(2) Wij duiden de tweede trend van Wooldridge (2002) aan met het begrip *situation awareness*. Daarmee doelt hij op de ontwikkeling dat bij het ontwerpen van computerprogramma's steeds meer uitgegaan wordt van de wijze waarop mensen *omgaan* met hun omgeving. Computers gaan in dat opzicht steeds meer lijken op mensen. Deze trend is ook duidelijk waarneembaar in ontwikkeling van software ter ondersteuning van opsporingsactiviteiten waarbij de wijze waarop opsporingsambtenaren kijken naar het rechercheproces als uitgangspunt wordt genomen voor de ontwikkeling van analysesoftware (Bex, Prakken en Verheij, 2007). Een ons inziens extreem standpunt wordt ingenomen door Levy (2007) in zijn proefschrift "Intimate relationship with artificial partners".

Hoe dan ook, deze twee trends leiden tot een sterke nadruk op onderzoek naar de mogelijke toepassingen van softwareagenten in uiteenlopende domeinen. Ons onderzoek richt zich op de mogelijkheden in het domein van de verwerking en uitwisseling van politiegegevens. Uit de hierboven door Wooldridge onderscheiden trends kan worden afgeleid dat ook informatiesystemen steeds intelligenter zullen omgaan met de daarin opgeslagen gegevens en steeds beter zullen aansluiten op de wijze waarop politieambtenaren opsporingsonderzoek verrichten. Wij verwachten zoals gezegd dat het belang van politiegegevens en de mogelijkheden van informatiesystemen in de komende tien jaar exponentieel zal toenemen. Dit biedt mogelijkheden voor de rechtshandhaving maar ook bedreigingen voor de rechtsbescherming. Welke rol softwareagenten en multi-agenttechnieken daarin precies kunnen spelen zal onderwerp zijn van hoofdstuk 6.

Naast het signaleren van deze twee trends in het huidige en toekomstige gebruik van computers worden binnen de AI veelbelovende voorspellingen gedaan over de ontwikkeling van intelligentie in computersystemen en over *situation awareness*. Het gaat daarbij vooral over de mate waarin de mens uiteindelijk in staat zal zijn om de processen die het menselijk brein intelli-

gent maken na te bouwen (c.q. te simuleren, te emuleren of te overtreffen) in computersystemen en ervoor te zorgen dat deze systemen de omgeving begrijpen.

Kurzweil (2005) gaat ervan uit dat er binnen de AI een zogenaamd *singularity point* zal worden bereikt. Hij doelt daarmee op het tijdstip dat de menselijke intelligentie wordt overtroffen door de kunstmatige intelligentie. Op diverse gebieden is dit al gebeurd of staat het te gebeuren. Een overtuigend voorbeeld is de overwinning van het schaakprogramma Deep Blue op de menselijke wereldkampioen Gary Kasparov in 1997 (Campbell, Hoane en Hsu, 2001). Zijn voorspelling over intelligentie in het algemeen baseert Kurzweil op het idee dat de ontwikkeling van verschillende technologieën (computertechnologie, nanotechnologie en gentechnologie) elkaar zodanig versnellen dat in 2030 het *singularity point* zal worden bereikt. Het zal dan volgens Kurzweil binnen afzienbare tijd mogelijk zijn dat de inhoud van menselijke hersenen wordt opgeslagen in computers waardoor niet langer meer een duidelijke scheiding tussen mens en machine kan worden gemaakt.

Los van de vraag of de voorspellingen van Kurzweil zullen uitkomen valt niet uit te sluiten dat computers op enig moment betere beslissingen kunnen nemen dan mensen. Dat maakt het noodzakelijk voor rechtswetenschappelijk onderzoekers om na te denken welke gevolgen dit zal hebben voor de houdbaarheid van bestaande rechtssystemen en de waarborging van fundamentele grondrechten. Binnen het kader van dit onderzoek dringt zich dan de vraag op wat de juridische status is van softwareagenten indien beslissingen over informatietransacties volledig worden overgelaten aan softwareagenten. Wanneer softwareagenten zulke beslissingen nemen in plaats van een politieambtenaar, wie is dan verantwoordelijk voor eventuele inbreuken op de privacy? Moet dat ondanks alles de politieambtenaar blijven of is de programmeur van de softwareagent daarvoor aansprakelijk? De voorspellingen van Kurzweil over de mogelijkheden van computers zijn uitdagend en veelbelovend tegelijkertijd. Hoe we er ook over denken, zij brengen voor ieder domein afzonderlijk nieuwe (juridische) vraagstukken met zich mee. Wij zullen in hoofdstuk 7 en 8 deze vraagstukken voor ons gebied nader adresseren.

In de volgende sectie gaan we voorts in op het concept softwareagent.

2.2 Het concept *softwareagent*

Er bestaat binnen de onderzoeksliteratuur in de artificiële intelligentie veel onduidelijkheid over de precieze definiëring van het concept softwareagent. Wij hebben in het vorige hoofdstuk voor een beter begrip daarvan aansluiting gezocht bij de definitie van Shoham (1997). In zijn definitie beschrijft hij

twee eigenschappen die softwareagenten onderscheiden van reguliere software. Het gaat dan om het *voortdurend* en *autonoom* kunnen handelen met andere partijen ten behoeve van de eigenaar van de softwareagent. Reguliere software wordt aangestuurd door menselijk handelen en doet uit zichzelf niets. Kenmerkend voor softwareagenten is dat menselijke tussenkomst niet langer vereist is, maar dat zij eenmaal werkend, *autonoom* hun gang kunnen gaan.

In de Nederlandse wetgeving is het concept softwareagent nergens gedefinieerd. Bij de beschrijving van het juridisch kader in hoofdstuk 3 zullen wij stilstaan bij het elektronisch uitwisselen van gegevens. De mogelijkheid van de inzet van softwareagenten bij de informatie-uitwisseling hebben wij geïnterpreteerd als een vorm van elektronische uitwisseling van gegevens die wel gereguleerd is. De wetgever heeft echter niet expliciet rekening gehouden met de toepassing van softwareagenten hetgeen te verklaren is door de relatieve onbekendheid van deze technologie binnen de juridische wereld. Derhalve is de juridische status van de softwareagenten vooralsnog onduidelijk in het domein van informatie-uitwisseling.

De Amerikaanse wetgever heeft softwareagenten wel gedefinieerd. In de Uniform Computer Information Transactions Act uit 1999 (UCITA) en in de Uniform Electronic Transaction Act (UETA) – eveneens uit 1999 – is een softwareagent als volgt omschreven.

> "A computer program or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part, without review or action by an individual." (art. 1 UCITA)

Ook in deze definitie is *autonomie* een terugkerend element waarbij in de definitie zelf al kort een vingerwijzing wordt gegeven naar wat daar precies mee wordt bedoeld. Kenmerkend voor autonomie is in dit verband dat de handelingen door een computerprogramma worden verricht zonder menselijke tussenkomst. Hierin zit de belangrijkste onderscheiding met reguliere softwareprogramma's die steeds aangestuurd worden door menselijk handelen. Deze ietwat technische interpretatie wordt gebezigd binnen de AI en de Computer Sience en moet niet worden verward met het juridische concept van autonomie. Autonoom ziet in het recht in beginsel op de onafhankelijkheid van de menselijke wil en de grondwettelijke bevoegdheid om in vrijheid zelf beslissingen te kunnen nemen. Het gaat daarmee dus om het onderscheid tussen de technische capaciteit om autonoom te handelen en de juridische bevoegdheid tot autonoom handelen (Schermer e.a., 2005). Dit zijn elkaar versterkende factoren want hoe meer bevoegdheid er wordt overgedragen aan een softwareagent des te meer technische capaciteiten deze moet krijgen.

Het concept softwareagent zullen wij hierna verder verduidelijken aan de hand van de bespreking van vier onderscheidende eigenschappen die tevens inzicht geven in de (theoretische) mogelijkheden van softwareagenten. In subsectie 2.2.1 bespreken wij de eigenschap *autonomie*. Subsectie 2.2.2 handelt over de *reactiviteit* en *adaptief gedrag* waarna in subsectie 2.2.3 de eigenschap *communicatie* wordt behandeld.

2.2.1 Autonomie

Het begrip autonomie is hierboven reeds kort toegelicht. Daarbij hebben wij onderscheid gemaakt tussen technische autonomie en juridische autonomie. Wanneer wij in de context van softwareagenten spreken over autonomie zal steeds gedoeld worden op de technische vorm daarvan. Van autonome software kan worden gesproken wanneer er geen rechtstreeks menselijk handelen is vereist voor het uitvoeren van bepaalde functies door de software. Brazier e.a., (2003) wijzen erop dat er onderscheid kan worden gemaakt in de mate van autonomie en categoriseert drie typen softwareagenten.

Ten eerste onderscheiden Brazier e.a., de 'slaaf', waarmee zij een softwareagent aanduiden die voor iedere beslissing eerst de gebruiker zal raadplegen. De softwareagent kan daarenboven zelfstandig geen veranderingen aanbrengen in de rechtspositie van zijn gebruiker. In de context van de uitwisseling van politiegegevens gaat het bij het uitwisselen van informatie in beginsel niet om het rechtstreeks veranderen van de rechtspositie van de gebruiker, maar om het uitoefenen van een bevoegdheid. Wel kunnen ons inziens informatietransacties gevolgen hebben voor de rechtspositie van derden waarvoor de gebruiker dan primair verantwoordelijk is.

Ten tweede onderscheiden Brazier e.a. (2003) de 'vertegenwoordiger', waarmee zij doelen op het type softwareagent dat in een bepaald domein en binnen strikt aangegeven grenzen zelfstandig beslissingen kan nemen. In het kader van de uitwisseling van criminele inlichtingen kan dan gedacht worden aan een softwareagent die bij de afhandeling van informatieverzoeken uitsluitend op basis van de geregistreerde afhandelingscode bepaalt of informatie al dan niet kan worden verstrekt. Er is dan sprake van een beperkte autonomie.

Ten derde onderscheiden Brazier e.a. (2003) de 'vrije agent' waarmee zij doelen op het type softwareagent dat vrijelijk en volledig autonoom beslissingen kan nemen die de doelstelling van de gebruiker dienen. Terugkomend op het voorbeeld van de gegevensuitwisseling. Een vrije agent zal de afhandeling van een informatieverzoek volledig voor zijn rekening nemen zonder raadpleging van zijn gebruiker. Een autonome beslissing van een vrije agent in het proces van informatie-uitwisseling kan bijvoorbeeld gebaseerd zijn op een communicatieprotocol waarbij na uitwisseling van argumenten met de

informatieverzoeker al dan niet wordt besloten tot het honoreren van het informatieverzoek (zie Dijkstra e.a., 2007).

Het onderzoek binnen de AI naar de mogelijkheden van autonome besluitvorming door softwareagenten richt zich thans onder meer op het ontwikkelen van (communicatie)modellen en protocollen waarbij softwareagenten overeenstemming trachten te bereiken over meerdere geschilpunten (Lai, Sycara en Li, 2007). Daarnaast worden onderhandelingsstrategieën voor softwareagenten ontwikkeld om ook op basis van onvolledige informatie in een onderhandeling, gelet op de doelstelling van de softwareagent, een optimaal resultaat te behalen.

2.2.2 Reactiviteit en adaptief gedrag

Met reactiviteit wordt de eigenschap bedoeld dat softwareagenten door middel van sensoren direct reageren op een verandering in hun omgeving. Hoewel het bij reactiviteit in feite gaat om relatief eenvoudige toepassingen zoals het registeren van een lichtsensor die aangeeft dat het donker wordt, waarna er een signaal wordt afgegeven waarmee een lamp wordt aanzet, laat recent AI-onderzoek echter zien dat reactiviteit bij softwareagenten zich ook evolutionair kan ontwikkelen (Van Dartel, 2006). In zijn onderzoek laat Van Dartel aan de hand van eenvoudige experimenten zien dat een softwareagent door middel van een evolutionair proces oplossingen kan vinden die niet slechts te maken hebben met het 'brein' van de softwareagent maar voortvloeien uit de interactie van het brein met de omgeving. Van Dartel laat zien in welke richting de mogelijkheden van reactieve agenten ontwikkelen, aangenomen dat softwareagenten inderdaad steeds effectiever zullen kunnen omgaan met hun omgeving (dankzij *situation awareness*). Binnen de AI wordt deze vorm van reactiviteit ook wel aangeduid als adaptief gedrag of als *performance learning.* De kennis die met leren is opgedaan wordt opgeslagen in de interne staat van de softwareagent en gebruikt bij het uitvoeren van toekomstige taken. Het AI-onderzoek ziet zich in dit verband gesteld voor een nieuwe uitdaging: is het mogelijk dat *performance learning* ook wordt toegepast in multi-agentsystemen waarin dan individuele softwareagenten door middel van *case-based reasoning* technieken ook kunnen leren van de 'ervaring' van andere softwareagenten in het systeem? (Plaza en Ontañón, 2007).

2.2.3 Communicatie

Bij de eigenschap communicatie gaat het om het vermogen van een softwareprogramma om te communiceren met mensen en met andere softwareagenten. Om softwareagenten te laten communiceren is naast een gemeenschappelijke taal ook een gemeenschappelijk beeld van de werkelijkheid nodig. Bij de communicatie moeten de agenten elkaars berichten en omge-

ving begrijpen. Dit wordt ook wel de semantische interoperabiliteit genoemd. Het wordt tot stand gebracht door gebruik te maken van ontologieën. Een ontologie is in de AI een beschrijving van alle objecten, relaties en regels binnen een bepaald domein. Wanneer softwareagenten gebruik maken van dezelfde ontologie zullen zij hetzelfde beeld hebben van de instituties en regels binnen het domein waarin zij opereren. In combinatie met een gemeenschappelijke taal kan communicatie tussen softwareagenten onderling tot stand worden gebracht.

Binnen de AI wordt veel onderzoek gedaan naar methoden voor het ontwikkelen van adequate ontologieën voor verschillende domeinen. Recent onderzoek richt zich daarbij op het afleiden van een ontologie uit een andere ontologie. Wanneer dat eenmaal mogelijk is nemen, met name in open netwerkomgevingen (zoals Internet), ideeën over complexe taakuitvoeringen aanzienlijk toe. Sukthankar en Sycara (2007) doen in dit verband onderzoek naar de mogelijkheden dat softwareagenten elkaars '*policies*' herkennen en begrijpen. Deze ontwikkeling kan op termijn een doorbraak betekenen in het domein van de uitwisseling van politiegegevens. Wij verwachten dat de schaal waarop politiegegevens rechtstreeks geautomatiseerd gaan worden uitgewisseld, in de komende jaren zal toenemen. Daarbij signaleren wij dat er niet alleen op nationaal niveau elektronische uitwisseling van politiegegevens zal plaatsvinden met de ketenpartners van de politie, ook op internationaal niveau zal de behoefte aan grensoverschrijdende elektronische informatie-uitwisseling toenemen. Daarbij is het goed denkbaar dat ketenpartners en de buitenlandse politiediensten verschillende policies hebben ten aanzien van de uitwisseling van gegevens. Indien softwareagenten in staat zijn deze te herkennen en daar op adequate wijze op te anticiperen zal dat een belangrijke stap voorwaarts zijn in de mogelijkheden tot elektronische gegevensuitwisseling .

2.3 Multi-agentsystemen

Doorgaans worden (netwerk)omgevingen waarin meerdere softwareagenten werken aangeduid als een multi-agent systeem. In een multi-agent systeem kunnen verschillende softwareagenten werken aan de uitvoering van een gemeenschappelijke taak. Een gemeenschappelijke taak is in de context van het onderhavige onderzoek, de rechtmatige en efficiënte uitwisseling van informatie. Wij laten in hoofdstuk 6 zien dat deze taak, wat de uitwisseling van criminele inlichtingen betreft, kan worden ontleed in een aantal kleine deeltaken. In een multi-agent systeem dat ingezet wordt voor de uitwisseling van criminele inlichtingen zouden verschillende softwareagenten ieder een deeltaak van het totale proces van uitwisseling voor zijn rekening moeten nemen. In subsectie 2.4.1. bespreken wij in dit verband het fenomeen van emergent gedrag dat kan voorkomen in multi-agent systemen. In subsectie 2.4.2 geven wij een toelichting op normatieve multi-agent systemen.

2.3.1 Emergent gedrag

Evenals dit het geval is met het concept softwareagent, bestaat er binnen de AI evenmin overeenstemming over de precieze definiëring van *emergent gedrag*. Vrij algemeen wordt aangenomen dat het gaat om gedrag dat niet is toe te schrijven aan individuele softwareagenten maar de uitkomst is van de collectieve interactie tussen individuele agenten. Het is dan ook geen functionaliteit die voorgeprogrammeerd is in een multi-agent systeem. Dyson (1997) definieert het als volgt.

> "Emergent behavior is that which cannot be predicted through analysis at any level simpler than that of the system as a whole. (…) Emergent behavior, by definition, is what's left after everything else has been explained."

Uit deze definiëring wordt duidelijk dat het bij emergent gedrag gaat om de onverklaarbaarheid en de onvoorspelbaarheid ervan (Aldewereld 2007). Overigens zijn sommige onderzoekers van mening dat emergent gedrag niet bestaat (Li e.a., 2006). Zij menen dat gedrag waarvan de ontwerper en gebruiker de achterliggende regels of principes niet kennen ten onrechte wordt geclassificeerd als emergent gedrag. Volgens hen is dat onjuist en betekent het slechts dat er meer onderzoek naar moet worden gedaan. Wat daar ook van zij, vast staat dat emergent gedrag niet van te voren geprogrammeerd is. Dat kan tot gevolg hebben dat het systeem bepaalde onverwachte gedragingen gaat vertonen. Dergelijk onverwacht gedrag kan natuurlijk als een voordeel worden aangemerkt wanneer dit het functioneren van het systeem als geheel ten goede komt. Daar tegenover staat dat emergent gedrag mogelijk ook bepaalde negatieve gevolgen kan hebben voor het functioneren van het systeem. In de context van informatie-uitwisseling kan dat betekenen dat in het multi-agent systeem onverwachte verwerkingen en uitwisselingen plaatsvinden in strijd met de wettelijke regels. Juist de onvoorspelbaarheid of onverwachtheid van het gedrag kan een bezwaar zijn voor potentiële gebruikers van multi-agent systemen (Li e.a., 2006).

Wanneer wij deze eigenschap plaatsen in het licht van de uitwisseling van criminele inlichtingen dan wijzen wij erop dat juist de controle van de eigenaar over wat er met de gegevens gebeurt in de praktijk één van de belangrijkste factoren is bij de uitwisseling. Met name verantwoordelijke CIE-hoofden of plaatsvervangende hoofden achten het van groot belang dat zij grip houden op de informatie die zij uitzetten. Wanneer een multi-agent systeem de uitwisseling zal ondersteunen dan kan emergent gedrag ons inziens een onoverkomelijk bezwaar vormen. Vanzelfsprekend zijn deze bezwaren niet beperkt tot toepassingen binnen de politieorganisatie maar is het een breder probleem bij mogelijke toepassing van multi-agenttechnieken. Om die reden wordt er steeds meer onderzoek gedaan naar de wijze waarop emergent gedrag kan worden begrepen en gestuurd. Ook voor eventuele toepassingen

van multi-agenttechnieken in het politiedomein is dit onderzoek van groot belang. Wanneer emergent gedrag niet kan worden gecontroleerd zal er binnen de CIE onvoldoende vertrouwen zijn voor het inzetten van softwareagenten bij de informatie-uitwisseling. Uitwisseling van criminele inlichtingen gaat immers over privacy- en onderzoeksgevoelige informatie. Wanneer het systeem onvoorspelbare en oncontroleerbare verwerkingen uitvoert zal er bij voorbaat onvoldoende vertrouwen zijn om dergelijke technieken in te zetten bij de uitwisseling van criminele inlichtingen.

Binnen het ANITA-project is dit probleem geadresseerd en heeft met name Aldewereld (2007) zijn onderzoek gericht op de vraag hoe autonomie en daarmee samenhangend emergent gedrag toch zoveel mogelijk in overeenstemming met geldende normen kan worden gebracht. Daarmee wordt het onderzoekterrein van normatieve multi-agent systemen betreden. In subsectie 2.3.2 komen wij daarop terug.

2.3.2 Normatieve systemen

Normatieve systemen waren in het begin van de jaren zeventig vooral het domein van (rechts)filosofen. Algemeen worden Alchourron en Bulygin (1971) als grondleggers beschouwd omdat zij als eerste een poging deden om de deontische logica van Von Wright (1951) toe te passen op het recht. Kort gezegd stellen zij daartoe een logische taal voor die onderscheid maakt tussen 'properties' en 'actions' en die verder gebruik maakt van vier modaliteiten: (1) P: het is toegestaan dat, (2) O: het is verplicht dat, (3) Ph: het is verboden dat, en (4) F: het is mogelijk dat. Met deze logische taal staan zij aan de basis van het AI-onderzoek naar normatieve systemen. Meyer en Wieringa (1993) hebben daarop voortgeborduurd en de deontische logica geïntroduceerd bij de ontwikkeling van normatieve multi-agent systemen. Zij definiëren deze systemen als:

> "systems in the behavior of which norms play a role and which need normative concepts in order to be described or specified." (Meyer en Wieringa, 1993)

Daarnaast wijzen zij erop dat sinds de opkomst van de computer er in systeemspecificaties weinig aandacht was voor het onderscheid tussen normatieve gedragingen van een systeem (zoals het zou moeten) en de feitelijke gedragingen van het systeem (zoals het is). De oorzaak voor dit gebrek aan aandacht zou volgens hen te verklaren zijn uit het feit dat het veelal onmogelijk is om van te voren te specificeren dat bepaald gedrag van het systeem niet normconform (illegaal), maar wel mogelijk is. Vaak wordt illegaal gedrag in de specificatie uitgesloten wat niet weg neemt dat het desondanks van belang is dat systeemontwerpers in staat zijn om te specificeren wat er gebeurt wanneer dit illegale gedrag zich toch voordoet. Daar ligt ook de link met het controleren van emergent gedrag in multi-agentsystemen waarover

wij in de vorige subsectie schreven. De niet gespecificeerde maar mogelijke illegale gedragingen die Meyer en Wieringa benoemen kunnen worden geduid als illegaal emergent gedrag. Het onderzoek naar normatieve multi-agent systemen is zodoende voor een belangrijk deel gericht op het controleren van dat gedrag en ontwikkelen van normconcepten die bruikbaar zijn in multi-agent systemen. Jones en Carmo (2001) hebben in dat licht normatieve systemen gedefinieerd als:

> "Sets of agents whose interactions are norm-governed; the norms prescribe how the agents ideally should and should not behave."

Het gaat er in normatieve multi-agent systemen met andere woorden om (1) het aanbrengen van de beperkingen in het gedrag van de softwareagenten en (2) het onder controle houden van (illegaal) emergent gedrag. Recent onderzoek binnen de AI richt zich daarbij met name op de mogelijkheden om *non-compliance* gedrag van softwareagenten in netwerkomgevingen te beperken. Aldewereld (2007 stelt daartoe een systeem voor waarbij een soort van strafpunten worden uitgedeeld aan softwareagentne die illegaal of ongewenst gedrag vertonen. Agotnes, Van der Hoek en Wooldridge (2008) wijzen erop dat dit systeem echter in open netwerkomgevingen, zoals Internet, niet voldoende adequaat zal kunnen werken in verband met de beperkingen die nationale grenzen met zich meebrengen. Zij richten zich in hun onderzoek op methoden om de robuustheid van multi-agentsystemen te vergroten. Uiteindelijk zal dat moeten leiden tot het vergroten van de betrouwbaarheid van normatieve multi-agentsystemen.

In ons onderzoek vormt het in hoofdstuk 3 te bespreken juridisch kader het aanknopingspunt voor het bepalen van de systeemnormen. Binnen het ANITA-project zijn door drie AI-onderzoekers voorstellen gedaan om juridische normen te vertalen naar normatieve systeemspecificaties. Wij zullen hun onderzoeksresultaten en voorstellen in de volgende sectie bespreken.

2.4 Resultaten ANITA-project

Het ANITA-project is in 2002 gestart om na te gaan hoe (normatieve) multi-agent technieken bruikbaar zijn in het domein van de uitwisseling van politiegevens. Binnen het project is samengewerkt door onderzoekers met een achtergrond in de artificiele intelligentie en onderzoekers met een juridische achtergrond. In deze sectie bespreken wij de resulaten die het AI-onderzoek binnen het ANITA-project heeft opgeleverd. Vervolgens zullen wij in hoofdstuk 6 aan de hand van een aantal conceptuele toepassingen laten zien hoe deze resultaten kunnen bijdragen aan een oplossingsrichting voor de knelpunten die wij in hoofdstuk 5 hebben geïnventariseerd. In deze sectie behandelen wij achtereenvolgens de onderzoeksresultaten van Teepe (subsectie 2.4.1), Aldewereld (subsectie 2.4.2) en Dijkstra (subsectie 2.4.3).

2.4.1 Teepe

Het onderzoek van Teepe (2006) richt zich op het spanningveld dat bestaat tussen het geheim houden van persoonsgegevens in het belang van de privacy enerzijds en het uitwisselen van deze gegevens in het belang van de opsporing anderzijds. Het uitwisselen van gegevens lijkt zich op het eerste gezicht niet te verenigen met het geheimhouden daarvan. In zijn proefschrift introduceert Teepe twee technische oplossingen die kunnen worden toegepast in elektronische omgevingen waarbij er (1) een nadrukkelijke behoefte is tot uitwisselen van informatie terwijl er (2) ook goede argumenten zijn om bepaalde informatie juist geheim te houden. De oplossingen die hij aandraagt zijn (1) de *information designator* en (2) de *knowledge authentication protocols*. Wij bespreken beide oplossingen op hoofdlijnen en gaan vervolgens in hoofdstuk 6 na (1) waar deze kunnen worden toegepast in het domein van de uitwisseling van criminele inlichtingen en (2) in welke knelpunten ze bijdragen aan een oplossing. Voor een uitgebreide technische beschrijving van de beide oplossingen verwijzen wij naar het proefschrift van Teepe (2006).

Information designator
De 'information designator' kan het beste worden gezien als een stukje informatie dat uitsluitend tot doel heeft te verwijzen naar andere informatie zonder dat het die andere informatie bevat en zonder dat er enige referentie naar een context van die ander informatie wordt gemaakt. De *designator* is met andere woorden een soort metadata, gerelateerd aan bijvoorbeeld de nawgegevens van persoon X zonder dat op enige manier uit die metadata zelf blijkt dat het gaat om persoon X.

In het voorstel van Teepe wordt iedere *designator* vervolgens voorzien van een adres zodat het mogelijk is voor een softwareagent, de zogenaamde *exchange agent,* om contact te leggen met de *designator* en vervolgens de *designator* te vertalen naar de informatie waarnaar deze verwijst. De exchange agent kan dan zo worden geprogrammeerd dat deze in bepaalde gevallen beperkingen en/of voorwaarden kan stellen aan de informatieverzoeker alvorens de *designator* wordt vertaald en de informatie dus wordt prijsgegeven. Het proces van uitwisselen met behulp van de *information designator* kent derhalve twee stappen.

(1) Het informatieverzoek formuleren. In deze stap wordt bijvoorbeeld door X, na een inlogprocedure, de adresgegevens van Y opgevraagd. Door Y wordt vervolgens de *information designator* van zijn adresgegevens verstrekt aan X. Feitelijk heeft X daarmee nog niet de adresgegevens van Y maar slechts een aanduiding van niet rechtstreeks indentificeerbare metadata die daarnaar verwijst. In deze fase van de informatie-uitwisseling heeft Y nog de volledige controle over de informatie. Dit betekent dat de adresgegevens bijvoorbeeld nog gewijzigd kunnen worden, maar ook dat Y nog kan besluiten om de verstrekking van de informatie in te trekken.

(2) De informatie materialiseren. In deze stap moet X de *exchange agent* van Y benaderen om de *information designator* te vertalen. Wanneer Y de verstrekking niet heeft ingetrokken en X akkoord gaat met de voorwaarden die de *exchange agent* stelt, dan verkrijgt X deze gegevens.

Het gebruik van *information designators* biedt zowel de informatiegebruikers als informatieverstrekker volgens Teepe vier belangrijke voordelen. (1) De gebruikers hebben in beginsel toegang tot de informatie die zij nodig hebben zonder dat die informatie door hen moet worden beheerd. Het beheer blijft bij de informatieverstrekker en dat heeft voor de verstrekker tot voordeel dat hij in hoge mate controle houdt over de informatie. (2) Bovendien kunnen met deze toepassing via de *exchange agent* beperkingen en eventuele voorwaarden voor verstrekking nauwkeuriger worden afgestemd dan mogelijk is via doorsnee autorisatiesystemen. (3) Ook de mogelijkheid om na verstrekking van de *information designator*, alsnog het daadwerkelijk verstrekken van de achterliggende informatie in te trekken is een functionaliteit waarvan Teepe verwacht dat bij informatieverwerkende organisaties daaraan veel behoefte is. (4) Tenslotte is het met de toepassing van *information designators* in de informatie-uitwisseling niet meer noodzakelijk dat de verschillende organisaties gebruik maken van dezelfde ontologie. Verschillende organisaties kunnen tegelijkertijd informatie verspreiden waarbij ieder gebruik maakt van zijn eigen ontologie.

> "Different organizations provide information under their own, simultaneously provided ontology. If this information is used, the provided ontology will be used. If this information is related to information from some other ontology, it will be related by means of a designator in the one ontology, pointing to the information in the other ontology. Technically this means that instead of multiple information sources storing identical information, there is one information source that stores the original information, while other information sources store references (information designators)." (Teepe, 2006, p. 89)

Op die manier functioneren de *information designators* als een soort lijm tussen de verschillende ontologieën van informatiesystemen en onderliggende databases waardoor deze ondanks het feit dat zij naast elkaar bestaan toch een geïntegreerd geheel kunnen vormen. Teepe wijst daarnaast op het voordeel dat deze toepassing de kans op inconsistenties van informatie van een geregistreerd subject verkleint om de eenvoudige reden dat die informatie niet telkens opnieuw in een andere database wordt geregistreerd maar dat slechts de *designators* worden geregistreerd. Bovendien levert het een betere bescherming van de privacy van geregistreerden op doordat informatie via de *designator* kan worden gekoppeld zonder dat de achterliggende informatie die normaal gesproken nodig is voor een koppeling, wordt prijsgegeven.

Knowledge authentication protocols

De tweede oplossing die Teepe in zijn proefschrift voorstelt betreffen twee *knowledge authentication protocols.* In eenvoudig Nederlands kan dit het beste

worden omschreven als een protocol waarmee de gebruiker in staat wordt gesteld om een geheim te delen met een persoon die het geheim mogelijk ook kent, maar zonder dat hij het geheim vooraf prijs behoeft te geven. Daarbij werkt Teepe twee varianten uit.

De eerste variant is het '1-to-many' probleem waarbij één geheim wordt vergeleken met vele geheimen. Hiervoor ontwikkelt hij het T1-protocol waarbij crypografische hashfuncties worden gebruikt waarmee als het ware een vingerafdruk kan worden gemaakt van een blok gegevens. Daarmee wordt het blok gegevens weliswaar uniek identificeerbaar maar wordt er niets prijsgegeven over de achterliggende gegevens.

De tweede variant is het *many-to-many* probleem waarbij vele geheimen worden vergeleken met vele geheimen. Om dit probleem aan te pakken optimaliseert Teepe kort gezegd het T1-protocol naar een T2-protocol dat dan in feite bestaat uit een groep parallel draaiende T1-protocollen. Hierdoor wordt het mogelijk om de informatie op twee lijsten met elkaar te vergelijken zonder dat bekend wordt wat er buiten het overlappende gedeelte van deze lijsten zit.

Beide protocollen kunnen gebruikt worden in situaties waarbij er twee partijen op de hoogte zijn van hetzelfde geheim, maar pas met elkaar informatie daarover willen uitwisselen wanneer beide partijen van elkaar weten dat zij hetzelfde geheim kennen. Vanuit het perspectief van de privacybescherming laat Teepe zien dat met behulp van de protocollen heel gericht persoonsgegevens kunnen worden uitgewisseld, namelijk slechts tussen belanghebbende gebruikers. De toepassing van de protocollen gaat ervan uit dat de belanghebbende gebruikers zelf al enige informatie bezitten over het subject waarover zij informatie gaan uitwisselen. Daarnaast zorgt de toepassing van crytografische hashfuncties ervoor dat er binnen computernetwerken berichten kunnen worden gecommuniceerd over persoonsgegevens zonder dat het nodig is deze persoonsgegevens zelf te communiceren. Met name bij het koppelen van gedistribueerde databestanden levert dat een aanmerkelijk privacyvoordeel op. Voor het vaststellen van overlappingen is het immers niet nodig alle persoonsgegevens uit de verschillende databestanden met elkaar te vergelijken, maar slechts de digitale 'vingerafdrukken'. Na een vergelijking kunnen gericht de persoonsgegevens van de overlappende vingerafdrukken worden uitgewisseld. De niet-overlappende gedeelten van de geregistreerde gegevens blijven zodoende geheim.

2.4.2 Aldewereld

Binnen het ANITA-project heeft Aldewereld (2007) zich in zijn onderzoek geconcentreerd op het spanningsveld dat bij de toepassing van multi-agent systemen bestaat, tussen enerzijds de mate waarin softwareagenten auto-

noom handelen en anderzijds de behoefte om het gedrag van softwareagenten te conformeren aan de geldende normen in het domein. Daarbij maakt hij nadrukkelijk onderscheid tussen normen op lokaal niveau en normen op globaal niveau. Lokale normen zijn procedures en protocollen die op de lokale informatietransacties van toepassing zijn. In het domein van de uitwisseling van criminele inlichtingen gaat het dan om de normen, uitgewerkt in lokale protocollen, die een regionale CIE toepast bij de uitwisseling van informatie. Daarbij gaat Aldewereld ervan uit dat deze protocollen op regionaal niveau zijn ontwikkeld en ook per politieregio kunnen verschillen. Dit heeft tot gevolg dat er behoefte bestaat aan het controleren van die lokale protocollen op globale rechtmatigheid. Daarmee wordt bedoeld dat lokale regelingen getoetst dienen te worden aan het van toepassing zijnde wettelijk kader. Dit maakt dat er behoefte is aan een systeem dat de individuele informatietransacties controleert.

In de gangbare methoden voor de ontwikkeling van softwareagenten worden reguleringen als deel van de softwareagenten geprogrammeerd. Er ontstaat echter een probleem wanneer de regelingen in het domein veranderen. Omdat de normen geïntegreerd zijn in de code en het ontwerp van de agents, moeten bij verandering van regelgeving alle verschillende ontwerpstappen bekeken worden en alle codes moeten worden gecontroleerd op overeenstemming met de nieuwe regelgeving. In grote informatiesystemen zoals die gebruikt wordt in het politiedomein is dat een zeer kostbare en tijdrovende taak. Aldewereld stelt een alternatief voor waarbij een expliciete representatie wordt gemaakt van de normen. Het wordt daarmee eenvoudiger om veranderingen in de regelgeving te implementeren in het systeem, maar zo stelt hij, daarvoor is wel een andere aanpak van normhandhaving vereist.

De andere aanpak vindt Aldewereld in de introductie van de elektronische institutie. Een elektronische institutie is een entiteit waarbinnen een verzameling normen en protocollen wordt gedefinieerd die het gedrag van de individuele softwareagenten binnen de institutie beschrijven. Het inzetten van elektronische instituties in een multi-agentsysteem heeft vier voordelen (Aldewereld, 2007, p. 23):

(1) de onzekerheid over andere participanten in het systeem wordt verkleind;
(2) er zijn minder misverstanden tussen de participanten omdat zij dezelfde normen delen;
(3) voorzienbare uitkomsten van de interacties tussen participanten;
(4) een vereenvoudiging van het beslissingsproces van individuele agenten omdat door de normen het aantal mogelijke acties drastisch wordt verkleind.

De normen en protocollen voor de elektronische institutie worden afgeleid uit de wetten en reguleringen die voor het domein van de criminele inlichtingen gelden (zie hoofdstuk 3). Om vervolgens te bereiken dat de softwareagenten in het multi-agent systeem zich ook conform deze normen gedragen is een vorm van normhandhaving noodzakelijk. En juist daar treedt het spanningsveld tussen autonomie en conformiteit op. Voor de handhaving kan gekozen worden uit twee handhavingsystemen.

Ten eerste kan het gedrag van de softwareagenten worden beperkt door specifieke procedures. Wanneer dan vooraf wordt gecontroleerd of deze procedures binnen de wettelijke normen blijven is het zeker dat de informatietransacties die deze softwareagenten verrichten conform de wet- en regelgeving geschiedt. Er is in die benadering nauwelijks sprake van autonomie en het is in hoge mate voorspelbaar hoe het systeem zal handelen. Dit betekent tevens dat emergent gedrag nauwelijks zal voorkomen in deze systemen en daarmee samenhangend dat softwareagenten niet in staat zijn om op onvoorziene situaties te reageren. Zij zitten als het ware vast in hun vooraf bedachte procedures.

Ten tweede kan het gedrag van softwareagenten gecontroleerd worden door het toedienen van 'straffen' ingeval er een norm wordt overtreden. De autonomie van softwareagenten blijft dan bewaard. Deze autonomie wordt slechts ingeperkt wanneer er daadwerkelijk normen worden overtreden.

Het tweede handhavingsysteem is een nieuwe benadering voor de ontwikkeling van normatieve multi-agent systemen. Het vraagt binnen een elektronische institutie om een actief systeem dat is gebaseerd op het detecteren en reageren op overtredingen. Het belangrijkste probleem dat Aldewereld bij het ontwerpen van zowel het eerste als het tweede handhavingsystemen ondervond betrof de in ons onderzoek geconstateerde abstractheid van de wet- en regelgeving in het domein van de politiële gegevensverwerking (zie hoofdstuk 3). Er bestaat een grote kloof tussen de abstracte en vage normen in de wetgeving en de concrete protocollen en procedures waarmee softwareagenten in de praktijk moeten werken. Om deze kloof te overbruggen introduceert Aldewereld een methode waarmee abstracte normen kunnen worden vertaald in concrete protocollen voor softwareagenten. Hij maakt daarbij gebruik van een tussenliggende vertaalslag die hij aanduidt met *landmarks* waarmee hij de belangrijkste stappen bedoelt die elk protocol zou moeten bevatten. Deze methode is afgeleid van de wijze waarop ook in de praktijk wetten worden vertaald naar procedures. In zijn proefschrift stelt Aldewereld uiteindelijk een *conceptual framework* voor waarin beide handhavingsystemen worden geïntroduceerd die beide gebruik maken van op deze wijze ontworpen protocollen. Daarmee stelt hij uiteindelijk een goede balans te hebben gevonden tussen autonomie en conformiteit in een normatief multi-agent systeem.

2.4.3 Dijkstra

In het ANITA-project heeft Dijkstra (2006, 2007) zijn onderzoek gericht op de mogelijkheden om gereguleerde uitwisseling van informatie mogelijk te maken via onderhandelingsprotocollen tussen softwareagenten. Deze invalshoek sluit nauw aan bij de CIE-praktijk waarbij politieambtenaren van verschillende regio's met elkaar telefonisch onderhandelen over de vraag of bepaalde informatie kan worden uitgewisseld en zo ja, onder welke voorwaarden. Dijkstra (2007) gaat in zijn publicaties uit van softwareagenten die deze CIE-ambtenaren uit de praktijk vertegenwoordigen. De bevoegdheid van een individuele CIE-ambtenaar om een informatieverzoek af te handelen, wordt in zijn voorstel gedelegeerd aan een softwareagent. Om een softwareagent dergelijke informatieonderhandelingen te laten uitvoeren zijn volgens Dijkstra drie competenties nodig.

Ten eerste dient de softwareagent te beschikken over drie soorten kennis: (1) kennis van de relevante regels in het domein, (2) kennis van het doel dat de softwareagent met zijn taakuitvoering nastreeft, en (3) kennis over de consequenties van zijn acties.

Ten tweede moet de softwareagent in staat zijn te redeneren. Dat wil zeggen dat de softwareagent in staat moet zijn om zelf argumenten te genereren en tegenargumenten te evalueren. Redeneren houdt verder in dat de agent zijn eigen overtuiging (belief) moet kunnen herzien op basis van de gevoerde dialoog. Tenslotte stelt Dijkstra dat redeneren inhoudt dat de softwareagent (om in staat te zijn om met voorwaarden belaste voorstellen te genereren) ook in bepaalde mate hypothetisch moet kunnen redeneren. Met dat laatste wordt bedoeld dat de softwareagent tot op zekere hoogte moet kunnen voorzien wat de consequenties zijn van de voorstellen die hij tijdens een argumentatiedialoog doet.

Ten derde is voor het voeren van een argumentatiedialoog communicatie als competentie vereist. De communicatie in het domein van de uitwisseling van criminele inlichtingen is gericht op twee elementen (1) onderhandeling en (2) verankerde overtuiging. De onderhandeling met betrekking tot de uitwisseling van informatie vindt plaats over de voorwaarden waaronder kan worden uitgewisseld en de overtuiging vindt plaats wanneer een softwareagent de andere softwareagent ervan probeert te overtuigen dat bijvoorbeeld een weigering om te voldoen aan een informatie verzoek onrechtmatig is.

Dijkstra (2006, 2007) werkt deze drie competenties op onderdelen verder uit en doet op conceptueel niveau een voorstel voor een transactie-agent die hij onder meer voorziet van een communicatieprotocol waarin zowel de onderhandeling over voorwaarden, als de verankerde overtuiging is geïmplemen-

teerd. Vervolgens laat hij aan de hand van een voorbeeld zien hoe met behulp van deze transactieagent een informatieverzoek rechtmatig kan worden afgehandeld. Het rechtmatige gedrag van de softwareagent zit daarbij geïmplementeerd in de verschillende regels, argumenten en overtuigingen en vloeit daarmee voort uit de onderhandeling.

2.5 Beantwoording eerste onderzoeksvraag

In dit hoofdstuk hebben we de mogelijkheden van multi-agenttechnieken aangegeven door (1) enkele algemene trends binnen de artificiële intelligentie te schetsen en de toekomstverwachtingen van een vooraanstaand informaticus (Kurzweil 2005) aan een nader onderzoek te onderwerpen (2) drie eigenschappen van softwareagenten nader te onderzoeken, en (3) normatieve multi-agent systemen te onderzoeken.

Ad 1) De algemene trends laten zien hoe artificiële intelligentie zich de laatste jaren heeft ontwikkeld en waar intelligente (software) systemen toe in staat zijn. Wij hebben daarnaast de recente voorspellingen van Kurzweil onderzocht en komen tot de conclusie dat het bereiken van het door hem onderscheiden *singularity point* vergaande consequenties zal hebben voor de wijze waarop in de toekomst zal worden omgegaan met informatiesystemen in de politieorganisatie. Op het moment dat computers intelligenter worden dan mensen en daarom betere beslissingen kunnen nemen zullen in het politiedomein alle geautomatiseerde informatietransacties worden afgehandeld door softwareagenten. Wij menen dat serieus rekening zal moeten worden gehouden met de voorspelling van Kurzweil (2007) dat het singularity point, waarbij de computer intelligenter is dan de mens, in deze eeuw zal worden bereikt (mogelijk zelfs in 2030 zoals Kurzweil zegt). Dat roept nieuwe (juridische) vraagstukken ten aanzien van de verantwoordelijkheid, de controle van emergent gedrag, de rol van de individuele politieambtenaar, en de positie van geregistreerde. In hoofdstuk 6 zullen wij nader ingaan op deze vraagstukken.

Ad 2) Voor juristen blijkt uit het literatuuronderzoek naar de eigenschappen van softwareagenten dat er binnen de AI geen eenduidigheid bestaat over de precieze definiëring van de mogelijkheden. Voor informatici ligt dat per specialisme verschillend. Niettemin bemoeilijkt deze uitkomst ons bij de beantwoording van de eerste onderzoeksvraag. Het is voor juristen niet altijd duidelijk waar het precies over gaat. Wij komen echter wel tot de conclusie dat de onderzochte eigenschappen (autonomie, reactief en adaptief gedrag, en communicatie) veelbelovende mogelijkheden lijken te bieden voor toepassing in het domein van de informatietransacties in zijn algemeenheid en de uitwisseling van politiegegevens in het bijzonder.

Ad 3) Vervolgens zijn wij nagegaan wat de mogelijkheden van normatieve multi-agent systemen zijn. Wij verwachten dat een van de eigenschappen van de toepassing van multi-agent technieken, het emergent gedrag, juist in het politiedomein als onwenselijk zal worden beschouwd. Met name in het CIE-domein wordt het controleren van informatiestromen zeer belangrijk gevonden en het mogelijk emergent gedrag binnen informatiesystemen staat op gespannen voet met deze controlebehoefte. Wij hebben daarnaast de resultaten besproken van de AI-deelonderzoeken die binnen het ANITA-project zijn verricht. Ons onderzoek naar multi-agent technieken heeft zich specifiek gericht op het domein van de politiële informatie-uitwisseling en laat zien dat er verschillende softwareagenttoepassingen mogelijk zijn die bruikbaar kunnen zijn in het politiedomein. In het bijzonder noemen wij de toepassingen die zijn gericht op het controleren van illegaal emergent gedrag en het vergroten van de robuustheid van normatieve multi-agent systemen.

3 Het Juridisch kader

In dit hoofdstuk beschrijven wij het juridisch kader voor de uitwisseling van politiële gegevens. Wij beogen daarmee een antwoord te geven op de tweede onderzoeksvraag (OV 2): op welke wijze heeft de wetgever de uitwisseling van criminele inlichtingen genormeerd? Het juridisch kader vormt in dit onderzoek het uitgangspunt voor de beoordeling van de huidige praktijk van informatie-uitwisseling.

In sectie 3.1 bespreken wij de historische achtergrond van de wet- en regelgeving. Sectie 3.2 geeft een beknopte beschrijving van het internationale juridische kader. In de secties 3.3 tot en met 3.6 behandelen wij de nationale normen die zien op de opslag en uitwisseling van gegevens: politieregister, beheer, en doel (in 3.3), algemene opnamecriteria en gevoelige gegevens (in 3.4), bijzondere opnamecriteria (in 3.5), en verstrekkingsbepalingen (in 3.6). Gedurende het onderzoek heeft de wetgever voorstellen gedaan om het wettelijke kader te wijzigen. Uiteindelijk is tijdens de onderzoeksperiode de Wpolr vervangen door de Wpolg die per 1 januari 2008 in werking is getreden. Wij zullen bij de behandeling van het juridisch kader dan ook uitgaan van de Wpolg. Desondanks achten wij het van belang om ook enkele begrippen en normen uit de Wpolr te bespreken. De politieorganisatie en meer specifiek, de CIE, waren immers wat de informatiesystemen en bedrijfsprocessen in de onderzoeksperiode betreft nog volledig ingericht op de Wpolr. In sectie 3.7. geven wij samenvattend een overzicht van de belangrijkste verschillen tussen de nieuwe en de oude wet. Ten slotte formuleren wij in sectie 3.8 een antwoord op de tweede onderzoeksvraag, OV 2.

3.1 Historische achtergrond

De historische ontwikkeling van het juridische kader valt uiteen in drie perioden. Iedere periode kenmerkt zich door een duidelijke verandering in de rechtsontwikkeling. In subsectie 3.1.1 behandelen wij de periode van 1955-1970, daarna in subsectie 3.1.2 de periode 1971-1991, en tenslotte in subsectie 3.1.3 de periode 1992- tot heden.

3.1.1 Periode van 1955 tot 1970

De eerste wettelijke regels betreffende de registratie van politiële informatie dateren van 1955. In die periode groeide het inzicht dat persoonsgegevens die aan politie en justitie gerelateerd waren in geval van openbaarmaking,

de belangen van de betrokken personen ernstig zouden kunnen schaden. In de toenmalige Wet op de Justitiële Documentatie[30] (hierna: Wet JD) werden daarom (1) gedetailleerde regels opgenomen die de soort gegevens normeerden en (2) beperkingen aangelegd ten aanzien van de groep van gebruikers. Verder kende deze wet een onderscheid tussen twee soorten registers: de strafregisters en de algemene documentatieregisters. De opgeslagen informatie bevatte hoofdzakelijk strafrechtelijke gegevens over personen.[31] Het beheer was in handen van de Justitiële Documentatiedienst die overigens organisatorisch los stond van de politieorganisatie.

De politie maakte in die periode gebruik van eigen registraties die niet onder het bereik van de Wet JD waren gebracht. Dat was vreemd omdat het merendeel van de gegevens zowel in de justitiële registers als in de politieregistraties was opgeslagen. Tijdens de parlementaire behandeling van de Wet JD in het begin van de jaren vijftig, is deze opmerkelijke situatie aan de orde gesteld. Het beperkte bereik van de wet maakte het immers mogelijk dat veel opgeslagen informatie via de politieregistraties aan iedere willekeurige derde kon worden verstrekt. De toenmalige regering achtte het echter niet nodig het bereik van de Wet JD te verruimen of een apart wettelijk regime in het leven te roepen voor de politieregisters. Wel werd er een circulaire uitgebracht waarin bepalingen stonden opgenomen met betrekking tot de verstrekking van politiële informatie.[32] Deze situatie duurde tot 1970.

3.1.2 Periode van 1971 tot 1991

In het begin van de jaren zeventig ontstond er maatschappelijke onrust omtrent de registratie van personen die mede veroorzaakt werd door de opkomst van de computertechnologie. Met behulp van daarvan werd het mogelijk om grote hoeveelheden persoonsgegevens op te slaan en te verwerken. Er werd gevreesd voor een steeds verder toenemende controle van de overheid op het leven van individuele burgers. Deze maatschappelijke onrust mondde uiteindelijk uit in een massaal verzet tegen de volkstelling van 1971 die sindsdien overigens ook nooit meer gehouden is (Kuitenbrouwer, 1991).

Naar aanleiding van deze onrust stelde de regering een commissie in – de Staatscommissie Koopmans – die de opdracht kreeg onderzoek te doen naar de mogelijkheden om de verwerking van persoonsgegevens te reguleren via een wettelijke regeling. Het doel van een dergelijke regeling was gelegen in

30 Wet van 15 augustus 1955, Stb. 395, houdende vaststelling van de Wet op de Justitiële Documentatie en op de verklaringen omtrent het gedrag.
31 In dit verband wordt vaak gesproken van (strafrechtelijke) antecedenten.
32 De circulaire is opgenomen in het Algemeen Politieblad van 14 februari 1959.

het beschermen van de persoonlijke levenssfeer. De Staatscommissie Koopmans kwam tot de conclusie dat het onvermijdelijk is dat individuele burgers in een aantal gevallen het nadeel moeten dulden dat verbonden is aan een bepaalde beeldvorming als gevolg van de registratie van persoonsgegevens.[33] In de benadering van de commissie wordt het privacyrecht beschouwd als een relatief recht dat steeds moet worden afgewogen tegen andere maatschappelijke belangen.[34] Een afweging die in belangrijke mate wordt bepaald door de maatschappelijke omstandigheden van dat moment en die daarom ook kan veranderen in de tijd. In haar eindrapportage had de commissie tevens een voorontwerp opgenomen van de Wet op de Persoonsregistraties die ook zou moeten gaan gelden voor de politieregisters. In 1981 werd dit voorontwerp als wetsvoorstel aan de Tweede Kamer gestuurd. In datzelfde jaar werd overigens in Straatsburg ook het Europese Dataverdrag getekend waarin de kaders werden neergelegd voor de nationale wetgeving met betrekking tot de registratie van persoonsgegevens.[35]

Deze nationale en internationale ontwikkelingen hebben er uiteindelijk toe geleid dat in 1983 het recht op de bescherming van de persoonlijke levenssfeer werd neergelegd als grondrecht in art. 10 van de Grondwet. Het tweede lid van dit artikel bepaalt dat bij formele wet regels worden gesteld ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens. De Wet Persoonsregistraties[36] (hierna: WPR) is daarvan de formeel-wettelijke uitwerking. Evenals de Wet JD werd de WPR echter niet van toepassing verklaard op de politieregisters. Daarvoor werd een aparte wettelijke regeling ontworpen.[37] Gedurende de parlementaire behandeling van dit wetsvoorstel voor de regulering van politieregisters formuleerde de Raad van Europa aanbevelingen met betrekking tot het gebruik van persoonsgegevens door politiële autoriteiten.[38] Het vastleggen van regels met betrekking tot de registratie van persoonsgegevens door de politie in een formele wet, vormde een belangrijk onderdeel van deze aanbevelingen. Uiteindelijk werd in 1990 de Wet Politieregisters (Wpolr)

---

33 Staatscommissie Koopmans, 'Eindrapport van de Staatscommissie bescherming persoonlijke levenssfeer in verband met persoonsregistratie' Den Haag 1976.

34 Staatscommissie Koopmans, 'Eindrapport van de Staatscommissie bescherming persoonlijke levenssfeer in verband met persoonsregistratie' Den Haag 1976, p. 22.

35 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, 28 januari 1981, *Trb.* 1988, 7. Dit verdrag is negen jaar later voor Nederland geratificeerd bij Wet van 20 juni 1990 (*Stb*. 1990, 351).

36 De wet treedt in werking in 1988, *Stb*. 665. In 2001 is de WPR vervangen door de Wet bescherming persoonsgegevens (hierna: Wbp) vanwege de Europese harmonisatie van de privacywetgeving, Stb. 2001, 180. In art. 2 lid 2 sub c Wbp wordt bepaald dat ook deze nieuwe wet niet van toepassing is op persoonsgegevens die door de politie worden geregistreerd bij de uitvoering van de politietaak.

37 Het Wetsvoorstel Regels ter bescherming van de persoonlijke levenssfeer in verband met politieregisters.

38 Recommendation Regulating the Use of Personal Data in the Police Sector, R(87)15.

gepubliceerd in het Staatsblad en niet lang daarna ook het uitvoeringsbesluit, dat de naam het Besluit Politieregisters (Bpolr) kreeg. Beide traden op 17 februari 1991 in werking.

De wetgever heeft met de invoering van deze wet de aanbeveling van de commissie Koopmans om de WPR ook van toepassing te laten zijn op de politieregisters niet overgenomen. Zij beoogde met de Wpolr de verwerking van informatie strakker te reguleren en daarmee aanzienlijk minder wettelijke ruimte te laten voor zelfregulering. De ruimte wordt vooral ingeperkt ten aanzien van de opslagbepalingen en de mogelijkheden tot informatieuitwisseling. Voor de keuze voor een aparte wet zijn destijds vier redenen aangevoerd. Deze redenen zijn nog altijd actueel omdat zij aangeven waarin de verwerking van politiegegevens zich onderscheidt van niet-politiële registraties. Het gaat kort samengevat om de volgende redenen.

1. "Politieregistraties bevatten gegevens die de betreffende persoon niet vrijwillig heeft geleverd, of zelfs niet van hem afkomstig zijn;
2. het gaat in veel gevallen om gegevens met een gevoelig karakter; dat maakt het ook wenselijk dat bij formele wet wordt vastgelegd wie verantwoordelijk is voor het beheer van deze politieregisters;
3. de politie vervult een bijzondere rol in de verhouding tussen de overheid en de burger omdat de politie meestal pas in beeld komt wanneer deze verhouding is verstoord;
4. tussen de verschillende politiële instanties wordt een vergaande noodzaak tot uitwisseling van informatie gevoeld waardoor er behoefte kan ontstaan aan het koppelen van verschillende gegevensverzamelingen; juist aan de (nieuwe) informatie die kan voortvloeien uit deze koppelingen kunnen gevaren kleven voor de persoonlijke levenssfeer."[39]

Met de Wpolr beoogde de wetgever structuur aan te brengen in een tamelijk diffuse en ongenormeerde praktijk van registraties en uitwisseling van informatie. In deze periode maakte niemand zich echt druk over de ontstane verwerkingspraktijk, dat kwam pas enkele jaren later met de IRT-affaire.

3.1.3 Periode van 1992 tot heden

In het begin van de jaren negentig ontstond er ophef rondom de opsporingsmethoden die werden gehanteerd door het Interregionaal Recherche Team (IRT) Noord Holland-Utrecht. Dit leidde in 1994 tot parlementaire bemoeienis die uitmondde in de instelling van de Bijzondere Onderzoekscommissie IRT. Het rapport van deze commissie vormde uiteindelijk de aanleiding voor een parlementaire enquête.[40] De enquête-commissie, genoemd naar haar voorzitter Maarten van Traa, kreeg de opdracht om (1) de organisatie van de

39 *Kamerstukken II* 1994/95, 23 945, nr. 2.
40 *Kamerstukken II* 1994/95, 23 945, nr. 2.

opsporing te onderzoeken en (2) het functioneren van de controle. De politiele informatievoorziening vormde aanvankelijk geen onderwerp van discussie. Toen evenwel kwam vast te staan dat een aantal problemen in de opsporing teruggevoerd kon worden op de informatievoorziening, werd dat alsnog een derde punt van onderzoek. De commissie concludeerde dat de regelgeving voor de informatievoorziening ondoorzichtig was, omdat op bepaalde registers het regime van de Wpolr van toepassing was, terwijl op andere registers de algemene regels uit de Wet Persoonsregistraties van toepassing waren. Daarnaast achtte zij de criteria voor registratie van zogenaamde CID-subjecten (CID staat voor Criminele inlichtingendienst, thans CIE) te ruim. CID-subjecten waren personen die veelal voordat zij officieel als verdachte konden worden aangemerkt in de zin van art. 27 Sv, onderwerp waren van CID-onderzoek. De criteria hadden volgens de Commissie Van Traa geleid tot een spectaculaire toename van persoonsregistraties in de CID-registers waarbij men zich sterk afvroeg of deze wel terecht waren.[41] Tenslotte bleek dat een groot deel van de verstrekkingen van gegevens uit de registers voornamelijk mondeling werd gedaan zonder dat daarop achteraf controle mogelijk was.

In haar aanbevelingen stelde de commissie Van Traa als algemeen uitgangspunt voor de opsporing dat:

> "het op elk moment (…) mogelijk moet zijn te achterhalen met welke methode bepaalde informatie is verzameld. Niet alleen de inhoud van de informatie, maar ook de wijze waarop de informatie is verkregen dient te worden vastgelegd. Op die manier wordt het mogelijk de wijze van informatieverwerving te controleren."[42]

De controleerbaarheid van de herkomst is uiteindelijk ook het uitgangspunt geweest voor de voorstellen van de commissie tot aanpassing van de Wet Politieregisters, in het bijzonder de aangescherpte regels voor de CID-registers. De voorstellen waren gebaseerd op het onderscheid dat moet worden gemaakt tussen de open en de gesloten recherchetrajecten. Met de open trajecten wordt gedoeld op het 'regulier' opsporingsonderzoek, ook wel aangeduid als het tactisch rechercheonderzoek. De gesloten recherchetrajecten worden gevormd door de CID-matige onderzoeken. De gegevens die in deze onderzoeken worden verzameld zijn niet bedoeld voor opname in het strafdossier en dienen niet primair een bewijsdoel.[43] Om het aantal registraties in de CID-registers terug te dringen heeft de commissie aanbevelingen gedaan tot het aanscherpen van de opnamecriteria. De regering nam deze aanbevelingen over en kwam in juni 1997 met het Wetsvoorstel Wet bijzon-

41 Ruim 60.000 subjecten stonden ten tijde van het onderzoek geregistreerd in de CID-registers.

42 *Kamerstukken II* 1995/96, 24 072, nr. 14.

43 De gegevens uit deze onderzoeken worden vooral gebruikt voor sturing van tactische onderzoeken en criminaliteitsanalyse.

dere politieregisters dat een aanvulling vormde op de Wpolr.[44] De Wet bijzondere politieregisters[45] is vanaf 1 februari 2000 tot en met 1 januari 2008 van kracht geweest.

3.2 Internationale normen

Op de verwerking van politiële informatie zijn verschillende internationaalrechtelijke regelingen van toepassing. Wij noemen er zes. Ten eerste noemen wij de privacybepalingen uit het EVRM en IVBPR (subsectie 3.2.1). Ten tweede heeft Nederland zich gebonden aan het Europese Databeschermingsverdrag[46] (subsectie 3.2.2). Ten derde spelen de aanbevelingen voor de Politiesector van de Raad van Europa[47] een rol (subsectie 3.2.3). Ten vierde heeft Nederland het verdrag van Schengen[48] – ook wel aangeduid als de uitvoeringsovereenkomst – geratificeerd; ten vijfde geldt dit ook voor het Europolverdrag[49]. Ten zesde noemen wij het Verdrag van Prüm dat op 27 mei 2005 is gesloten tussen enkele Europese landen om intensiever te gaan samenwerken bij de bestrijding van terrorisme, grensoverschrijdende criminaliteit en illegale migratie.[50] Aangezien de drie laatstgenoemde verdragen voornamelijk bepalingen bevatten die van toepassing zijn op de *internationale* of grensoverschrijdende uitwisseling van politiegegevens binnen de eurozone, zullen wij deze niet verder behandelen. In dit onderzoek beperken wij ons tot de *interregionale* uitwisseling van gegevens binnen de Nederlandse politieorganisatie.

3.2.1 Het EVRM en het IVBPR

Het EVRM en het IVBPR zijn beide verdragen die rechtstreeks van toepassing zijn binnen de Nederlandse rechtsorde. Het EVRM stelt evenwel striktere eisen als het gaat om de bescherming van de privacy. Om die reden laten wij de privacybepaling uit het IVBPR hier verder buiten beschouwing. Art. 8 EVRM is zodoende de bepalende internationaal rechtelijke norm. Deze luidt als volgt:

---

44 *Kamerstukken II* 1996/97, 25 398, nrs. 1-2.

45 Wet van 27 mei 1999, *Stb*. 1999, 244.

46 Verdrag tot bescherming van personen met betrekking tot geautomatiseerde verwerking van persoonsgegevens (Straatsburg, 28 januari 1981, *Trb*. 1988, 7). Goedgekeurd bij Wet van 20 juni 1990, *Stb*. 351, gewijzigd bij Wet van 27 november 1991, Stb. 654.

47 Recommendation No. R (87) 15, regulating the use of personal data in the police sector, Council of Europe, Strassbourg, 1988.

48 Trb. 1990, 145; Goedkeuringswet in *Stb*. 1993, 138.

49 Overeenkomst tot oprichting van een Europese Politiedienst (Europol-Overeenkomst), *Trb*. 1995, 282.

50 *Trb* 2005, 197; Goedkeuringswet in *Stb*. 2008, 25; inwerking gereden op 20 februari 2008, *Trb*. 2008, 74.

1. "Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and necessary in a democratic society in the interest of national security, public safety or the economic well being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

De toepasselijkheid van deze bepaling valt uiteen in een abstracte en concrete werking. De abstracte werking stelt eisen aan de formeel-wettelijke regeling op nationaal niveau. De nationale normen zoals die voortvloeien uit de Wet en het Besluit Politiegegevens dienen te blijven binnen de grenzen die art. 8 EVRM daaraan stelt. De abstracte werking is voornamelijk van belang bij het wetgevingsproces.

Dit is anders voor de concrete werking. Art. 8 EVRM heeft allereerst rechtstreeks consequenties voor de verwerking van politiegegevens. De verwerking dient noodzakelijk te zijn met het oog op drie belangen:

(1) de verwerking moet worden gerechtvaardigd door een zwaarwegend maatschappelijk belang;
(2) de verwerking moet in overeenstemming zijn met het beginsel van proportionaliteit;
(3) de verwerking moet in overeenstemming te zijn met het beginsel van subsidiariteit.

Er moet zodoende een evenwicht worden gezocht in de verwerking van politiegegevens en het doel dat daarmee wordt beoogd (proportionaliteit); bovendien moet het doel niet kunnen worden bereikt op een minder ingrijpende wijze (subsidiariteit). De Memorie van Toelichting bij de goedkeuringswet van het Databeschermingsverdrag merkt in verband met deze doelspecificatie op:

> "dat gegevens niet met het oog op een eventueel mogelijk nut in de toekomst mogen worden opgeslagen, maar dat alleen een concreet bestaande legitieme behoefte van de houder de opslag kan rechtvaardigen."[51]

Aangezien de uitwisseling van politiegegevens een vorm van het verwerken van politiegegevens is, is art. 8 EVRM rechtstreeks van toepassing op de informatie-uitwisseling. Iedere verstrekking van informatie uit een politiedatabase dient zodoende te blijven binnen de grenzen van proportionaliteit en subsidiariteit. Toepassing van deze beginselen houdt in dat naarmate de gevoeligheid van de te verstrekken gegevens toeneemt het belang van dergelijke verstrekkingen ook meer moet worden aangetoond (Van Ruth en

51 *Kamerstukken II* 1998/89, 21 093, nr. 2, p. 4.

Schreuders, 2000). Dit geldt in het bijzonder wanneer het gaat om de verstrekking van informatie aan personen of instanties buiten de politieorganisatie. Verstrekkingen binnen de organisatie zijn gekoppeld aan de uitvoering van de politietaak die deze verstrekkingen in beginsel voldoende rechtvaardigen.[52]

3.2.2 Het Europees Databeschermingsverdrag

Anders dan het EVRM bevat het Databeschermingsverdrag geen rechtstreeks werkende bepalingen. Een beroep op het verdrag zou wel indirect geconstrueerd kunnen worden via art. 8 EVRM omdat het in feite een verdere uitwerking van de uitzonderingsgrond bevat. Het verdrag heeft in beginsel dus alleen een abstracte werking en richt zich daarmee primair tot de verdragsstaten. In het verdrag zijn beginselen opgenomen waaraan de nationale wetgever gebonden is. Wij noemen zes beginselen uit het verdrag die van toepassing zijn op de verwerking van politiegegevens. Deze internationale beginselen vloeien voort uit art. 5, 6, en 8 van het Databeschermingsverdrag en vormen de belangrijkste uitgangspunten voor de Wpolg, en voorheen de Wpolr.

1. "De gegevens dienen op eerlijke en rechtmatige wijze te worden verkregen en verwerkt;
2. de gegevens dienen te worden opgeslagen voor bepaalde legitieme doelen en niet te worden gebruikt op een wijze die onverenigbaar is met die doeleinden;
3. de gegevens moeten toereikend, ter zake dienend en niet overmatig zijn, uitgaande van de doelen waarvoor ze worden opgeslagen;
4. de gegevens dienen nauwkeurig te zijn en zo nodig te worden bijgewerkt;
5. de gegevens moeten worden bewaard in zodanige vorm dat de betrokkene hierdoor niet langer te identificeren is dan strikt noodzakelijk voor het doel waarvoor de gegevens zijn opgeslagen;
6. de gegevens dienen afdoende beveiligd te zijn tegen toevallige of ongeoorloofde vernietiging, toevallig verlies en ongeoorloofde toegang, wijziging of verspreiding ." (Van Ruth en Schreuder, 2000)

Een strikte toepassing van het tweede beginsel strekt ertoe dat de uitwisseling van politiegegevens uitsluitend is toegestaan voor zover deze in overeenstemming is met het doel van de gegevensverwerking. De Wpolg kent evenwel een verstrekkingenregime waarin het onder bepaalde voorwaarden wel mogelijk is om gegevens te verstrekken buiten het doel van de verwerking. Hoewel dit in strijd is met het tweede beginsel, beroept de wetgever zich in dat geval op de uitzonderingsgrond zoals die is vastgelegd in art. 9 van het Databeschermingsverdrag. Hierin is opgenomen dat van de bovenstaande beginselen kan worden afgeweken:

52 *Kamerstukken II* 1996/97, 25 398, nr. 2.

> "(…) when such derogation is provided by law of the Party and constitutes a necessary measure in a democratic society in the interest of: protection of State security, public safety, the money interest of the State or the suppression of criminal offences (…)."[53]

Wij constateren dat onder invloed van een toegenomen terroristische dreiging na 9/11, de wetgever een ruimere interpretatie van de internationale norm *necesssary in a democratic society* hanteert. In zijn algemeenheid voorziet de Wpolg in ruimere mogelijkheden tot gegevensverwerking en ruimere mogelijkheden om politiegegevens uit te wisselen met ketenpartners buiten de politieorganisatie. Wij menen dat deze verruimingen extra privacyrisico's meebrengen voor geregistreerden en dat het rechtstatelijke beginsel van effectieve rechtsbescherming in dit verband vraagt om effectievere waarborgingsmechanismen.

3.2.3 Aanbevelingen van de Raad van Europa

De aanbevelingen van de Raad van Europa hebben evenals het Europees Databeschermingsverdrag slechts een abstracte werking. De directe betekenis voor de individuele burger van deze bepalingen is daarom gering. De aanbevelingen moeten daarom worden beschouwd als adviezen aan de nationale regeringen. Hoewel de nationale regeringen strikt genomen de aanbevelingen naast zich neer kunnen leggen, is gebleken dat deze in de praktijk wel degelijk indirect invloed hebben op het wetgevingsproces (Kooijmans, 2008). Voor het onderzoek is het van belang dat de aanbevelingen met betrekking tot de verstrekking van persoonsgegevens uit politieregistraties een onderscheid maken tussen drie categorieën van verstrekkingen. Dit zijn (1) verstrekkingen binnen de politiesector, (2) verstrekkingen aan personen en instanties met een publieke taak en (3) verstrekkingen aan private personen en instanties.[54] Aan de twee laatste categorieën kan uitsluitend worden verstrekt wanneer er sprake is van een "*clear legal obligation or authorisation of the supervisory authority*". Voor verstrekkingen aan personen en instanties met een publieke taak geldt dat de verstrekkingen slechts kunnen plaatsvinden op basis van de publieke taak die in het verlengde ligt van de politietaak. Op de uitwerking van deze verstrekkingsvoorwaarden komen wij uitgebreider terug in sectie 3.6.

3.3 Nationale normen: begrip, beheer, en doel

De nationale normen voor de uitwisseling van politiële gegevens en de uitwisseling van criminele inlichtingen zijn, zoals eerder aangegeven, geduren-

53 Art. 9 lid 2 Europees Databeschermingsverdrag.
54 Een dergelijk onderscheid wordt ook gemaakt door Ruth en Schreuders, 2000.

de de periode van onderzoek (2005 – 2008) gewijzigd. Bij aanvang van het onderzoek waren op de verwerking en uitwisseling van informatie de Wpolr en het Bpolr van toepassing. De Wpolr kende een reglementplicht zodat voor ieder regionaal gevoerd politieregister een reglement moest worden opgesteld. Met de inwerkingtreding van de Wpolg op 1 januari 2008 is de reglementplicht komen te vervallen. Omdat (1) ons onderzoek naar de uitwisseling van informatie tot stand is gekomen onder de Wpolr, en (2) de politieorganisatie en werkprocessen gedurende de onderzoeksperiode gebaseerd waren op deze wet, besteden wij bij de bespreking van de nationale normen ook aandacht aan de Wpolr. Wij merken daarbij op dat in de 'nieuwe' Wpolg de bepalingen ten aanzien van de verwerking en uitwisseling van politiegegevens voor een belangrijk deel overeenkomen met de 'oude' Wpolr.

In deze sectie bespreken wij allereerst enkele algemene uitgangspunten van de Wpolr te weten: het begrip politieregister (subsectie 3.3.1), het beheer van een politieregister (subsectie 3.3.2), de doelbinding en de uitvoering van de politietaak (subsectie 3.3.3).

3.3.1 Het begrip 'politieregister'

In de oude Wpolr vormde het begrip 'politieregister' het aangrijpingspunt voor de normering van de verwerking van politiegegevens. Blijkens de definitiebepalingen, art. 1 lid 1 sub c Wpolr, moeten drie elementen worden onderscheiden om te kunnen spreken van een politieregister.

Ten eerste moet er sprake zijn van een gegevensverzameling die samenhangende persoonsgegevens bevat over verschillende personen. De samenhang kan onder meer volgen uit één of meer gemeenschappelijke kenmerken. In de meeste gevallen kan dat worden afgeleid uit de (data)structuur van de gegevensverzameling en de bijbehorende methode om de verzameling te kunnen raadplegen. Voor de samenhang is het verder van belang dat de verschillende onderdelen van de gegevensverzameling als één logisch geheel kunnen worden beschouwd. Het begrip persoonsgegeven uit deze voorwaarde wordt verder niet gedefinieerd in de Wpolr. Daarvoor wordt aansluiting gezocht bij de Wbp waarin "elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon" geldt als een persoonsgegeven. Via de koppelbepaling in art. 1 lid 1 sub i Wbp gold deze definitie ook voor de Wpolr. Het criterium is daarbij dat het steeds moet gaan om gegevens die daadwerkelijk informatie bevatten over een persoon en dat de gegevens (mede) bepalend kunnen zijn voor de wijze waarop deze persoon in het maatschappelijke verkeer wordt beoordeeld of behandeld (cf. Buruma, Goos en Michels, 2003). De aard van het politiewerk brengt met zich mee dat vrijwel altijd aan dit criterium wordt voldaan.

Ten tweede geldt dat (1) de verzameling langs geautomatiseerde weg tot stand wordt gebracht of (2) op andere wijze is aangelegd met het oog op een doeltreffende raadpleging. Uit het tweede element van de definitie blijkt dat de wetgever geen onderscheid heeft willen maken tussen geautomatiseerde gegevensverzamelingen en verzamelingen die handmatig worden gevoerd. Voor de bescherming van de persoonlijke levenssfeer is het in beginsel ook niet relevant of de persoonsgegevens systematisch liggen opgeslagen in een kaartenbak of in een geautomatiseerde database. Het gaat primair om de opslag en verwerking van de gegevens en daarvoor is de systematiek, die er feitelijk voor zorgt dat de gegevensverzameling toegankelijk wordt gemaakt, belangrijker dan het medium waarop de gegevens zijn opgeslagen. Natuurlijk is dit een louter theoretische benadering, in de praktijk ligt het geheel anders als we spreken over enkele honderden miljoenen gegevens.

Ten derde dient de verzameling te zijn aangelegd in het kader van de uitvoering van de politietaak. Hiermee wordt gedoeld op de politietaak zoals die is neergelegd in art. 2 van de Politiewet 1993. Met deze laatste voorwaarde heeft de wetgever het onderscheid tussen de oude Wpolr en de Wpolg enerzijds en de Wbp anderzijds, duidelijk willen markeren. Registraties die niet zijn aangelegd ter uitvoering van de politietaak vallen onder het regime van de Wbp. Dat geldt binnen de politieorganisatie bijvoorbeeld voor registraties die niet direct voortvloeien uit de politietaak, zoals de personeelsregistraties en financiële administratie.[55]

Onder de Wpolg wordt het begrip politieregister niet langer als aangrijpingspunt voor de normering genomen. In plaats daarvan is het begrip 'verwerken' centraal komen te staan. In de definitiebepaling, art. 1 sub c Wpolg wordt onder verwerken verstaan: "elke handeling of geheel van handelingen met betrekking tot politiegegevens". Het aangrijpingspunt heeft voor het wettelijk kader tot gevolg dat het onderscheid tussen de verschillende soorten registers komt te vervallen. Deze verandering in wetgeving betekent echter niet dat in de politiepraktijk daarmee ook tegelijkertijd de registerstructuur is verdwenen. De registers (dat wil zeggen politiedatabases) blijven ook onder de Wpolg als zodanig functioneren omdat de politiële informatiesystemen volgens die structuren zijn ontworpen. Of liever gezegd, bij het ontwerpen van de (oude) Wpolr is nadrukkelijk rekening gehouden met de wijze waarop de destijds bestaande informatiesystemen functioneerden. In juridische termen wordt thans niet meer gesproken over de aanleg van een politieregister, maar over de verwerking van politiegegevens.

55 In art. 2 Wpolr wordt deze beperking in het bereik van de Wpolr nogmaals uitdrukkelijk vastgelegd.

3.3.2 Het beheer van politieregisters en databases

In de Wpolr werd aangesloten bij de beheersstructuur van de Politiewet 1993.[56] Dit betekende dat het beheer van een politiekorps was gekoppeld aan het beheer van de daar gevoerde politieregisters.

In het derde lid van art. 4 Wpolr werd aan de beheerder de verplichting opgelegd zorg te dragen voor de juistheid en de volledigheid van de geregistreerde gegevens. Dat kon de beheerder doen door bijvoorbeeld organisatorische en procedurele maatregelen te nemen. We geven een voorbeeld. Een uitgangspunt was dat de registratie van onjuiste of onvolledige gegevens onrechtmatig is. Dergelijke gegevens dienen dus zo spoedig mogelijk, dat wil zeggen binnen een redelijke termijn, gewijzigd of aangevuld te worden. Is dat niet mogelijk dan moeten zij worden verwijderd uit het register. Onzorgvuldige registratie van gegevens kan immers leiden tot een onjuist beeld van personen hetgeen kan leiden tot inbreuken op diverse grondrechten.

Binnen het kader van dit onderzoek rijst de vraag hoe de beheersverantwoordelijkheid ligt wanneer een politieregister door meerdere regio's tegelijk wordt gebruikt. Voor het antwoord op deze vraag moet onderscheid worden gemaakt tussen het raadplegen van het register en het (on-line) kunnen invoeren en muteren van gegevens. Het raadplegen van een politieregister wordt door de Wpolr beschouwd als een bijzondere vorm van verstrekken en is als zodanig geen onderdeel van het voeren van een register. Bepalend voor de vraag of er sprake is van een zogenaamd gemeenschappelijk gevoerd register is de mogelijkheid dat meerdere regiokorpsen gegevens kunnen invoeren en muteren. Is dat het geval dan geldt de bepaling van art. 1 lid 1 sub f onderdeel 5 Wpolr. De beheerder die is belast met de feitelijke zeggenschap en zorg voor het goed functioneren van dat register geldt als de verantwoordelijke beheerder. Uiteindelijk zal dat afhangen van de afspraken die de korpsen onderling daarover hebben gemaakt.

In de Wpolg wordt niet meer gesproken over de beheerder, maar is aansluiting gezocht bij het begrippenkader zoals dat ook wordt gehanteerd in de Wbp. In plaats van een beheerder spreekt de Wpolg over de 'verantwoordelijke'. Gelet op de regionale organisatiestructuur van de politie is hier slechts sprake van een taalkundige wijziging. De verantwoordelijke onder de Wpolg is evenals de beheerder onder de Wpolr, in iedere afzonderlijke politieregio, de korpsbeheerder (art. 1 sub f. Wpolg).

56 Zie art. 1 lid 1 sub 1 Wpolr.

3.3.3 Doel register en goede uitvoering van politietaak

Het aanleggen van een politieregister werd onder de Wpolr genormeerd in art. 4 door het stellen van twee cumulatieve voorwaarden voor de aanleg van een politieregister.[57] Ten eerste moest de aanleg een duidelijk en concreet doel dienen dat moest worden vastgelegd in het registerreglement.[58] Ten tweede diende de aanleg van een register noodzakelijk te zijn voor de goede uitvoering van de politietaak. De wetgever heeft met deze voorwaarden tot uitdrukking willen brengen dat politieregisters niet onbeperkt kunnen worden aangelegd en in stand gehouden.[59] Onder de Wpolg is dat in feite niet heel veel veranderd. Het doel voor de gegevensverwerking behoeft niet in een apart reglement te worden vastgelegd. In de plaats daarvan zijn in de Wpolg zelf vijf doelen voor gegevensverwerking vastgelegd en dient de verwerking van politiegegevens noodzakelijk te zijn met het oog op één of meer van deze doelen. In subsectie 3.7.1. komen wij nader terug op deze doelstellingen.

De feitelijke normering van de gegevensverwerking zit daarmee in de *noodzakelijkheidsvoorwaarde*. In beginsel houdt deze voorwaarde in dat er een afweging moet worden gemaakt tussen de verschillende beschikbare methoden die de politie ter beschikking staan. Die afweging moet er toe leiden dat uiteindelijk wordt gekozen voor de methode die het minst schadelijk is voor de persoonlijke levenssfeer (subsidiariteit). Overigens komt deze afweging pas daadwerkelijk aan de orde wanneer aannemelijk is dat er naast het aanleggen van een politieregister nog andere, minder ingrijpende, mogelijkheden zijn. Verder dient de aanleg noodzakelijk te zijn voor de 'goede' uitvoering van de politietaak. De betekenis van deze normatieve verwijzing is echter gering omdat de kwaliteit van de uitvoering van het politiewerk moeilijk te meten is (cf. Buruma, Goos en Michels, 2003, p. 84). De toevoeging 'goede' geeft daarom slechts aan dat er geen *conditio sine qua non*-verband wordt geëist tussen de taakuitvoering en het politieregister. Op die manier is het mogelijk registers aan te leggen die weliswaar niet absoluut noodzakelijk zijn voor de goede uitvoering van de politietaak, maar de kwalitatieve uitvoering daarvan wel kunnen verhogen.

---

57 Met 'aanleggen' bedoelt de wetgever blijkens de Memorie van Toelichting "het geheel van activiteiten dat erop is gericht dat een registratie tot stand komt." *Kamerstukken II* 1988/89, 19 589, nr. 11, p. 16.

58 In art. 9 Wpolr is bepaald dat voor ieder register afzonderlijk een reglement wordt opgesteld. Vervolgens wordt in art. 10 lid 2 Wpolr voorgeschreven ten aanzien van welke onderwerpen een duidelijke regeling opgenomen dient te worden in het reglement; een omschrijving van het doel is een van die onderwerpen.

59 *Kamerstukken II* 1988/89, 19 589, nr. 3, p. 7 & 17.

3.4 Nationale normen: algemene opnamecriteria en gevoelige gegevens

In deze sectie behandelen wij de bepalingen betreffende de opslag van gegevens die voor alle politiedatabases gelden. Deze zogenaamde algemene opnamecriteria zijn onderwerp van subsectie 3.4.1. In subsectie 3.4.2 bespreken wij de normen met betrekking tot opslag van gevoelige gegevens. De algemene opname criteria en het regime van de verwerking van gevoelige gegevens zijn in de Wpolg nauwelijks gewijzigd maar vrijwel geheel gelijk gebleven aan het regime zoals dat gold onder de Wpolr.

3.4.1 Algemene opnamecriteria

Voordat gegevens mogen worden opgenomen in een database van de politie (voorheen dus politieregister), moet er aan twee cumulatieve algemene opnamecriteria worden voldaan, te weten *rechtmatigheid* en *doelbinding*.

Het eerste algemene opnamecriterium, de rechtmatigheid, houdt in dat de wijze van gegevensverkrijging getoetst dient te worden aan het geschreven en ongeschreven recht. Concreet moet worden nagegaan hoe bepaalde gegevens in een database terecht zijn gekomen (Buruma, Goos en Michels, 2003, p. 87). Het hangt onder meer af van de manier waarop de politie aan de informatie is gekomen maar het kan ook samenhangen met de uitwisseling van gegevens tussen databases onderling. Wij onderscheiden in dit verband twee rechtmatigheidperspectieven.

1) *Het strafvorderlijke perspectief.* Het strafvorderlijke perspectief wordt bepaald door het leerstuk van het onrechtmatig verkregen bewijs. De verkrijging van gegevens dient in de opsporingsfase te voldoen aan de wettelijke eisen zoals die zijn vastgelegd in het Wetboek van Strafvordering. Daarnaast wordt de rechtmatigheid bepaald door de ongeschreven beginselen van een goede procesorde (Cleiren, 1989). Onrechtmatig verkregen gegevens mogen niet worden opgeslagen in de politieregisters en wanneer onrechtmatigheid achteraf blijkt, dienen de gegevens te worden verwijderd.

2) *Het privacyrechtelijke perspectief*. In het privacyrechtelijke perspectief kan de onrechtmatigheid van de verkrijging voortvloeien uit handelingen die in strijd zijn met privacyvoorschriften van onder meer de Wpolg.[60] Het is evenwel denkbaar dat databestanden met persoonsgegevens door derden aan de politie ter beschikking worden gesteld in strijd met bijvoorbeeld de Wbp. In dat geval is de verwerking van deze gegevens ook in strijd met de Wpolg.

60 Eventueel kunnen ook voorschriften uit de Wbp worden geschonden, maar vanwege de beperkte toepassing op politieregisters is dat vooral een theoretische mogelijkheid.

Het wettelijke stelsel van rechtsbescherming van waaruit een waarborgende werking dient uit te gaan, ook ten aanzien van de rechtmatigheid van de gegevensverwerking is echter reactief. Dit wil zeggen dat altijd pas achteraf controle plaatsvindt door de rechter op de rechtmatigheid van de gegevensverwerking. Vanuit het oogpunt van de privacybescherming is dit onwenselijk omdat het kwaad dan immers reeds is geschied. Voor een effectieve rechtsbescherming zou een controlesysteem van meer pro-actieve toetsing beter zijn en meer bescherming bieden aan de geregistreerden.

In het huidige systeem kan het voorkomen dat een strafrechtelijke procedure leidt tot onrechtmatige verkrijging of verwerking van gegevens en op basis daarvan uiteindelijk tot uitsluiting van die gegevens als bewijs.[61] Dan ontstaat echter het volgende probleem: dezelfde rechter dient na uitsluiting van het bewijsmateriaal op basis van het overige bewijsmateriaal zich een oordeel te vormen over de zaak. Volgens Enschedé (1966) en Melai (1975) is het daarbij niet ondenkbaar dat het, als onrechtmatig uitgesloten bewijs, toch via 'oncontroleerbare psychische en intellectuele banen' invloed zal uitoefenen op de uiteindelijke beantwoording van de schuldvraag. Enschedé acht het uitsluiten van onrechtmatig verkregen bewijs om deze reden zinloos en pleitte voor afschaffing daarvan. Melai komt met een genuanceerdere opvatting. Hij stelt dat het onderzoek naar de rechtmatigheid van de verkrijging van het bewijs niet thuis hoort in het onderzoek ter terechtzitting en daarom bepleitte hij dat de controle dient te geschieden door een andere rechter dan de zittingsrechter.

De discussie rond onrechtmatig verkregen bewijs blijft actueel en heeft zich ook uitgebreid naar de privacyrechtelijke rechtmatigheid. Kielman en Koelewijn (2005) hebben in dat verband betoogd dat onder invloed van technologische ontwikkelingen privacynormen een steeds belangrijkere positie krijgen binnen het strafproces. Door nieuwe technieken vormen politiedatabases niet meer uitsluitend een collectief geheugen van de politie maar lijkt men hoe langer hoe meer in staat om juist uit de gecombineerde gegevensverwerkingen ' verdenkingen' in de zin van art. 27 Sv te construeren. Daarmee vindt ook een verschuiving plaats in de belangen die de privacyregels beogen te beschermen. Er wordt niet langer meer uitsluitend een privacybelang beschermd maar de regels dienen steeds meer ook ter bescherming van een strafvorderlijk belang van verdachte burgers. De verwerking van politiegegevens wordt immers meer en meer gebruikt als opsporingsmiddel. In dat verband wijzen wij ook op het in hoofdstuk 2 besproken *singularity point* (Kurzweil, 2005) en het *data driven decision process*. Naarmate computers slimmere beslissingen kunnen nemen op basis van zeer grote hoeveelheden data,

61 Zie daarover uitgebreid: M.C.D. Embregts, *Uitsluitsel over bewijsuitsluiting. Een onderzoek naar de toelaatbaarheid van onrechtmatig verkregen bewijs in het stafrecht, het civiele recht en het bestuursrecht*, diss. Tilburg, Kluwer: 2003.

ontstaat daardoor vroeg of laat een potentieel grote bedreiging van de persoonlijke levenssfeer. Wij menen in dit licht dat daarom niet meer kan worden volstaan met een uitsluitend reactief systeem van rechtsbescherming, maar pleiten voor een pro-actief systeem dat wordt geïmplementeerd in het computersysteem zelf. Daarmee is de privacybescherming het beste gewaarborgd en kan het een onderdeel vormen van de 'intelligente' beslissingen van de computer.

Hoewel in dit onderzoek de focus ligt op de privacyrechtelijke rechtmatigheid van verstrekkingen uit politiedatabases tekenen wij hier aan dat wij verwachten dat in de nabije toekomst, gelet op de snelheid waarmee de technologie zich ontwikkelt, ook een steeds groter wordend strafvorderlijk belang gediend is met de verwerking van gegevens. Binnen tien jaar verwachten wij dat een substantieel deel van de strafvorderlijke beslissingen uiteindelijk *data driven* zal zijn en dus gebaseerd op de verwerking van zeer grote hoeveelheden persoonsgegevens.

In de huidige praktijk vindt nauwelijks effectieve controle plaats op de rechtmatigheid van de gegevensverwerking. Wanneer gegevens uit de ene database worden verstrekt in strijd met deze algemene verstrekkingsvoorschriften zijn, dan leidt dat in feite tot een onrechtmatige verkrijging door de verzoekende politieambtenaar. Deze mag de gegevens niet gebruiken. Volgens Buruma, Goos en Michels (2003) speelt het daarbij echter wel een rol of de ontvanger zich van de onrechtmatigheid van de verstrekking in redelijkheid bewust kon zijn. Voor ons onderzoek is dat een belangrijk punt. Het verstrekken van informatie is bijvoorbeeld onrechtmatig wanneer vaststaat dat die informatie niet langer noodzakelijk is met het oog op het doel waarvoor de database was aangelegd. De mate waarin de verkrijger zich bewust kan zijn van deze onrechtmatigheid is vanzelfsprekend zeer gering. In de praktijk zal het om die reden weinig aannemelijk zijn dat een schending van dat doelbindingsvoorschrift uiteindelijk ook zal leiden tot een onrechtmatige verkrijging van gegevens. De nuancering geldt niet voor verstrekkingen aan het openbaar ministerie. De officier van justitie is immers verantwoordelijk voor de opsporing. Hij[62] zal zich om die reden niet kunnen beroepen op onwetendheid of goede trouw ter zake van de rechtmatigheid van de verkrijging (cf. Buruma, Goos en Michels, 2003). Wij denken dat de houdbaarheidsdatum van deze opvatting beperkt is in het licht van de technologische ontwikkelingen. In de nabije toekomst zal het belang aan (geautomatiseerde) controle op de doelbinding toenemen omdat deze samen met de noodzakelijkheidsafweging de kern vormt van de informationele privacybescherming.

62 Kortheidshalve gebruiken wij 'hij' en 'zijn' als wij bedoelen te zeggen 'hij/zij' of 'zijn/haar'.

Dit brengt ons op het tweede algemene opnamecriterium dat voortvloeit uit de genoemde doelbinding. Het opnemen van gegevens diende onder de Wpolr noodzakelijk te zijn met oog op het doel waarvoor het register werd aangelegd en thans voor het doel waarvoor de gegevens worden verwerkt. Nu strekt het criterium zich uit tot ieder individueel opgenomen persoonsgegeven. Onder deze omstandigheden kan het gebeuren dat een categorie van personen op zichzelf genomen voldoet aan de noodzakelijkheidstoets, maar dat een concreet gegeven binnen die categorie de noodzakelijkheidstoets niet kan doorstaan. Hiermee wordt duidelijk dat de verantwoordelijke voor iedere gegevensverwerking een aparte afweging zal moeten maken.

Uit onderzoek is gebleken dat politieambtenaren moeite hebben met het toepassen van deze noodzakelijkheidstoets en het maken van dergelijke afwegingen (Cozijn e.a., 1996 en Schreuder e.a., 2005). Vooral wanneer het gaat om de registratie van criminele inlichtingen is de vraag relevant op welk moment de noodzakelijkheid van een opgenomen gegeven voor het doel van dat register vast moet staan. Uit de aard van het inlichtingenwerk vloeit immers voort dat vaak nog niet kan worden vastgesteld of er sprake is van relevante en juiste gegevens. Om die reden is de noodzakelijkheidstoets als algemeen opnamecriterium met name in de proactieve fase van de opsporing in feite niet toe te passen.

3.4.2 Gevoelige gegevens

In het eerste lid van art. 5 Wpolg (voorheen art. 5 Wpolr) heeft de wetgever limitatief acht categorieën van gegevens neergelegd die moeten worden aangemerkt als bijzonder privacygevoelige gegevens. Dat zijn gegevens betreffende (1) godsdienst of (2) levensovertuiging, (3) ras, (4) politieke gezindheid, (5) seksualiteit, (6) intiem levensgedrag, en gegevens betreffende (7) medische of (8) psychologische kenmerken van een persoon. In beginsel is de registratie van personen op basis van deze kenmerken verboden.

In de praktijk kan de toepassing van dit artikel problemen opleveren omdat niet altijd duidelijk is wanneer nu sprake is van een gevoelig gegeven. Extra complicerend is het onderscheid tussen impliciet en expliciet gevoelige gegevens. Bij impliciet gevoelige gegevens moet ook worden gekeken naar de omstandigheden waaronder een registratie plaatsvindt. Wanneer in een politieregio bijvoorbeeld een database wordt aangelegd waarin alle moslims uit de regio worden geregistreerd, dan wordt weliswaar niet bij iedere geregistreerde persoon afzonderlijk vermeld dat deze moslim is, maar is deze 'gevoelige' informatie over de levensovertuiging wel als zodanig af te leiden uit het register. Elke categorie van gevoelige gegevens moet daarom nader worden geïnterpreteerd; de exacte grenzen van het bereik zijn immers niet altijd duidelijk.

Toch heeft de wetgever heel goed begrepen dat er in de politiepraktijk ook veel gevallen zijn waarin het voor de uitvoering van de politietaak wel noodzakelijk is dat er gevoelige gegevens worden geregistreerd. Om daarin te voorzien zijn in art. 5 Wpolg twee cumulatieve voorwaarden neergelegd waaronder het mogelijk is gevoelige gegevens te registreren.

Voorwaarde 1: De gevoelige gegevens moeten een *aanvulling* vormen op andere (niet-gevoelige) gegevens. De politie moet een zelfstandige reden hebben om de gegevens te registreren. De reden mag uitdrukkelijk niet liggen in de gevoelige gegevens zelf.

Voorwaarde 2: De registratie van de gevoelige gegevens moet onvermijdelijk zijn voor het doel waarvoor het register is aangelegd. De doelbinding die de wetgever hier voorschrijft is vergelijkbaar met het tweede algemene opnamecriterium dat voortvloeit uit het tweede lid van art. 3 Wpolg. Het verschil zit echter in het gebruik van de term *onvermijdelijk* in tegenstelling tot het begrip *noodzakelijk.* De wetgever heeft met de onvermijdelijkheid aangegeven dat er een striktere relatie wordt vereist tussen de gevoelige informatie en het doel dan het geval is bij de algemene noodzakelijkheidseis. Er moet een *conditio sine qua non*-verband bestaan tussen de gevoelige gegevens en het doel van het register. *Conditio sine qua non* houdt in dat het doel in een concreet geval niet gehaald kan worden wanneer de gevoelige gegevens niet worden geregistreerd.

3.5 Registers en verwerkingscriteria

Bij de bespreking van de historische achtergrond in subsectie 3.1.3 is aangegeven dat de parlementaire enquête naar de opsporingsmethoden onder andere heeft geleid tot een wijziging van de Wpolr. Kort gezegd bestonden deze wijzigingen eruit dat voortaan een onderscheid gemaakt wordt tussen 'gewone politieregisters' en 'bijzondere politieregisters'. Onder deze laatste vielen drie categorieën te weten: (1) de tijdelijke registers, (2) de voorlopige registers, en (3) de registers zware criminaliteit. Tijdelijke registers worden aangelegd voor de uitvoering van de politietaak in een bepaald geval of in het kader van een verkennend onderzoek.[63] De zinsnede 'een bepaald geval' doelt veelal op een concreet misdrijf. Het is daardoor in tijd en plaats beperkt en moest worden gesloten en vernietigd wanneer dat doel was gehaald.

In dit onderzoek hebben wij ons beperkt tot de voorlopige registers (subsectie 3.5.1) en de registers zware criminaliteit (subsectie 3.5.2). In de Wpolg wordt als gezegd geen onderscheid meer gemaakt tussen de verschillende soorten registers maar worden gegevensverwerkingen onderscheiden al

63 Zie de oude definitiebepaling, art. 1 lid 1 sub j Wpolr.

naar gelang het doel voor de verwerking. Desondanks bespreken wij hier het oude onderscheid tussen de verschillende registers omdat gedurende de onderzoeksperiode dat onderscheid nog wel gold en de CIE-organisatie daarop is ingericht.

3.5.1 Het voorlopig register

De voorlopige registers functioneerden onder de Wpolr als een extra waarborg bij de verwerking van persoonsgegevens. Deze registers werden, evenals de registers zware criminaliteit, beheerd door de regionale CIE.[64] Het voorlopig register was bedoeld om informatie op te slaan die (nog) niet in aanmerking kwam voor opname in het register zware criminaliteit. Het ging dan om informatie waarvan de CIE vermoedde en verwachtte dat deze in de nabije toekomst wel kon worden opgeslagen in het register zware criminaliteit. Omdat het om (zeer) zachte informatie gaat kon de betrouwbaarheid daarvan meestal niet worden ingeschat. De bedoeling van de tijdelijke registratie in de voorlopige registers was om te onderzoeken of de informatie in samenhang met andere nog te verkrijgen gegevens alsnog zou kunnen voldoen aan de eisen van betrouwbaarheid en juistheid zoals die gelden voor het register zware criminaliteit.[65]

De normering van het voorlopig register moet worden gelezen in samenhang met de bijzondere opnamecriteria die gelden voor het register zware criminaliteit. Het verschil tussen beide registers was echter moeilijk te duiden. Voor beide registers golden weliswaar dezelfde opnamecriteria maar in het voorlopig register werden gegevens opgeslagen die nog niet 'rijp' waren voor het register zware criminaliteit. Nadat namelijk was vastgesteld dat de gegevens voldoen aan de algemene en bijzondere opnamecriteria moest de betrokken CIE zich een oordeel gaan vormen over de aard, de betrouwbaarheid, en de verifieerbaarheid van de informatie. Dit oordeel was bepalend voor de vaststelling of de gegevens konden worden opgenomen in het register zware criminaliteit of dat zij eerst in het voorlopig register moesten worden opgeslagen.

De beoordeling kende twee toetsen. Ten eerste moest worden nagegaan in welke mate de te registreren persoon daadwerkelijk betrokken was bij feiten waarmee hij in verband werd gebracht. Ten tweede moest er een inschatting worden gemaakt van de juistheid van het vermoeden van die betrokkenheid. Wanneer bijvoorbeeld de mate van betrokkenheid uitsluitend gebaseerd kon worden op één enkele tip van een onbekende informant en een

64 Ieder regionaal politiekorps dient ingevolge art. 5 lid 1 Besluit beheer regionale korpsen te beschikken over een Criminele Inlichtingen Eenheid.

65 Om deze reden wordt het voorlopig register ook wel het vaststellingsregister genoemd.

inschatting van de juistheid van het vermoeden niet goed mogelijk was, dan kwamen de gegevens in beginsel in aanmerking voor registratie in het voorlopig register. Steeds was het bij de beoordeling van belang of de CIE bevestiging voor de tip kon vinden in andere bronnen of bij andere informanten. Ingeval deze bevestiging niet gevonden kon worden, dan mochten de gegevens voor ten hoogste een periode van 6 maanden opgeslagen worden in het voorlopig register. Wanneer voor de afloop van deze periode nog altijd geen bevestiging was gevonden in andere bronnen dan dienden de gegevens verwijderd en vernietigd te worden.[66]

Onder de Wpolg is geen aparte regeling opgenomen voor de 'oude' voorlopig register-informatie. Dit betekent dat alle informatie die wordt verwerkt door de CIE komt te vallen onder art. 10 Wpolg dat grotendeels overeenkomt met het oude regime dat gold voor de register zware criminaliteit. Dit regime bespreken wij in de volgende subsectie.

3.5.2 Het register zware criminaliteit

In de registers zware criminaliteit werden tot 1 januari 2008 persoonsgegevens en andere relevante informatie geregistreerd over de zwaardere vormen van criminaliteit. Ondanks dat in de Wpolg het begrip 'register zware criminaliteit' niet meer voorkomt blijven de databases feitelijk ongewijzigd bestaan tot tenminste 2010. Tot die tijd blijft de politie gebruik maken van de oude informatiesystemen die volledig zijn ingericht op de registerstructuur. Slechts stapsgewijs zullen deze systemen worden geoptimaliseerd en aangepast aan de Wpolg.[67] De veranderingen zullen vooralsnog uitsluitend optreden in de inhoud van de databases. Wij blijven vanwege deze overgangsperiode in het vervolg van het onderzoek de term 'register zware criminaliteit' gebruiken en bedoelen daarmee de database waarin de criminele inlichtingen liggen opgeslagen. Wij zijn ons er terdege van bewust dat de opnamecriteria, vanwege het vervallen van het voorlopig register, veranderd zijn per 1 januari 2008.

In het register zware criminaliteit worden tips en aanwijzingen van informanten opgeslagen waarvan in veel gevallen de juistheid en de betrouwbaarheid nog niet volledig vaststaat of kan worden ingeschat.[68] De aard van deze informatie brengt mee dat er vaak nog geen concrete verdenking bestaat tegen de geregistreerde personen. De noodzaak tot registratie van deze onverdachte personen doet zich bij de bestrijding van zware criminali-

66 Art. 13b lid 5 Wpolr.

67 Raad van Hoofdcommissarissen, Wenkend perspectief. Strategische visie op politieel informatiemanagement en technologie 2006-2010, Projectgroep visie op de politiefunctie, 2006.

68 *Kamerstukken II* 1996/97, 25 398, nr. 3 p. 5.

teit vooral voor wanneer dat plaatsvindt in georganiseerd verband. Om inzicht te verkrijgen in de organisatie moet de politie voor langere perioden allerlei uiteenlopende gegevens opslaan en analyseren. Dat zijn bijvoorbeeld gegevens over de levenswijze van personen, hun contacten, en hun gedragingen. Deze gegevens kunnen uiteindelijk, al dan niet in combinatie met andere informatie, inzicht gegeven in de omvang en activiteiten van een bepaalde criminele organisatie. Het langdurig registreren van deze gegevens vormt echter een vergaande inbreuk op de persoonlijke levenssfeer. In de proactieve fase van de opsporing wordt deze inbreuk nog niet gerechtvaardigd door een concrete strafvorderlijke verdenking. Daarom zijn in de wettelijke regeling naast de hiervoor besproken algemene opnamecriteria ook bijzondere opnamecriteria vastgelegd waarmee de wetgever beoogt de opslag en het gebruik van dergelijke informatie te beperken. De bijzondere opnamecriteria voor het register zware criminaliteit leggen twee beperkingen op. Ten eerste geldt er een beperking ten aanzien van de soort misdrijven (A). Ten tweede is er een beperking aangelegd in de omschreven categorieën van personen ten aanzien van wie persoonsgegevens mogen worden geregistreerd (B).

Ad A: Vier categorieën van misdrijven
In art 10 lid 1 sub a Wpolg (voorheen: art. 1 lid 1 sub k Wpolr) heeft de wetgever limitatief vier categorieën van misdrijven vastgelegd ten aanzien waarvan de CIE gegevens mag vastleggen in het register zware criminaliteit.

De eerste categorie betreft de misdrijven waarvoor krachtens art. 67 lid 1 Sv voorlopige hechtenis is toegestaan. Als aanvullende voorwaarde op deze categorie geldt dat de misdrijven daarnaast in georganiseerd verband beraamd of gepleegd dienen te worden en dat deze misdrijven gezien hun aard of de samenhang met andere misdrijven die in georganiseerd verband worden beraamd of gepleegd, een ernstige inbreuk op de rechtsorde opleveren. Onder een georganiseerd verband moet blijkens de Memorie van Toelichting worden verstaan: "een vast verband of wisselende verbanden die deel uitmaken van de georganiseerde criminaliteit". Daarmee is aansluiting gezocht bij de kenmerken die de commissie-Van Traa heeft omschreven in haar eindrapportage.[69] Van een georganiseerd verband is sprake wanneer het gaat om een groep personen die de volgende drie kenmerken heeft.

(a) De groep is primair gericht is op illegaal gewin.
(b) De groep pleegt systematisch misdaden met ernstige gevolgen voor de samenleving.
(c) De groep is in staat deze misdrijven op betrekkelijk eenvoudige wijze af te schermen, in het bijzonder door de bereidheid te tonen fysiek geweld te gebruiken of personen door corruptie uit te schakelen.

69 *Kamerstukken II* 1995/96, 24 072, nrs. 10-11, p.25.

Wanneer er voldaan is aan één of meer van deze kenmerken kan er gesproken worden van een georganiseerd verband. De wetgever spreekt verder over het beramen of plegen van misdrijven. Het begrip 'beramen' doelt op de betrokkenheid van een persoon (of een groep) bij al datgene wat in verband met het plegen van een strafbaar feit vooraf is gegaan aan dat strafbare feit. Of er sprake is van een beraming hangt vooral af van de feiten en omstandigheden van het geval. Met plegen wordt gedoeld op degene die in fysieke of in maatschappelijke zin alle elementen van de delictsomschrijving vervult (Kelk, 1998, p. 329).

Vervolgens geldt de eis dat de misdrijven gezien hun aard of de samenhang met andere misdrijven die worden beraamd of gepleegd in het georganiseerd verband, een ernstige inbreuk op de rechtsorde dienen op te leveren. De 'aard van het misdrijf' ziet op de ernst van de vermoedelijk gepleegde of vermoedelijk beraamde misdrijven en de omstandigheden waaronder deze zijn gepleegd (Buruma, Goos en Michels, 2003, p. 66). Met de 'samenhang' wordt gedoeld op de minder ernstige feiten die toch een ernstige inbreuk op de rechtsorde opleveren juist door de combinatie met andere misdrijven. Van een ernstige inbreuk op de rechtsorde is sprake wanneer de misdrijven door hun omvang en de gevolgen voor de samenleving het rechtsgevoel van burgers in die samenleving ernstig schokken. Onder deze categorie misdrijven vallen bijvoorbeeld drugshandel en mensenhandel.

De tweede categorie zijn de misdrijven waarop naar de wettelijke omschrijving een gevangenisstraf staat van acht jaar of langer. Aan de registratie van persoonsgegevens ten aanzien van deze categorie misdrijven zijn verder geen aanvullende eisen verbonden. De misdrijven zijn naar hun aard al voldoende ernstig zodat de wetgever aanvullende eisen niet nodig achtte. Het gaat bij deze categorie om ernstige misdrijven, zoals moord en diefstal met geweldpleging.

De derde categorie wordt gevormd door een flexibele lijst misdrijven die in feite een aanvulling vormt op de eerste categorie. Deze zogenaamde art. 67-gevallen kunnen nader worden omschreven bij een algemene maatregel van bestuur. In art. 3:1 Bpolg zijn deze misdrijven omschreven. Als aanvullend criterium voor deze misdrijven geldt dat zij gezien hun aard of de samenhang met andere door betrokkene begane misdrijven, een ernstige inbreuk op de rechtsorde opleveren. Het belangrijkste verschil ten opzichte van de eerste categorie is dat hier niet de eis van het beramen of plegen in georganiseerd verband geldt. Het gaat dan bijvoorbeeld om misdrijven tegen de zeden, ambtelijke corruptie, en valsheid in geschrifte.

De vierde catergorie is nieuw ten opzichte van de Wpolr en betreft de verwerking van politiegegevens met het oog op het verkrijgen van inzicht in de betrokkenheid van personen bij handelingen die kunnen wijzen op het beramen of plegen van bij algemene maatregel van bestuur aangewezen misdrij-

ven. Het betreft hier de zogenaamde themaverwerking. In art. 3:2 Bpolg is bepaald dat het gaat om terroristische misdrijven, mensenhandel en mensensmokkel. Met deze bepaling zal naar verwachting de omvang van de gegevensverwerking bij de CIE behoorlijk toenemen. Het betreft hier immers een zeer ruime norm. Met het verzamelen van informatie over de "betrokkenheid bij *handelingen* die kunnen wijzen op (...)" kan met enige creativiteit zeer veel informatie onder het bereik van dit artikel worden gebracht. Gedacht kan worden aan informatie over personen die vlieg- of duiklessen nemen, met de mogelijke bedoeling om aanslagen te plegen. Maar het kan ook gaan om allerlei informatie over handelingen die personen verrichten op Internet. Kortom het ligt in de lijn van de verwachtingen dat de verwerking van informatie bij de CIE en het aantal geregistreerde subjecten aanzienlijk zal toenemen. Ook dat vraagt ons inziens om effectieve privacywaarborgen ten aanzien van de geautomatiseerde gegevensverwerking en uitwisseling. Wij komen daar in hoofdstuk 6 op terug.

In de Wpolg zijn onder art. 10 ook de gegevensverwerking door de Regionale Inlichtingendiensten (RID) gebracht. In ons onderzoek beperken wij ons echter tot de CIE en daarom bespreken wij hier verder niet de gegevensverwerking door de RID.

Ad B: Drie categorieën van personen
In art. 10 Wpolg (voorheen art. 13a Wpolr) wordt bepaald dat naast de registratie van de betrokken ambtenaren van politie ten aanzien van drie soorten personen gegevens kunnen worden geregistreerd. De waarborgende werking die hiervan uitgaat, is gelegen in het feit dat de CIE niet willekeurig personen mag registreren.

De eerste categorie wordt gevormd door de 'verdachten'. Het gaat dan om personen "te wiens aanzien uit feiten en omstandigheden een redelijk vermoeden van schuld aan enig strafbaar feit voortvloeit."[70]

De tweede categorie van personen betreft de 'betrokkenen'. Dit zijn personen die nog geen verdachte zijn maar ten aanzien van wie wel een redelijk vermoeden bestaat dat zij betrokken zijn bij het beramen of plegen van misdrijven. Het is echter onduidelijk wanneer nu precies sprake is van een dergelijk vermoeden. Vast staat dat het vermoeden in ieder geval niet louter op een speculatie mag berusten. Wanneer het bijvoorbeeld gaat om een persoon die meer dan incidenteel contact heeft met een criminele organisatie kan deze als betrokkene worden geregistreerd.[71] Verder merkt de wetgever expliciet in de Memorie van Toelichting op dat er voor het vermoeden sprake moet zijn van betrekkelijk betrouwbare informatie. Informatie afkomstig van

70 Art. 27 lid 1 Sv.
71 *Kamerstukken II* 1996/97, 25 398, nr. 3, p.7.

een onbekende of onbetrouwbare bron is daarvoor onvoldoende en mag niet worden opgeslagen in het register zware criminaliteit.[72]

De derde categorie wordt aangeduid met het begrip 'relaties'. Het gaat hier om een redelijk ruime categorie aangezien het personen betreffen die in een bepaalde relatie staan tot de verdachten of betrokkenen. Dit kunnen bijvoorbeeld kennissen of vrienden van de verdachte of betrokkene zijn. Daarmee biedt de Wpolg bijzonder ruime mogelijkheden tot het registreren van personen. Onder het wettelijk regime van de Wpolr werd in art. 6 lid 2 van het Modelreglement nog wel een beperking aangebracht in de soort gegevens die van 'relaties' kunnen worden geregistreerd. Deze beperking is in de Wpolg losgelaten waarmee opnieuw een wettelijke privacywaarborg is komen te vervallen.

3.6 Wettelijk verstrekkingsregime

De Wpolr en het Bpolr kenden twee verstrekkingenregimes die wij hierna aanduiden met het algemeen en het bijzonder verstrekkingenregime.[73] Het algemene verstrekkingenregime gold in beginsel voor alle politieregisters. Het bijzondere verstrekkingenregime was van toepassing op het voorlopig register en op een gedeelte van het register zware criminaliteit. Met het vervallen van het onderscheid tussen het voorlopig register en het register zware criminaliteit in de Wpolg wordt ook geen onderscheid meer gemaakt tussen het algemene en het bijzonder verstrekkingregime. In de onderzoeksperiode golden deze regimes echter nog wel en daarom bespreken wij beide regimes.

In subsectie 3.5.2 is duidelijk geworden dat binnen het register zware criminaliteit onderscheid moet worden gemaakt tussen de registratie van 'verdachten en betrokkenen' enerzijds en de registratie van 'relaties' anderzijds. Op de registratie van 'verdachten en betrokkenen' is het algemeen verstrekkingenregime van toepassing en op de registratie van 'relaties' is het bijzonder verstrekkingenregime van toepassing. In deze sectie gaan wij allereerst in op het bereik van het begrip 'verstrekken' (subsectie 3.6.1). Vervolgens worden het algemeen verstrekkingenregime (subsectie 3.6.2) en het bijzonder verstrekkingenregime (subsectie 3.6.3) behandeld. Daarna besteden wij in subsectie 3.6.4 kort aandacht aan de protocolplicht en bespreken wij in subsectie 3.6.5 de bijzondere weigeringsgrond. In subsectie 3.6.6 geven wij tenslotte inzicht in het verstrekkingsregime onder de Wpolg en de verschillen met de Wpolr.

72 Gegevens van een onbekende of onbetrouwbare bron konden vroeger wel in aanmerking komen voor registratie in het voorlopig register. Zie subsectie 3.5.1.

73 *Kamerstukken II* 1996/97, 25 398, nr. 3.

3.6.1 Het begrip 'verstrekken'

De wetgever heeft bij het bepalen van de reikwijdte van het verstrekkingsbegrip aansluiting gezocht bij de definitie van 'verstrekken' zoals die voorkwam in de toenmalige Wet Persoonsregistratie. Deze wet kende evenals de huidige Wbp, een bijzonder ruime definitie. In de definitiebepaling van art. 1 lid 1 sub h Wpolr wordt 'verstrekken' als volgt omschreven.

> "Het bekend maken of ter beschikking stellen van persoonsgegevens, voor zover zulks geheel of grotendeels steunt op gegevens die in dat politieregister zijn opgenomen, of die door de verwerking daarvan, al dan niet in verband met andere gegevens, zijn verkregen."

Onder de Wpolg wordt in art. 1 sub d het verstrekken van politiegegevens gedefiniëerd als het bekend maken of ter beschikking stellen van politiegegevens. Vervolgens is in sub e van datzelfde artikel het ter beschikking stellen omschreven als het verstrekken van politiegegevens aan personen die overeenkomstig deze wet zijn geautoriseerd voor het verwerken van politiegegevens.

Uit beide definities blijkt dat de *wijze van verstrekken* van gegevens op zichzelf niet van betekenis is.[74] Door de ruime definitiebepaling worden in beginsel alle mogelijke verstrekkingen onder het bereik van de Wpolg gebracht hetgeen onder de Wpolr ook het geval was (Van Ruth en Scheuder, 2001, p. 50). Dit heeft echter ook tot gevolg dat de wetgever daarmee impliciet ruimte laat aan de politiepraktijk om zelf aan de wijze van verstrekken vorm te geven. In ons onderzoek naar de CIE-praktijk maken wij onderscheid tussen twee verschijningsvormen.

De eerste verschijningsvorm betreft de rechtstreekse toegang. Daarbij hebben politieambtenaren met een CIE-status zelf toegang tot het betreffende politieregister en kunnen zij de daarin opgeslagen informatie doorzoeken en raadplegen. Bij geautomatiseerd gevoerde registers wordt deze toegang geregeld via verschillende autorisatieniveaus en bij fysiek gevoerde registers kan dat door de betreffende politieambtenaar rechtstreeks toegang te geven tot de mappen waarin de registers worden onderhouden.

De tweede verschijningsvorm betreft het verstrekken van informatie aan een ontvanger die zelf geen rechtstreekse toegang heeft tot het register. Het gaat dan om mondelinge en schriftelijke verstrekkingen maar ook kan worden gedacht aan verstrekkingen door middel van het overhandigen van gegevensdragers (floppydisk of cd-rom). Van Ruth en Schreuder (2001, p. 51) wijzen er in dit verband op dat aan personen die weliswaar niet geautoriseerd

74 *Kamerstukken II* 1984/85, 19 095 nrs. 1-3, p.36.

zijn tot geautomatiseerde politieregisters toch op elektronische wijze gegevens kunnen worden verstrekt.

> "Dergelijke verstrekkingen vinden dan wel rechtstreeks langs geautomatiseerde weg plaats maar de ontvanger heeft hierbij geen rechtstreekse toegang tot het register van waaruit de gegevens afkomstig zijn."[75]

Het verstrekkingenbegrip laat ruimte voor het op elektronische wijze verstrekken van gegevens aan niet-geautoriseerde personen. Het (oude) Bpolr legt echter wel beperkingen op ten aanzien van het rechtstreeks langs geautomatiseerde weg verstrekken van gegevens.[76] Slechts een beperkte categorie van ambtenaren komt voor deze elektronische wijze van verstrekken in aanmerking. De beheerder moet hen voorzien van een schriftelijke autorisatie voor een bepaald omschreven doel. De bepaling gold als een extra waarborg voor een rechtstreekse uitwisseling met behulp van software.

3.6.2 Algemene gesloten verstrekkingenregime

Het algemene gesloten verstrekkingenregime was onder de Wpolr neergelegd in de artikelen 14 t/m 18. Het sluitstuk van dit systeem werd gevormd door art. 30 Wpolr waarin een geheimhoudingsplicht was neergelegd voor een ieder die binnen het regime van de Wpolr gegevens verstrekt had gekregen. Het verstrekken van informatie buiten de wettelijke regeling is verboden en kan aanleiding geven tot disciplinaire maatregelen wegens plichtsverzuim. In het uiterste geval kan het leiden tot een strafvervolging wegens een schending van de geheimhoudingsplicht.[77]

Evenals de Wpolr kent de Wpolg binnen het verstrekkingenregime zowel een mogelijkheid als een plicht tot het verstrekken van informatie. De mogelijkheid om gegevens te verstrekken wordt aangegeven met de zinsnede "politiegegevens kunnen (…) worden verstrekt". De verantwoordelijke heeft daarbij een zekere beoordelingsvrijheid in het al dan niet verstrekken van gegevens. Hij kan gegevens verstrekken maar hij is daartoe niet verplicht.

Bij de mogelijkheid tot het verstrekken is in art. 17 Wpolg bijvoorbeeld een verstrekking neergelegd aan de inlichtingen- en veiligheidsdiensten. Het betreft een spiegelbepaling van art. 62 Wiv 2002. In de Wiv 2002 is de verplichting neergelegd voor politieambtenaren om gegevens die zij van belang achten voor de beide inlichtingen- en veiligheidsdiensten[78], via de korpschef

---

75 Registratiekamer, 3 april 1996, nr. 96.V.186.01.
76 Art. 17 lid 1 Bpolr.
77 *Kamerstukken II* 1985/86, 19 589, nr. 3, p.9.
78 Het gaat hier ingevolge art. 1 sub a Wiv 2002 om de Algemene Inlichtingen- en Veiligheidsdienst en de Militaire Inlichtingen- en Veiligheidsdienst.

ter beschikking te stellen aan de diensten. In de praktijk verlopen deze verstrekkingen via de RID. Ambtenaren van de RID verrichten ingevolge art. 60 Wiv 2002 feitelijk de werkzaamheden ten behoeve van de AIVD. De RID-registers vallen niet onder het bereik van de Wpolr omdat de RID geen werkzaamheden verricht ter uitvoering van de politietaak, maar werkzaamheden ingevolge de Wiv 2002. Het tweede lid van art. 15 Wpolr heeft zodoende geen zelfstandige betekenis maar vormt in combinatie met art. 62 Wiv 2002 de formeel-wettelijke grondslag voor de verstrekkingen uit een politieregister aan de inlichtingen- en veiligheidsdiensten.

Voor verstrekkingen binnen de politieorganisatie geldt echter een *verstrekkingsplicht*. Deze plicht blijkt uit de zinsnede: "politiegegevens worden (…) verstrekt (…)". Aan de verplichting wordt een aantal voorwaarden verbonden. Wanneer er aan deze voorwaarden is voldaan bestaat er in beginsel een plicht van de verantwoordelijke tot het verstrekken van de gegevens. De Memorie van Toelichting zegt dat de achtergrond van het verplichtende karakter is gelegen in de aanname dat de politieorganisatie vanuit het oogpunt van (interregionale) gegevensverstrekking gezien moet worden als één organisatie.[79] Een verplichting tot het verstrekken van gegevens heeft zodoende tot doel het voorkomen van ongewenste concurrentie tussen politieonderdelen maar ook het bevorderen van de samenwerking tussen de politieregio's.

Tegenover de verplichting tot het verstrekken staat een claim van de ontvangstgerechtigde. Als is voldaan aan de materiële voorwaarden, dan heeft de ontvangstgerechtigde een claim tot het ontvangen van de informatie. Deze juridische modaliteit roept vragen op met betrekking tot de afhandeling van informatieverzoeken en de toetsing van het verzoek aan de voorwaarden. In hoeverre dient de verstrekker een verzoek te toetsen en mag hij het verzoek weigeren? Deze toetsing staat namelijk tegenover het uitgangspunt van de wetgever dat de politie met betrekking tot de gegevensverstrekking geacht wordt samen te werken en als één geheel moet worden gezien.[80] Dit brengt met zich mee dat binnen de politieorganisatie moet worden uitgegaan van interregionale openheid en vrij verkeer van informatie. Een te strikte toetsing aan de voorwaarden zou dit in de weg kunnen staan. Van Ruth en Schreuder (2003) menen dat de verstrekker in zijn algemeenheid niet bevoegd is zelf ten gronde te beoordelen of de gevraagde gegevens inderdaad nodig of noodzakelijk zijn in verband met de taak of werkzaamheden waarvoor deze worden gevraagd.[81] De verstrekking dient bijvoorbeeld wel achterwege te blijven indien moet worden aangenomen dat de

79 *Kamerstukken II* 1988/89, 19 589, nr. 6 p. 3 & p.11.
80 *Kamerstukken II* 1988/89, 19 589, nr.6 p. 3 en 11.
81 In de Wpolr wordt voor 'nodig' de term behoeven gebruikt, zie bijvoorbeeld art. 15 lid 1 Wpolr. Noodzakelijk wordt o.a. gebruikt in art. 14 lid 1 sub c en e Bpolr.

gevraagde gegevens in redelijkheid niet nodig, noodzakelijk of onvermijdelijk zijn, in verband met de uitoefening van de taak waarvoor deze zijn gevraagd (Van Ruth en Schreuder, 2003, p. 53). Het betreft zodoende een marginale toetsing door de verstrekker.

3.6.3 Het bijzonder verstrekkingenregime

De Wpolr kende naast het algemene verstrekkingenregime een bijzonder verstrekkingenregime dat van toepassing was op het voorlopig register en op de persoonsgegevens over 'relaties' die staan opgenomen in het register zware criminaliteit. Het regime kenmerkte zich door een aanzienlijk striktere verstrekkingsbepalingen dan in het algemeen verstrekkingenregime. Verstrekking voor operationele doeleinden waren uitdrukkelijk uitgesloten. De reden daarvoor is gelegen in de aard van de gegevens. Omtrent de juistheid en de betrouwbaarheid daarvan kan immers vaak (nog) geen oordeel worden gevormd. In de Wpolg is het bijzondere verstrekkingenregime komen te vervallen.

Bij een doelgebonden verstrekking mogen gegevens slechts worden verstrekt met het oog op het doel waarvoor het register is aangelegd.[82] De doelgebonden verstrekking is zowel op het voorlopig register als op de 'relaties' in het register zware criminaliteit van toepassing. In subsectie 3.5.1 is reeds aan de orde gekomen dat het doel van het voorlopig register het verrijken van informatie is waarmee wordt bedoeld het vaststellen of de persoonsgegevens opgenomen kunnen worden als subject in het register zware criminaliteit. De verstrekking van gegevens wordt verder beperkt doordat slechts de gegevens mogen worden verstrekt die nodig zijn voor de identificatie. Het gaat dan uitsluitend om gegevens die de ontvanger in staat stelt om met een behoorlijke mate van zekerheid vast te stellen om welke persoon het gaat (cf. Buruma, Goos en Michels, 2003, p. 201). De ontvanger mag deze gegevens niet vastleggen in enig ander register.

3.6.4 Protocolplicht

Zowel de oude Wpolr als de huidige Wpolg kennen een protocolplicht. Dit betekent onder de huidige Wpolg dat iedere verstrekking uit het register zware criminaliteit in beginsel moet worden geregistreerd. De Wpolg spreekt in art. 32 lid 1 sub d over de *schriftelijke* vastlegging van verstrekkingen. Het doel van deze bepaling is gelegen in het feit dat registratie van verstrekkingen nodig is om achteraf controle op de uitwisseling van politiegegevens te kunnen uitoefenen. De protocolplicht voor het register zware criminaliteit

82 *Kamerstukken II* 1996/97, 25 398, nr. 3, p.10.

geldt voor alle verstrekkingen van dat register met uitzondering van de verstrekkingen aan de inlichtingen- en veiligheidsdiensten. Van deze verstrekkingen wordt nooit aantekening bij gehouden. Van de overige verstrekkingen wordt de identiteit van de ontvanger, het doel van de verstrekking, en de verstrekkingsdatum vastgelegd.

3.6.5 De weigeringsgrond

De wetgever heeft ruimte gelaten om informatie die is opgeslagen in het register zware criminaliteit vergaand binnen de politieorganisatie af te schermen. Dat was onder de Wpolr zo en die mogelijkheid tot afschermen is in de Wpolg overgenomen. Daarvoor is in de bepalingen voor dit register een bijzondere weigeringsgrond opgenomen. De voorwaarde om te voldoen aan de weigeringsgrond is evenals de verstrekkingen gekoppeld aan de uitvoering van de politietaak. Op deze manier worden CIE-en in staat gesteld om de identiteit en overige gegevens met betrekking tot informanten af te schermen.[83] Wanneer er geen noodzaak bestaat tot het weigeren van de verstrekking, dan kunnen er beperkende voorwaarden worden gesteld. Dergelijke voorwaarden zijn bedoeld om grenzen te stellen aan het verdere gebruik van de verstrekte informatie. In de praktijk wordt veel gebruik gemaakt van de voorwaarde dat informatie pas operationeel gebruikt mag worden na overleg met de verstrekker. Zodoende behoudt de verstrekker enige mate van controle over de informatie.

De bevoegdheid om een verstrekking te weigeren geldt ingevolge art. 16 lid 2 Wpolg niet voor gezagdragers. Dit betekent dat de verstrekking van gegevens niet kan worden geweigerd aan de burgemeester in zijn hoedanigheid als korpsbeheerder en het openbaar ministerie. Wel kan verstrekking geweigerd worden aan burgemeesters en korpschefs die in het kader van de Wet Wapens en Munitie en de Wet particuliere beveiligingsorganisaties en rechercheburéaus om informatie vragen. Datzelfde geldt ook voor de commandant van de Koninklijke Marechaussee waarbij tegenover hem eveneens verstrekkingsverzoeken in het kader van art. 37s Luchtvaartwet mogen worden geweigerd.

Onder de Wpolr deed zich een merkwaardige situatie voor ten aanzien van de personen en instanties die belast zijn met een publieke taak. Deze categorie van personen die in aanmerking komen voor verstrekkingen valt namelijk niet onder het bereik van de weigeringsgrond. Buruma (2005, p. 205) stelt dat uit de expliciete uitzondering op de weigeringsgrond die geldt ten aanzien van het Meldpunt Ongebruikelijke Transacties (MOT), afgeleid zou kunnen worden dat de weigeringsgrond ook geldt ten aanzien van personen

83 K*amerstukken II* 1996/97, 25 398, nr. 6, p.33.

en instanties die evenals het MOT zijn belast met een publieke taak. Daarentegen kan worden betoogd dat met het verstrekken van gegevens aan deze personen en instanties geen operationeel risico wordt gelopen omdat deze niet belast zijn met de uitvoering van de politietaak. De wetgever liet over de precieze uitleg van de weigeringsgrond echter onduidelijkheid bestaan. Onder de Wpolg is deze onduidelijkheid weggenomen doordat voor deze verstrekkingen in beginsel niet meer de plicht tot verstrekken geldt maar de mogelijkheid. De verantwoordelijke heeft ten aanzien van deze verstrekkingen dus een zekere mate van beoordelingsvrijheid.

3.6.6 Verstrekkingenregime in de Wpolg (2008)

Voor de goede orde vatten wij in deze subsectie de belangrijkste veranderingen die zich in de loop van het onderzoek hebben voorgedaan in het wettelijk regime samen. Op 1 januari 2008 is de Wpolg tezamen met het uitvoeringsbesluit, het Besluit Politiegegevens (Bpolg) in werking getreden. Met deze herziening heeft de wetgever beoogd meer ruimte te bieden dan de Wpolr deed voor het verwerken van politiële gegevens ten behoeve van een zo goed mogelijke uitvoering van de politietaak.[84] Allereerst is er in de Wpolg een groot aantal wijzigingen van wettechnische aard doorgevoerd. Zij moeten de wet toegankelijker en begrijpelijker maken voor onder andere het politiedomein. Op een aantal punten zijn er ook inhoudelijk *normen* gewijzigd. Deze wijzigingen bespreken wij hieronder in de vorm van (1) algemene veranderingen, (2) veranderingen in de opnamecriteria, (3) vijf verschillen in het verstrekkingenregime.

Algemene veranderingen
De algemene veranderingen zijn samen te vatten in het verminderen van de administratieve last en het overzichtelijker worden van de regelingen. Het wegvallen van het onderscheid tussen de verschillende soorten registers heeft echter ook tot gevolg dat het in sectie 3.5 besproken onderscheid tussen het voorlopig register en het register zware criminaliteit komt te vervallen. Dit heeft tot gevolg dat gegevens die vroeger werden geregistreerd in de voorlopige registers, onder de Wpolg vallen onder het regime van het 'register zware criminaliteit'.

In de plaats van de regulering van de verschillende politieregisters hanteert de Wpolg een systematiek die uitgaat van vijf doelen waarvoor gegevensverwerking mogelijk is, te weten:

84 *Kamerstukken II* 2005/06, 30 327, nr. 3.

1. de uitvoering van de dagelijkse politietaak (art. 8 Wpolg);
2. het onderzoek in verband met de handhaving van de rechtsorde in een bepaald geval (art. 9 Wpolg);
3. het inzicht in de betrokkenheid van personen bij bepaalde ernstige bedreigingen van de rechtsorde (art. 10 Wpolg);
4. het beheer van informanten (art. 12 Wpolg);
5. de ondersteunende taken (art. 13 Wpolg).

In deze vijf doelen zijn de oude politieregisters uit de Wpolr nog herkenbaar. In de Wpolg vallen het voorlopig register en het register zware criminaliteit onder gegevensverwerking binnen het derde doel, het verkrijgen van inzicht in de betrokkenheid van personen bij bepaalde ernstige misdrijven. Onder de Wpolr werden het register zware criminaliteit en het voorlopig register gebruikt voor dat doel. Het belangrijkste verschil tussen de Wpolg en de Wpolr is dat in de Wpolg dit doel nu expliciet is benoemd. Uit de formulering van art. 10 Wpolg, verkrijgen van inzicht, blijkt dat de verwerking van personagegegevens is gericht op het opbouwen en in stand houden van een min of meer permanente informatiepositie. Met deze informatiepositie wordt beoogd ontwikkelingen en verschijnselen als zware criminaliteit, terrorisme, en andere bedreigingen van de rechtsorde in kaart te brengen en te volgen. De opbouw van een informatiepositie en de daarbij behorende gegevensverwerking heeft in strafvorderlijke zin een proactieve functie. De verwerking mag slechts plaatsvinden door speciaal daarvoor geautoriseerde politieambtenaren.[85] Dit zijn de ambtenaren die werkzaam zijn voor de regionale CIE en RID.

Veranderingen in de opnamecriteria
De algemene opnamecriteria blijven in het nieuwe regime op hoofdpunten ongewijzigd. In art. 3 Wpolg wordt de koppeling gemaakt naar de doeleinden voor gegevensverwerking. De Wpolg is op dit punt specifieker dan de Wpolr. Expliciet wordt vermeld dat gegevensverwerking:

> "(…) gelet op de doeleinden waarvoor zij worden verwerkt, toereikend, ter zake dienend en niet bovenmatig zijn."

Daarmee sluit de wet aan bij de in sectie 3.2 besproken beginselen van het Europees Databeschermingsverdrag. Op de verantwoordelijke voor de gegevensverwerking rust zodoende de zorgplicht om 'passende' organisatorische en technische maatregelen te nemen. Verder gelden vergelijkbare bepalingen voor de rechtmatigheid van de gegevensverwerking en de verwerking van gevoelige gegevens.

85 *Kamerstukken II* 2005/06, 30 327, nr. 3, p.96.

Wat de bijzondere opnamecriteria betreft zijn de veranderingen eveneens gering. In de Wpolg komt de verwerking van zware criminaliteitsgegevens als gezegd te vallen onder het regime van art. 10 Wpolg. Daarin gaat het om misdrijven of handelingen die een ernstige bedreiging vormen voor de rechtsorde. In deze bepaling worden evenals in de Wpolr categorieën van misdrijven en personen als aangrijpingspunt genomen voor de verwerking van gegevens. In art. 10 lid 1 sub a Wpolr is daarom het CIE-criterium overgenomen uit de Wpolr. Nieuw ten opzichte van de Wpolr is de mogelijkheid voor de politie om themaregisters aan te leggen. In deze themaregisters kunnen gegevens worden opgeslagen over groepen van onverdachte personen ten aanzien van wie aanknopingspunten bestaan dat zij betrokken zijn bij handelingen die kunnen wijzen op het beramen, voorbereiden, of plegen van misdrijven die verband houden met het te onderzoeken thema.[86] Bij AMvB worden de categorieën van misdrijven vastgelegd waaromtrent themaregisters kunnen worden aangelegd. De Wpolg stelt voor deze categorieen van misdrijven dat het moet gaan om misdrijven die door hun omvang of ernst of hun samenhang met andere misdrijven een ernstig gevaar voor de rechtsorde opleveren.[87] Het zal dan gaan om gegevens betreffende terroristische misdrijven en delicten als mensenhandel. De themaregisters vormen een significante uitbreiding ten opzichte van het huidige regime omdat grotere groepen onverdachte personen kunnen worden geregistreerd (zie Kielman en Koelewijn, 2005).

Tenslotte zijn ook de registraties van de RID in de Wpolg voorzien van een formeel-wettelijke grondslag. In dit onderzoek hebben wij ons echter beperkt tot de registers die gevoerd worden bij de CIE-en.

Vijf verschillen in het verstrekkingenregime
Het verstrekkingenregime van de Wpolr wordt in zoverre gehandhaafd dat er ook in de Wpolg een onderscheid gemaakt wordt tussen verstrekkingen binnen de politieorganisatie en verstrekkingen buiten de politieorganisatie. Er zijn echter vijf verschillen ten opzichte van het verstrekkingenregime in de Wpolr die van belang zijn voor dit onderzoek.

Het eerste verschil heeft te maken met de definiëring van 'verstrekken'. Onder de nieuwe wet is verstrekken "het bekend maken of ter beschikking stellen van politiegegevens." Vervolgens wordt het 'ter beschikking stellen van politiegegevens' gedefinieerd als het verstrekken aan personen die overeenkomstig deze wet zijn geautoriseerd voor het verwerken van politiegegevens. Het verstrekken van politiegegevens binnen de politieorganisatie is blijkens art. 15 Wpolg gekoppeld aan een autorisatie door een verantwoordelijke. Daarmee beoogt de wetgever te anticiperen op de verdere automati-

86 *Kamerstukken II* 2005/06, 30327, nr. 3, p. 38.
87 Art. 10 lid 1 sub b Wpolg.

sering van het gegevensverwerkingsproces. Voor het onderzoek naar software-toepassingen betekent dit dat verstrekken met behulp van softwareagenten binnen het regime van de Wpolg slechts is toegestaan voorzover gebruikers van de softwareagenten geautoriseerd zijn door de verantwoordelijke (zie: Koelewijn en Kielman, 2006).

Het tweede verschil is het wegvallen van het onderscheid tussen een algemeen verstrekkingenregime en een (beperkter) bijzonder verstrekkingenregime. Deze verandering hangt samen met het wegvallen van het voorlopig register. Dit heeft tot gevolg dat de 'zeer zachte' gegevens, die onder de Wpolr opgeslagen lagen in het voorlopig register, in de Wpolg komen te vallen onder het algemene verstrekkingenregime. Datzelfde geldt voor gegevens die in het register zware criminaliteit worden opgeslagen met betrekking tot 'relaties'. De wijziging heeft tot gevolg dat deze gegevens onder de Wpolg dus wel voor operationele doeleinden verstrekt kunnen worden en dat vormt een aanmerkelijke uitbreiding.

Het derde verschil is gelegen in de categorieën van ontvangstgerechtigden. In de Wpolg wordt voor iedere categorie het verstrekkingenregime uitgebreid met de mogelijkheid om zowel structureel als incidenteel politiegegevens te verstrekken aan personen en instanties met het oog op bepaalde omschreven doeleinden. De doeleinden (het voorkomen en opsporen van strafbare feiten, het handhaven van de openbare orde, het verlenen van hulp aan hen die deze behoeven, of het uitoefenen van toezicht op het naleven van regelgeving) sluiten nauw aan bij de politietaak. De uitbreiding betreft de voorwaarde dat dergelijke verstrekkingen uitsluitend kunnen plaatsvinden met het oog op een zwaarwegend algemeen belang. In de Memorie van Toelichting wordt aangegeven dat daarvan al sprake is wanneer de verstrekking voor de samenleving van meer dan gewone betekenis is.[88] Tenslotte kan de beslissing tot het verstrekken alleen plaatsvinden in overeenstemming met het bevoegde gezag.

Het vierde verschil heeft te maken met het uitgangspunt van de Wpolr dat de verstrekking van gegevens uit een politieregister in beginsel plaatsvindt door tussenkomst van een ambtenaar van politie. Slechts ten aanzien van de meest voorkomende verstrekkingen, welke noodzakelijk zijn voor de goede uitvoering van de politietaak, kan aan een beperkte categorie ambtenaren gegevens rechtstreeks en geautomatiseerd worden verstrekt. In de Wpolg wordt deze mogelijkheid aanzienlijk verruimd. De Memorie van Toelichting overweegt in dat verband:

88 *Kamerstukken II* 2005/06, 30 327, nr. 3, p. 58.

> "Rekeninghoudend met de technische ontwikkelingen, en ook gelet op de ontwikkeling van de bovenregionale informatiehuishouding binnen de politie, kan de verantwoordelijke ervoor kiezen de politiegegevens rechtstreeks en geautomatiseerd beschikbaar te stellen aan ambtenaren die vallen onder het beheer van een andere verantwoordelijke."[89]

Gelet op de internationale ontwikkelingen betreffende de intensivering van grensoverschrijdende politiële samenwerking, zoals vastgelegd in het verdrag van Prüm[90], verwachten wij dat binnen afzienbare tijd ook de internationale uitwisseling van informatie hoe langer hoe meer rechtstreeks en geautomatiseerd zal gaan plaatsvinden.

Het vijfde verschil heeft te maken met de weigeringsgrond. In tegenstelling tot de Wpolr kent de verwerking van gegevens met betrekking tot zware (georganiseerde) criminaliteit geen bijzondere weigeringsgrond meer. In de plaats daarvan is een algemene weigeringsgrond opgenomen voor alle verstrekkingen. Deze luidt:

> "In bijzondere gevallen kan, indien dit noodzakelijk is voor een goede uitvoering van de politietaak, de terbeschikkingstelling van politiegegevens door de verantwoordelijke worden geweigerd dan wel kan de verantwoordelijke beperkende voorwaarden stellen aan de verdere verwerking."

De zinsnede 'in bijzondere gevallen' is toegevoegd aan de weigeringsgrond. Met deze toevoeging geeft de wetgever aan dat weigering niet tot een algemene gedragslijn mag verworden maar alleen in uitzonderingsgevallen is toegestaan. Onder de Wpolr is de weigeringsgrond bij CIE-en in de loop van de tijd verworden tot een algemene gedragslijn. Onder de Wpolg is dat duidelijk niet meer de bedoeling.

3.7 Beantwoording tweede onderzoeksvraag

In dit hoofdstuk stond de tweede onderzoeksvraag (OV 2) centraal die luidt: Op welke wijze heeft de wetgever de uitwisseling van criminele inlichtingen genormeerd? Wij geven hieronder het antwoord tezamen met ons commentaar. In subsectie 3.7.1. bespreken wij kort de vier leidende rechtsbeginselen voor de uitwisseling van criminele inlichtingen en in subsectie 3.7.2 gaan wij in op de normatieve beperkingen en de bedreigingen voor de privacy.

89 *Kamerstukken II* 2005/06, 30 327, nr. 3, p. 59.

90 *Trb.* 2005, 197; Goedkeuringswet in Stb. 2008, 25; inwerking gereden op 20 februari 2008, *Trb*. 2008, 74.

3.7.1 Vijf leidende rechtsbeginselen

Het antwoord op deze onderzoeksvraag is duidelijk. De wetgever is bij de wijze van normering van de gegevensverwerking door de politie niet volledig vrij maar gebonden aan internationale rechtsbeginselen die onder meer zijn vastgelegd in het EVRM en het Europees Dataverdrag. Wij noemen vijf rechtsbeginselen te weten: (1) rechtmatigheid, (2) doelmatigheid, (3) proportionaliteit, (4) subsidiariteit en (5) transparantie. Hiermee beschrijven wij het juridisch kader waarbinnen we in het ANITA-project de normatieve multiagenttoepassingen ontwikkelen.

Rechtmatigheid
Het rechtmatigheidsbeginsel houdt in dat de gegevensverwerking door de politie, en daaronder valt ook de gegevensuitwisseling, uitsluitend mag plaatsvinden met gegevens die rechtmatig zijn verkregen. Wij hebben vastgesteld dat in het huidige systeem van rechtsbescherming de rechtmatigheidstoets pas achteraf plaatsvindt of kan plaatsvinden door de rechter. In het licht van de technologische ontwikkelingen menen wij dat deze reactieve vorm van rechtsbescherming op termijn onvoldoende de privacy van betrokkenen zal kunnen waarborgen.

Doelmatigheid
Het doelmatigheidsbeginsel betekent dat de verwerking (en daarmee uitwisseling) van gegevens gekoppeld dient te zijn aan een bepaald doel. De geregistreerde gegevens mogen slechts worden opgeslagen en verwerkt voor zover dat voor dat doel noodzakelijk is. In de huidige Wpolg is het hoofddoel nader geconcretiseerd in vijf subdoelen (zie subsectie 3.6.6). Het normerende subdoel voor de verwerking en uitwisseling van gegevens in het CIE-domein is het verkrijgen van inzicht in personen en organisaties die zich bezighouden met bepaalde categorieën van ernstige misdrijven. In beginsel is het verwerken en uitwisselen van politiegegevens in het CIE-domein, buiten dit doel, onrechtmatig. De bescherming van de privacy vloeit bij de uitwisseling van gegevens tevens voort uit de doelmatigheidstoets. Daarbij dient steeds te worden nagegaan of de uitwisseling van gegevens noodzakelijk is voor het doel.

Proportionaliteit
Het proportionaliteitsbeginsel heeft een bijzondere normerende werking op de informatie-uitwisseling in het CIE domein. Concrete toepassing van dit beginsel houdt in dat bij iedere gegevensverstrekking moet worden nagegaan of de verstrekking in een redelijke verhouding staat tot het doel dat daarmee beoogd wordt. Er moeten met andere woorden niet meer gegevens worden verstrekt dan strikt noodzakelijk is voor het doel waarvoor de gegevens gevraagd worden.

Subsidiariteit
Het subsidiariteitsbeginsel betekent voor de gegevensverwerking en uitwisseling dat er geen minder ingrijpend middel voor handen moet zijn. Er zal met andere woorden steeds moeten worden nagegaan of hetzelfde doel niet kan worden bereikt met een middel dat minder ingrijpend is dan gegevensuitwisseling of verwerking.

Transparantie
Het transparantiebeginsel houdt in dat degene die de persoonsgegevens verwerkt hierover op verzoek van de betrokkene de nodige informatie zal moeten verstrekken. In het CIE-domein speelt dit beginsel een geringe rol omdat in de praktijk vrijwel altijd inzage in de gegevens geweigerd of beperkt zal worden in het belang van de uitvoering van de politietaak (zie daarover: Kielman, 2009). Een tweede aspect van het transparantiebeginsel is het uitgangspunt dat achteraf de gegevensverwerking en uitwisseling controleerbaar dient te zijn. Om die reden dient aantekening te worden gehouden van de gegevensverstrekkingen zodat bijvoorbeeld het Cbp bij een steekproef kan toetsen of de uitwisseling rechtmatig was.

Bovenstaande rechtsbeginselen vormen gezamenlijk het juridische kader waarbinnen de normatieve beperkingen in de informatiesystemen moeten worden ontwikkeld. De wetgever heeft deze beginselen voor een deel wel nader uitgewerkt in de wetgeving maar daarbij concepten als 'rechtmatigheid' en 'noodzakelijk' niet nader ingekleurd. Het stelsel van rechtsbescherming is thans zo ingericht dat de controle op deze beginselen een voornamelijk reactief karakter heeft. De rechter toetst pas achteraf of de verwerking dan wel uitwisseling rechtmatig was. De inbreuk op de privacy heeft dan echter al plaatsgevonden.

3.7.2 Normatieve beperkingen en de privacy

Wij hebben voorts gewezen op de snelheid waarmee de technieken zich thans ontwikkelen. Computers kunnen steeds intelligentere beslissingen nemen en een groeiende hoeveelheid data en persoonsgegevens verwerken. Daarnaast laten internationale ontwikkelingen op het gebied van de grensoverschrijdende politiële samenwerking zien dat ook in de nabije toekomst hoe langer hoe meer rechtstreeks en geautomatiseerd op internationaal niveau politiegegevens zullen worden uitgewisseld.

Deze ontwikkelingen vormen in toenemende mate een bedreiging voor de privacy van burgers en daarom kan ons inziens niet meer worden volstaan met een voornamelijk reactief systeem van rechtsbescherming. Op grond daarvan pleiten wij ervoor dat, gelet op het doel van de privacybescherming, er nadrukkelijk meer aandacht moet worden besteed aan een geautomatiseerde proactieve controle op de hierboven genoemde rechtsbeginselen en

met name op het beginsel van de rechtmatigheid. Een geautomatiseerde controle is noodzakelijk omdat, gelet op de groeiende omvang van de gegevensverwerking en op de schaalvergroting, deze controle niet meer uitsluitend door mensen kan plaatsvinden. Een mens kan nu eenmaal niet de verwerking van miljoenen persoonsgegevens controleren. Een geautomatiseerde controle zou een veel effectievere waarborging van de privacy inhouden die, gelet op de genoemde ontwikkelingen, ook noodzakelijk is. Naast deze controle moet de rechter wel het sluitstuk blijven vormen van de reactieve rechtsbescherming.

4 De Criminele inlichtingeneenheden

Dit hoofdstuk geeft een beschrijving van de criminele inlichtingeneenheden (CIE-en) die binnen de regiokorpsen verantwoordelijk zijn voor de verwerking van 'bijzondere' politiegegevens, de criminele inlichtingen.[91] Voor de definiëring van het begrip criminele inlichtingen zoeken wij aansluiting bij de CIE-regeling waarin criminele inlichtingen worden omschreven als: "gegevens die in aanmerking komen voor registratie in het register zware criminaliteit of het voorlopig register."[92] Deze definitie vormt een verbijzondering van de algemene definiëring van het begrip 'politiegegeven' zoals vastgelegd in art. 1 sub a Wpolg. Een politiegegeven is in dit artikel gedefinieerd als: "elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon dat in het kader van de uitoefening van de politietaak wordt verwerkt."

Wij beschrijven in sectie 4.1 de historische achtergronden van de CIE. In sectie 4.2 behandelen wij de taak en werkwijze. Sectie 4.3 geeft een overzicht van de verschillende wijzen waarop criminele inlichtingen worden uitgewisseld. Ten slotte trekken wij in sectie 4.4 enkele tussenconclusies.

4.1 Historische ontwikkeling van de CIE

In deze sectie gaan wij in op twee elementen in de historische ontwikkeling van de CIE-en die van belang zijn voor het onderzoek. In subsectie 4.1.1 beschrijven wij welke ontwikkeling de CIE heeft doorgemaakt als het gaat om de taakopvatting en werkwijze. Subsectie 4.1.2 handelt vervolgens over de ontwikkelingen met betrekking tot het gebruik van geautomatiseerde informatie- en registratiesystemen door de CIE.

---

91 Zie: *Stb.* 1994, 224, Besluit beheer politiekorpsen, in werking getreden op 1 april 1994.

92 Deze definitie volgt uit art. 1 sub e CIE-regeling. Het is opvallend dat ondanks de inwerkingtreding van de Wpolg op 1 januari 2008, en de daarmee samenhangende afschaffing van het registerbegrip, in de CIE-regeling uitgegaan blijft worden van het register zware criminaliteit en het voorlopig register. Dit ondersteunt onze stelling in hoofdstuk 3 inhoudende dat, ondanks de inwerkingtreding van de Wpolg, de CIE-en voorlopig blijven werken met de registerstructuur zoals die is opgezet onder de Wpolr.

4.1.1 Van CID tot CIE

In het begin van de jaren zestig van de vorige eeuw werd bij enkele gemeentepolitiekorpsen door zelfstandig opererende rechercheurs voor het eerst informatie verzameld via een persoonlijk netwerk van informanten. De informatie werd gebruikt voor recherche-onderzoeken. De informanten en de informatie werden door de rechercheurs beschouwd als hun eigendom en om die reden nauwelijks gedeeld met anderen (Aalbersberg e.a., 1993, p. 52). In de loop van de jaren zestig werd deze manier van inlichtingen vergaren bij de grotere korpsen geïnstitutionaliseerd door de oprichting van Criminele Inlichtingendiensten (CID-en). Een CID kreeg als primaire taak het zogenaamd 'runnen' van informanten om daarmee een informatiepositie op te bouwen over personen en criminele activiteiten in de regio. Met behulp van die informatiepositie werd beoogd inzicht te krijgen in het doen en laten van (potentiële) criminelen. Dit inzicht kon vervolgens worden gebruikt bij de opsporing en voorkoming van misdrijven. Kenmerkend voor deze periode was dat de CID-en zich vooral zaaksgericht ontwikkelden; de informatiepositie was daarom vooral gericht op het boeken van directe concrete resultaten in lopende recherche-onderzoeken.

In het begin van de jaren zeventig van de vorige eeuw kreeg Nederland hoe langer hoe meer te maken met een nieuw criminaliteitsfenomeen, de illegale handel in verdovende middelen (Van de Bunt, 1993). Voor de bestrijding van deze vorm van criminaliteit kwamen de politie en het openbaar ministerie langzaam maar zeker tot het inzicht dat de reguliere opsporingsmethoden onvoldoende effectief waren. De opsporingsmethoden waren tot dan toe ontwikkeld om onderzoek te doen naar misdrijven die reeds gepleegd waren. Er werd met andere woorden vooral gebruik gemaakt van reactieve opsporingsmethoden. De 'nieuwe' criminaliteit onttrok zich echter vrijwel geheel aan het blikveld van de politie doordat er nauwelijks aangifte van werd gedaan en het bovendien geen (klassieke) sporen naliet. Hierdoor waren de reactieve opsporingsmethoden weinig effectief. Voor de bestrijding van deze vorm van criminaliteit stapten rechercheurs daarom hoe langer hoe meer over op pro-actieve opsporingsmiddelen. In deze ontwikkeling ichting de pro-activering van de opsporing bleek de verwerking van inlichtingen een effectief middel voor het verkrijgen van inzicht in de illegale handel in verdovende middelen. Naast het 'runnen' van informanten werd ook informatie verkregen vanuit surveillancemeldingen en via de zogenaamde caférecherche. Bij deze laatste methode bezochten rechercheurs horecagelegenheden waar gehandeld werd in verdovende middelen. Zij probeerden vervolgens via contacten in deze cafés informatie te verzamelen over de criminele activiteiten (Aalbersberg e.a., 1993).

Binnen de politieorganisatie was het werk van CID-en omgeven door een waas van geheimzinnigheid. De CID werd daarom ook wel gekenschetst als de geheimendienst of de afdeling 'stiekem' van de politie. Dit had tot gevolg dat andere onderdelen binnen de politie niet goed op de hoogte waren van de werkzaamheden van de CID. Het zorgwekkende van deze situatie was dat er ook een kloof ontstond tussen de CID en de rechercheafdelingen ten behoeve waarvan de informatie werd verzameld. Dit leidde ertoe dat rechercheurs vaak niet wisten wat zij konden verwachten van de dienst. De CID-en schermden echter ook onderling hun informatie vergaand af. Van samenwerking en informatie-uitwisseling was in die periode dan ook nauwelijks sprake (Wilzing, 1993).

In 1981 werd een aanzet gegeven om daarin verandering aan te brengen doordat bij de Centrale Recherche Informatiedienst (CRI) de Criminele Inlichtingen Centrale (CIC) werd opgericht. Met de CIC werd beoogd de verwerking van criminele inlichtingen op een nationaal niveau te coördineren. De CIC kwam daartoe met een standaard informatieformulier met behulp waarvan criminele inlichtingen tussen de diensten konden worden uitgewisseld. Het formulier bevatte gestandaardiseerde evaluatiecodes waarmee de bron en de betrouwbaarheid van de informatie konden worden aangegeven. Bovendien werd met deze codering beoogd om ook de recherche meer aanknopingspunten te bieden bij de beoordeling van de informatiewaarde (Rademaker, 1993).

Tot ongeveer 1985 was het gebruikelijk dat informanten niet alleen door de CID maar ook door leden van de tactische recherche werden gerund. Dit had tot gevolg dat er binnen de gemeentelijke korpsen versnipperde maar veelal ook parallelle informatieposities ontstonden. In 1985 wilde het College van Procureurs-generaal daaraan een einde maken via de regeling 'Tip-, Toon- en verkoopgelden' (Aalbersberg e.a., 1993). In de regeling werd aan de CID een centrale en coördinerende rol toegekend bij het inwinnen en verwerken van informatie met behulp van informanten. In 1985 kwam de toenmalige regering met het beleidsplan 'Samenleving en Criminaliteit' waarin voor het eerst specifiek beleid werd vastgesteld voor de aanpak van georganiseerde criminaliteit.[93] In de toelichting op het beleidsplan werd geconstateerd dat de criminaliteit zich hoe langer hoe meer uitstrekte buiten de lokale grenzen van de gemeentelijke politiekorpsen hetgeen zou vragen om een verdere professionalisering van de pro-actieve opsporingsmiddelen. Om deze professionalisering te bereiken werd in het beleidsplan onder meer een landelijke CID-structuur voorgesteld om daarmee de samenwerking tussen de regionale diensten verder te stimuleren. Deze structuur werd in 1986 vastgelegd in de eerste CID-regeling waarin onderscheid werd gemaakt tussen drie organisatorische niveaus: lokaal, regionaal, en landelijk.

93 *Kamerstukken II* 1984/85, 18 995, nrs. 1-2.

(1) De lokale CID was verantwoordelijk voor het plaatselijk inwinnen en verwerken van de criminele inlichtingen.
(2) De regionale CID kreeg een verbindende, analyserende, en coördinerende taak binnen de regio.[94]
(3) De landelijke CID werd ondergebracht bij het CRI en deze dienst werd belast met de internationale uitwisseling van inlichtingen en de coördinatie op bovenregionaal niveau.

Het bleek echter veel tijd te kosten om deze structuur te implementeren omdat de politiële organisatiestructuur en de primaire verantwoordelijkheid voor het politieoptreden in deze periode op gemeenteniveau lagen. Daarnaast werd het uitwisselen van criminele inlichtingen door het merendeel van de CID-en beschouwd als een (te) groot risico voor de informanten. Ondanks de herstructureringspogingen bleef de CID vooral georiënteerd op de eigen regio en werden slechts op zeer beperkte schaal nationaal inlichtingen uitgewisseld.[95]

Aan het einde van de jaren tachtig van de vorige eeuw verschijnt dan het rapport 'Bedrijfsmatig Onderzoek Recherche' waarin dit beeld werd bevestigd (IME Consult, 1989). De conclusies met betrekking tot de CID waren niet verrassend: (1) de CID werkte te weinig klantgericht, (2) de kwaliteit van de informatie was onvoldoende omdat te weinig werd nagedacht over de tactische haalbaarheid van onderzoeken en (3) er bestond nog steeds, met name bij de rechercheteams, te veel onbekendheid over de mogelijkheden van de CID vanwege het nog altijd aanwezige 'waas van geheimzinnigheid' (IME Consult, 1989). Langzaam maar zeker groeide ook bij de diensten het besef dat er een cultuuromslag nodig was waarbij het niet langer ging om de kwantiteit van de informatie-inwinning maar vooral om de kwaliteit en de klantgerichtheid. Om de samenwerking tussen de regionale CID-en verder te verbeteren werden op organisatorisch niveau twee maatregelen genomen.

Ten eerste stelde de diensten landelijk een zwarte lijst samen van onbetrouwbaar gebleken informanten en werden er afspraken gemaakt voor een centrale codering van informanten bij de landelijke CID. Hiermee moest worden voorkomen dat dezelfde informanten door meerdere diensten werden gerund. Dat was, en is, van belang omdat bij verificatie van de juistheid van de informatie het noodzakelijk is om te weten of dezelfde informatie niet ook van dezelfde informant afkomstig is.

94 Regio in de zin van de Basisregeling samenwerking politie van 1979.
95 Werkgroep functioneren CRI, Recherche Advies Commissie (voorz. R.B.M. Berger), Aanbevelingen ten behoeve van de verhouding tussen de CRI en zijn gebruikers, Den Haag, Recherche Advies Commissie, 1988.

Ten tweede werd er een landelijke verwijsindex ontwikkeld waarin alle regionaal geregistreerde CID-subjecten moesten worden opgenomen. Met deze index werd het mogelijk om bovenregionaal vast te stellen of er bij meerdere regionale CID-en tegelijk informatie over hetzelfde subject aanwezig was, waardoor de uitwisseling van informatie over dezelfde subjecten zou kunnen worden vergoot.

Ondanks deze maatregelen bleef de uitwisseling van informatie ook in het begin van de jaren negentig problematisch. Het belangrijkste terugkerende knelpunt was het spanningsveld dat er bestaat tussen de bronafscherming en de behoefte om opsporingsinformatie te delen. Door de regionale CID werden pogingen gedaan om te komen tot onderlinge afspraken over het gebruik van de elkaars inlichtingen. Hierdoor hoopte men het wederzijds vertrouwen te vergroten. Daarnaast bleef ook de relatie tussen de recherche en de CID in de loop van de jaren negentig van de vorige eeuw moeizaam. Door de noodzaak die de CID-en voelden om hun informatie vergaand af te schermen bleven er bij de recherche informatiekanalen bestaan die min of meer parallel liepen aan de informatiekanalen van de CID-en. Het gevolg van deze situatie was dat de recherche omgekeerd de door haar verzamelde informatie op haar beurt weer afschermde van de CID. Van een adequate informatiecoördinatie ten behoeve van de opsporing was daarom ook in het begin van de jaren negentig nauwelijks sprake.

Bij de reorganisatie van de politie en de invoering van de Politiewet 1993 ontstonden er 25 regiokorpsen en een Korps Landelijke Politiediensten (KLPD), in totaal dus 26 korpsen. Door de reorganisatie kwam het onderscheid tussen lokale en regionale CID-en te vervallen. Vanaf 1993 zijn er grofweg twee organisatievormen te onderscheiden.

De eerste vorm kwam vooral in de grote steden voor. In deze organisatievorm vond binnen het regiokorps de coördinatie en analyse van de inlichtingen plaats op centraal niveau terwijl de inwinning en de verstrekking decentraal was geregeld in districten. Voor de inwinning en de verstrekking is dan de districtsleiding verantwoordelijk.

In de tweede vorm werden alle taken van de CID op centraal niveau aangestuurd. Toch zorgde ook deze reorganisatie niet tot een betere informatieuitwisseling en interregionale coördinatie. De CID bleef ook binnen de regiokorpsen nog altijd bekend als de 'afdeling stiekem'. Illustratief voor deze gesloten CID-cultuur en de achtergrond daarvan is een uitspraak van een toenmalige CID-chef.

> "Mensen, en dat zijn informanten voor mij nog steeds, zijn gegarandeerd verzekerd van minimaal een kogel, als ik hun rol duidelijk maak. Als je met steun van het openbaar ministerie belooft dat je iemands identiteit zult beschermen, moet je dat ook doen. (…) Afspraak is afspraak. Nooit zal ik alles kunnen vertellen (Langendoen en Vierboom, 1998, p. 235)."

In diezelfde periode ontstond er enige *maatschappelijke* onrust rondom een opsporingsmethode die door de CID van de regio Kennemerland was ontwikkeld. Deze zogenaamde Delta-methode werd gebruikt binnen het interregionaal rechercheteam (IRT) Utrecht-Kennemerland en had als doel de leiding van een vermeende criminele organisatie te ontmantelen. Een informant van de CID-Kennemerland speelde in dat onderzoek een centrale rol bij het opzetten van softdrugslijnen door de CID. Met behulp van de softdrugslijnen probeerde de CID inzicht te krijgen in de handel en wandel van de criminele organisatie met het doel om bewijs te verzamelen tegen de leiding. Deze opsporingsmethode leidde tot grote politieke onrust toen onder meer bleek dat het openbaar ministerie onvoldoende controle en toezicht hield op de handelswijze van het IRT en de 'geheime' CID-trajecten. In de geheime trajecten werden onder leiding van de CID zogenaamde groeiinformanten ingezet die het vertrouwen van de criminele organisatie moesten verkrijgen door middel van het transporteren van grote hoeveelheden soft- en harddrugs. De handelswijze vormde voor de Tweede Kamer aanleiding om een parlementaire enquête te houden naar de omstreden opsporingsmethoden. De parlementaire enquêtecommissie, de Commissie Van Traa, trok in dat onderzoek ook een aantal belangrijke conclusies ten aanzien van de organisatie en het functioneren van de CID-en die nog altijd relevant zijn binnen het kader van dit onderzoek. [96]

De Commissie Van Traa concludeerde onder meer dat de verschillende toepasselijke wettelijke regimes (Wet persoonsregistraties naast de Wet politieregisters) het geheel van regelgeving voor de politieorganisatie ondoorzichtig maakte. Bovendien constateerde de commissie grote verschillen tussen korpsen bij de inrichting van de politieregisters. Ook het lokale toezicht schoot tekort door het ontbreken van een wettelijke regeling. Mede als gevolg hiervan kon het aantal personen omtrent wie informatie was opgeslagen spectaculair groeien. Niet alleen het toezicht maar ook het ontbreken van duidelijke criteria voor de opname van gegevens had geleid tot een situatie waarin naar het oordeel van de commissie meer informatie werd opgeslagen dan noodzakelijk was. Verder bleek dat er ook informatie werd opgeslagen in de verkeerde registers en dat verwijdering van de opgeslagen informatie nauwelijks plaatsvond. De Commissie Van Traa concludeerde voorts dat de uitwisseling van CID-informatie met bijzondere opsporingsdiensten (BOD-en) ernstig tekortschoot omdat deze werd bemoeilijkt door de verschillende wettelijke regimes waaronder deze diensten vielen. Daarnaast vond een groot deel van de informatie-uitwisseling mondeling plaats en speelde het *old boys-network* een grote rol bij de toegankelijkheid van informatie binnen de politie. Deze situatie maakte de informatiestromen ondoorzichtig en werkte belemmerend voor de controle.

96 *Kamerstukken II* 1995/96, 24 072, nr. 14.

De Commissie Van Traa deed onder andere de aanbeveling om de registraties van CID-subjecten te beperken via duidelijke opnamecriteria. Uitgangspunt van deze criteria zou moeten worden dat het gaat om de registratie van informatie over verdachten van misdrijven waarvoor (1) voorlopige hechtenis is toegelaten, (2) die gepleegd worden in georganiseerd verband en (3) een ernstige inbreuk op de rechtsorde vormen. Verder moest ook informatie geregistreerd kunnen worden over personen tegen wie een redelijk vermoeden bestaat dat zij deze misdrijven zullen plegen. Het is opvallend dat de commissie ook de aanbeveling deed tot opheffing van de voorlopige registers omdat in de praktijk bleek dat een opwaardering tot CID-subject nagenoeg automatisch verliep. [97] Naast de conclusies en aanbevelingen ten aanzien van de organisatie en werkwijzen van de CID deed de PEC vergaande voorstellen om te voorzien in een formeel-wettelijke basis voor de door de politie gebruikte bijzondere opsporingsmethoden. Naar aanleiding daarvan zijn deze methoden uitgewerkt in de Wet bijzondere opsporingsbevoegdheden (de wet BOB).

De uitkomsten van de parlementaire enquête vormden aanleiding voor de Tweede Kamer tot vervolgonderzoek om daarmee de effecten van de aanbevelingen van de Commissie Van Traa te volgen en te evalueren.[98] De Tijdelijke Commissie uitvoering aanbevelingen IRT-enquêtecommissie (hierna: "de commissie-Kalsbeek") werd daartoe ingesteld. Het onderzoek door deze commissie diende primair een evaluatief karakter te hebben. Ten aanzien van de CID-en kwam ook de commissie-Kalsbeek tot de conclusie dat de differentiatie in organisatie en werkwijzen voor een belangrijk deel konden worden teruggevoerd op het ontbreken van een duidelijke regeling. Deze vaststelling heeft uiteindelijk geleid tot de aanpassing van de CID-regeling 1995.

In de 'nieuwe' CID-regeling zijn de taken en bevoegdheden van de dienst ingeperkt en kwam het accent primair te liggen op de informatieverwerking en informatievoorziening ten behoeve van de recherche.[99] Om het 'nieuwe' karakter van de dienst te articuleren kreeg de CID bij de inwerkingtreding van de nieuwe regeling op 1 november 2000 ook een andere naam: Criminele Inlichtingeneenheid (CIE). [100] In 2001 werden in de Wpolr bijzondere bepalingen opgenomen die specifiek zagen op de informatieverwerking

97 Deze aanbeveling werd uiteindelijk niet gevolgd maar deze registers zijn met de Wpolg alsnog komen te vervallen. Zie daarover hoofdstuk 3 alsmede Kielman en Koelewijn (2005).

98 *Kamerstukken II*, 1995/96, 24 072, nr. 43.

99 Naast de 25 politieregio's beschikt de Nationale Recherche over een eigen CIE, de NCIE. Daarnaast zijn er een aantal CIE-en die zijn opgericht bij een aantal BOD-en en de Koninklijke Marechaussee.

100 Art. 5 lid 1 Besluit Beheer Regionale Politiekorpsen (versie 17-05-2005).

betreffende zware criminaliteit.[101] Deze bepalingen voorzagen onder meer in striktere opslagcriteria en een beperkter verstrekkingenregime voor de informatie die werd verwerkt door CIE-en. De opslagcriteria zijn gehandhaafd in de Wpolg. In hoofdstuk 3 zijn beide wettelijke regimes reeds besproken.

4.1.2 De informatie- en registratiesystemen

Als onderdeel van de ontwikkeling van informatie- en registratiesystemen in de organisatie (dat wil zeggen in taken en in bevoegdheden) besteden wij hieronder specifiek aandacht aan de totstandkoming en het gebruik van de informatiesystemen bij de CID-en.

De eerste initiatieven tot het automatiseren van de opslag en verwerking van criminele inlichtingen werden ontplooid omstreeks het midden van de jaren tachtig. De ontwikkeling van de eerste informatiesystemen hangt nauw samen met de totstandkoming van de eerste CID-regeling en het beleidsplan voor de automatisering van de politiële informatievoorziening. Uitgangspunt van het toenmalige beleid was het terugbrengen van centrale overheidsbemoeienis.[102] Het beleidsplan en de CID-regeling brachten enige mate van duidelijkheid in de verantwoordelijkheden en de eisen waaraan de systemen zouden moeten voldoen. Het eerste CID-registratiesysteem, aangeduid als het Recherche Basis Systeem (RBS), werd ontwikkeld door de gemeentepolitie Groningen en sloot nauw aan bij het eveneens in Groningen ontwikkelde Bedrijfsprocessen Systeem (BPS). Doordat het beleid primair gericht was op decentralisatie van de organisatie werden er geen afspraken gemaakt om de ontwikkeling van deze systemen centraal te coördineren. Het gevolg daarvan was dat op regionaal niveau besloten kon worden tot de ontwikkeling van een 'eigen' informatiesysteem. Dat gebeurde onder andere in de toenmalige politieregio Noord-Brabant Noord. Deze regio kwam tot de conclusie dat het Groningse systeem ongeschikt was voor de CID in Den Bosch. Om die reden werd er in deze regio overgegaan tot de ontwikkeling van een eigen systeem, het VIDOCQ[103] (Kranenburg e.a., 1988). Hetzelfde gebeurde ook in andere politieregio's waardoor er langzaam maar zeker een gedifferentieerd landschap van verschillende informatiesystemen ontstond. De knelpunten die deze ontwikkelingen opleverden voor de uitwisseling

101 Art. 2 CIE-regeling juncto art. 1 lid 1 onder k Wpolr.

102 *Kamerstukken II*, 1984/85, 19 159, nrs. 1-2.

103 De naam van het VIDOCQ-systeem vormt een verwijzing naar de memoires (*Memoires de Vidocq, chef de la police de Sûreté, jusqu'en 1827)* van de Franse politiechef Eugène François Vidocq (1775-1857). De memoires verhandelen over de periode dat Vidocq rechercheur was en veel misdadigers wist te pakken door zich onherkenbaar te vermommen. Naar deze heimelijkheid van het recherchewerk verwijst de naam het Bossche CID-registratiesysteem.

van informatie was voor het overleg van regionale CID-coördinatoren de aanleiding om een werkgroep in te stellen die onderzoek ging doen naar de mogelijkheden voor centraal georganiseerde automatisering in de CID-praktijk. De werkgroep, genoemd naar de haar voorzitter Keizerwaard, kreeg de opdracht om verslag uit te brengen ten aanzien van de ontwikkelingen van een geautomatiseerd verwerkingsbestand voor criminele inlichtingen. Daarnaast moest de werkgroep gebruikerseisen voor zo'n systeem formuleren waarbij rekening gehouden moest worden met de CID-regeling en het Privacyreglement. Tenslotte werd de werkgroep ook gevraagd om een plan van aanpak voor de automatisering van het systeem te ontwerpen en een raming te geven voor de voor het systeem benodigde kosten (Keizerwaard, 1988).

De werkgroep-Keizerwaard veranderde echter op eigen initiatief haar taakomschrijving en kwam tot de conclusie dat de ontwikkeling van een landelijk uniform CID-systeem niet de hoogste prioriteit had omdat dit niet haalbaar werd geacht. Zo overwoog de werkgroep dat:

> "(…) op lokaal en regionaal gebied al diverse systemen operationeel zijn of worden ontwikkeld. Het is een utopie te veronderstellen dat deze ontwikkelingen gestopt zullen worden ten behoeve van een landelijk systeem." (Keizerwaard, 1988, p. 18 e.v.).

In plaats van de ontwikkeling van een landelijk informatiesysteem moest volgens de commissie gekomen worden tot de vaststelling van een landelijk geldend datamodel ten behoeve van een gestandaardiseerde informatie-uitwisseling tussen CID-en. Tegelijkertijd betekenden deze conclusies evenwel dat aan de CID-en grote vrijheid werd gegeven om naar eigen inzicht informatiesystemen te ontwikkelen die dan, zo luidde de redenering, konden worden toegesneden op de lokale en regionale behoeften. Ondanks de aanbeveling tot standaardisatie bleef een landelijk geldend datamodel uit.[104]

Ondertussen werden er naast het Groningse RBS en het Bossche VIDOCQ nog zeven andere systemen ontwikkeld.[105] In het totaal waren er in 1991 negen verschillende informatiesystemen in gebruik voor de registratie van criminele inlichtingen. De aanvankelijk geconstateerde knelpunten met betrekking tot de elektronische uitwisseling waren daardoor groter geworden en dat vormde voor de begeleidingscommissie CID opnieuw aanleiding om onderzoek te laten doen naar de ontwikkelingen ten aanzien van de geautomatiseerde CID-applicaties. Eind 1991 concludeerde het adviesbureau In-pact:

---

104 *Kamerstukken II*, 1989/90, 21 302, nrs. 1-2, p. 9.

105 Enkel bekende systemen zijn OCTOPUS (Rotterdam en Haaglanden), SUSPECT (Flevoland), ACIS (Arnhem), en Xpol (Amsterdam en Limburg).

> "De aanbevelingen van het rapport 'Keizerwaard' – inclusief het daarin aangereikte datamodel – hebben niet tot de gewenste convergentie geleid. De datamodellen van de diverse CID-applicaties lopen sterk uiteen. Op dit moment kan met de huidige gegevensdefinities van enige vorm van elektronische uitwisseling tussen verschillende CID-systemen geen sprake zijn. Blijkbaar hebben ontwikkelaars van deze programma's hieraan geen of onvoldoende aandacht besteed." (In-pact, 1991)

Van landelijke samenwerking bij de ontwikkeling van de systemen was dus niet of nauwelijks sprake geweest, sterker nog, in het rapport concludeert het adviesbureau In-pact dat korpsen elkaar bij de ontwikkeling van systemen de loef probeerden af te steken. Het adviesbureau spreekt in dat verband van het *not-invented-here syndroom* waardoor deze ongewenste polarisatie was ontstaan. Wanneer we naast deze situatie de sterk ontwikkelde regiocultuur en de heimelijkheid van de informatieverwerking in ogenschouw nemen, dan kan worden gesteld dat slechts op zeer beperkte schaal CID-gegevens werden uitgewisseld, en dat er nauwelijks sprake was van een *elektronische* uitwisseling van gegevens. Een ondervraagde CID-medewerker verwoordde de toenmalige situatie in dat verband kernachtig als volgt: "Iedereen rotzooit maar wat aan." (In-pact, 1991, p. 30)

Het adviesbureau In-pact deed vier aanbevelingen.

- Ten eerste zou het aantal verschillende CID-systemen beperkt moeten worden. Dit betekende concreet dat het aantal van negen verschillende informatie- en registratiesystemen teruggebracht zou moeten worden naar één of twee systemen.
- Ten tweede zou er alsnog een landelijk verplicht CID-datamodel moeten worden ontwikkeld zodat er een uniforme en gestandaardiseerde registratie van informatie zou kunnen plaatsvinden. Door middel van standaardisatie zou het elektronische uitwisselen van informatie kunnen worden gerealiseerd.
- Ten derde was aanvullend onderzoek nodig naar de functionele eisen en de prestatie-eisen van CID-systemen waarbij rekening moest worden gehouden met: (1) de relatie van de CID-systemen tot verwante recherche- en basisregistratiesystemen, (2) de eisen van gegevensuitwisseling en (3) de eisen op het gebied van misdaadanalyse.
- Ten vierde zou er een landelijke verwijzingsindex moeten worden aangelegd waarin alle CID-subjecten konden worden opgenomen. De index had tot doel om door middel van het matchen van subjecten de interregionale uitwisseling van informatie te bevorderen. Noodzakelijk daarvoor was dat er elektronische gegevensuitwisseling mogelijk zou moeten worden gemaakt tussen de landelijke index en de regionale systemen.

De Minister van Justitie en de Minister van Binnenlandse Zaken namen deze aanbevelingen over en erkenden dat een grotere samenhang van de CID-automatisering dringend gewenst was. Vanuit de ministeries werd er echter niet concreet ingegrepen omdat zij verwijzend naar het toen 'nieuwe' politie-

bestel, de verantwoordelijkheid voor de inrichting van de informatievoorziening neerlegden bij de korpsbeheerders. Uitgangspunt bleef zodoende wederom een decentrale verantwoordelijkheid voor de inrichting van regionale informatiesystemen. Wel zouden de ministers zorg gaan dragen voor een bovenregionale datacommunicatiestructuur voor een landelijke verwijsindex van CID-subjecten.

In de loop van de jaren negentig van de vorige eeuw ziet men langzaam maar zeker in dat het gedifferentieerde landschap van informatiehuishoudingen belemmerend werkt. Er worden dan ook geen nieuwe systemen voor de CID meer ontwikkeld. In plaats daarvan wordt het aantal van negen verschillende informatie- en registratiesystemen teruggebracht naar twee. De CID-en van enkele grotere politiekorpsen gebruiken OCTOPUS terwijl de overige CID-en hebben gekozen voor RBS. Desondanks blijft het elektronisch uitwisselen van inlichtingen problematisch. In 1998 wordt een systeem opgeleverd voor de landelijke registratie van recherche-onderzoeken en CID-subjecten (thans CIE-subjecten), de zogenaamde landelijke Verwijsindex Recherche Onderzoeken en Subjecten, kortweg het VROS-systeem. In deze landelijke index kunnen de subjecten in recherche-onderzoeken en de CIE-subjecten onderling worden vergeleken. Sinds 1998 heeft de ontwikkeling echter niet stil gestaan en is naast VROS een nieuwe applicatie ontwikkeld voor de uitwisseling van criminele inlichtingen, het zogenaamde Platform Zwacri Uitwisseling (PZU). In sectie 4.3 behandelen wij de verschillende wijzen waarop de huidige elektronische uitwisseling van gegevens is vormgegeven.

4.2 Taken van de CIE

In art. 2 CIE-regeling is de algemene taakstelling van de CIE vastgelegd. De eenheden zijn belast met de informatievoorziening in het kader van de uitvoering van de politietaak, voorzover het gaat om ernstige vormen van criminaliteit.[106] Zoals hierboven al aan de orde is gesteld concentreert het werk van de CIE zich vooral op de informatievoorziening in de pro-actieve fase van de opsporing. Corstens (2002, p. 251) omschrijft dit als de fase waarin nog geen sprake is van een verdenking van een concreet gepleegd delict. Deze fase moet nadrukkelijk worden onderscheiden van de 'actieve' opsporingsfase waarin het gaat om de verzameling van bewijsmateriaal. In de proactieve fase hebben de gegevens primair het doel om inzicht te verkrijgen in criminele activiteiten. In de actieve opsporingsfase staat het vergaren van strafrechtelijk bewijs centraal. Het onderscheid tussen informatie in de proactieve en actieve fase van de opsporing wordt ook wel aangeduid als het

106 Met zware criminaliteit wordt gedoeld om misdrijven in de zin van art. 10 lid 1 sub a Wpolg.

onderscheid tussen *intelligence* en *evidence* (Van Straelen, 2002). De bevoegdheid tot het verzamelen van intelligence en het opbouwen van een informatiepositie door de politie wordt afgeleid uit de taakomschrijving die is neergelegd in art. 2 Politiewet 1993. Deze algemene taakomschrijving brengt echter wel beperkingen met zich mee met name waar het gaat om de rechtvaardiging van inbreuken op de persoonlijke levenssfeer door de politie. De Hoge Raad heeft in het arrest Zwolsman[107] erkend dat een beperkte inbreuk op de persoonlijke levenssfeer gebaseerd kan zijn op de algemene politiële taakomschrijving. Het verzamelen van informatie met behulp van informanten is volgens de Hoge Raad mogelijk binnen art. 2 Politiewet 1993.[108] Bij het opbouwen van een informatiepositie door de CIE kunnen we twee deeltaken onderscheiden te weten; (1) het inwinnen van informatie, en (2) het veredelen en analyseren van informatie. Een uitgebreide beschrijving van de actieve fase van de opsporing en het rechercheproces is te vinden in 'Rechercheportret' (De Poot e.a., 2004).

4.2.1 Inwinnen van informatie

Een belangrijke vraag die bij het inwinnen van informatie met behulp van informanten rijst is: wat moet er worden verstaan onder informanten? In de wettelijke regelingen worden daarvoor verschillende definities gebruikt. Het gemeenschappelijke element daarin is dat het gaat om personen die, anders dan als getuigen, heimelijk informatie verstrekken aan opsporingsambtenaren. Een informant is altijd op een bepaalde manier betrokken bij het misdrijf waarover hij informatie verstrekt of is gerelateerd aan de persoon waarover hij informatie verstrekt. In de minst verwijtbare vorm is die betrokkenheid beperkt tot informatie die verkregen is van derden. Daarbij kan worden gedacht aan een informant die in een bepaald café iets heeft opgevangen over een op handen zijnde bankoverval. In de meest verwijtbare vorm strekt de betrokkenheid zich echter uit tot het in strafrechtelijke zin medeplegen van een misdrijf. Vanwege die relatie en/of betrokkenheid van informanten bij misdrijven willen informanten vrijwel altijd anoniem blijven. Het verstrekken van informatie aan de politie brengt immers grote risico's mee voor de betrokken informanten. In zijn algemeenheid kan worden gesteld dat die risico's groter worden naarmate de betrokkenheid van de informant groter is. De CIE pleegt in dit verband te spreken van zogenaamde afbreukrisico's waarbij de meest ernstige vorm de liquidatie van de informant betreft. Deze risico's zijn de belangrijkste reden voor de CIE om uiterst zorgvuldig met de ingewonnen informatie om te gaan en ook intern terughoudend te zijn met

107 HR 19 december 1995, *NJ* 1996, nr. 249.

108 De Wpolg voorziet niet in zelfstandige wettelijke basis voor het verzamelen van informatie door middel van informanten maar vormt het wettelijke kader voor de verwerking van informatie nadat deze is verzameld.

het verstrekken van de informatie. Wanneer de informatie wel als bewijs wordt gebruikt dan zal de informant in beginsel wel als getuige moeten worden gehoord.[109]

Er zijn twee formeel-wettelijke grondslagen voor het runnen van informanten door de CIE. De eerste grondslag is hiervoor al besproken en wordt ontleend aan art. 2 Politiewet 1993. De tweede grondslag volgt uit art. 126v Sv en kan uitsluitend plaatsvinden op bevel van de officier van justitie. Het belangrijkste verschil tussen beide grondslagen is gelegen in de stelselmatigheid waarmee de informatie van de burger wordt ingewonnen. De wetgever geeft in de Memorie van Toelichting echter geen duidelijke criteria aan de hand waarvan vastgesteld kan worden of er sprake is van het stelselmatig runnen van een informant. In de literatuur is daarover wel discussie. Zo gaat het handboek dat de politie gebruikt bij de opsporing ervan uit dat elke vraag van een runner aan een informant om wat uit te zoeken omtrent een subject, onmiddellijk leidt tot de situatie die gedekt moet worden door een bevel in de zin van art. 126v Sv. Dit handboek laat verder weinig ruimte voor interpretatie. Volgens Van Straelen (2002) is dat onjuist. Volgens hem moeten bij de vraag of de bevoegdheid tot inwinning voortvloeit uit art. 126v Sv dan wel art. 2 Politiewet 1993 aanknopingspunten gezocht worden in de mate waarin – als gevolg van de informatie-inwinning – de persoonlijke levenssfeer wordt aangetast (Van Straelen, 2002). Deze redenering past in de lijn die door de Hoge Raad in het Zwolsman-arrest is uitgezet. Van Straelen werkt deze lijn verder uit en komt dan tot drie beoordelingscriteria om vast-stellen of er een bevel nodig is in de zin van art. 126v Sv, te weten; (1) de aard van de informatie die wordt ingewonnen, (2) de redelijke verwachting die iemand mag hebben omtrent zijn privacy en (3) de indringendheid van het inwinningsproces. Meer in zijn algemeenheid geldt dan dat naarmate (1) de ingewonnen informatie 'gevoeliger' is en (2) het vermoeden van criminele activiteiten van het subject kleiner is en (3) de wijze waarop de informant aan zijn informatie komt ingrijpender is voor het subject, eerder een bevel in de zin van art. 126v Sv nodig is.

Naast het inwinnen van informatie via informanten staan de CIE tal van andere bronnen ter beschikking. Uit ons veldwerk kwam naar voren dat CIE-en ook steeds meer gebruik gaan maken van open bronnen als Internet om aanvullende informatie te verkrijgen over subjecten. Daarnaast kan veel informatie worden ingewonnen uit lopende of afgesloten recherche-onderzoeken. Uit de interviews die wij in het kader van dit onderzoek hebben gehouden met CIE-ers (zie hoofdstuk 5) kwam echter naar voren dat van deze manier van inwinnen in de praktijk nog weinig gebruik werd gemaakt. Dit hing samen met de situatie dat informatie uit recherche-onderzoeken vaak wordt geregistreerd in verschillende soorten informatiesystemen. Niet

109 HR 19 januari 1999, *NJ* 1999 nr. 253.

zelden komt het voor dat onderzoeksinformatie wordt opgeslagen in Word-bestanden en dat de database met opsporingsinformatie zodoende feitelijk bestaat uit een digitale map met grote hoeveelheden Word-documenten hetgeen de toegankelijkheid en uitwisselbaarheid van deze informatie belemmert.

4.2.2 Veredelen en analyseren van informatie

Bij de tweede deeltaak maken wij onderscheid tussen (2a) het *veredelen* en (2b) het *analyseren* van de informatie.

Veredelen
Bij (2a) het veredelen gaat het allereerst om het controleren van de juistheid en volledigheid van de ingewonnen inlichtingen. Een vast onderdeel daarvan vormt het controleren van de juistheid en volledigheid van de Naw-gegevens van de personen waarover de inlichtingen worden verwerkt. Dergelijke gegevens worden onder andere gecontroleerd met behulp van de registraties in de Gemeentelijke Basis Administratie (GBA). Gegevens die onjuist blijken of nog ontbreken kunnen worden verbeterd en aangevuld. Daarnaast worden gegevens ook zoveel mogelijk gecontroleerd op de inhoudelijke juistheid. Er moet daarbij worden vastgesteld of hetgeen een informant heeft verteld ook daadwerkelijk klopt. Wij geven een voorbeeld. Er is van informant X een tip binnengekomen dat er in loods Y een XTC-laboratorium is opgesteld. Deze informatie zal door de CIE op haar juistheid moeten worden gecontroleerd. Dat zou bijvoorbeeld gedaan kunnen worden door de inzet van een observatieteam. Het komt echter ook regelmatig voor dat het verifiëren van de juistheid en volledigheid niet of slechts gedeeltelijk mogelijk is. In die gevallen wordt de oordeelsvorming van de betrouwbaarheid van de informatie een onderdeel van het veredelen. Uit ons onderzoek kwam naar voren dat een belangrijk deel van deze oordeelsvorming geschiedt op basis van de intuïtie van de betrokken politieambtenaar. Wij constateren dat er in de laatste twintig jaar in feite nauwelijks iets is veranderd waar het gaat om de rol van intuïtie bij de registratie en beoordeling van criminele inlichtingen. In 1989 kwam namelijk de toenmalige Commissie van Toezicht (de voorloper van de Registratiekamer, het huidige Cbp) al tot een soortgelijke conclusie ten aanzien van het registreren van gegevens door de CID. De Commissie van Toezicht concludeerde met betrekking tot de juistheid en betrouwbaarheid van de registratie dat vele CID-en dit niet wisten te onderbouwen maar daarbij vooral wezen op de intuïtie van de politieman.[110]

110 Jaarverslag Commissie van Toezicht 1989 en 1990, p. 4.

Analyseren
Bij (2b) het analyseren van informatie kan grofweg onderscheid worden gemaakt in twee typen analyses. Ten eerste de strategische beleidsanalyses. Voor dit type analyse worden politiegegevens gebruikt waarbij in de analyse bijvoorbeeld wordt gekeken naar een bepaald soort type criminaliteit en bijvoorbeeld de mate waarin dit type zich al dan niet concentreert in een deel van de politieregio. Dergelijke analyses geven beleidsmakers informatie over waar zij prioriteiten zouden moeten leggen in de regio. Ten tweede kunnen de tactische analyses worden onderscheiden. Deze analyses zijn bedoeld om recherche-onderzoeken te ondersteunen en richting te geven. Met behulp van een tactische analyse kan bijvoorbeeld een vermeende criminele organisatie nauwkeurig in kaart worden gebracht waarmee een rechercheteam inzicht krijgt in de verschillende betrokkenen en de onderlinge hiërarchische verhoudingen binnen de organisatie.

4.3 Verstrekken van informatie

Naast het inwinnen, veredelen en analyseren van informatie bestaat de belangrijkste kerntaak van de CIE uit het verstrekken van informatie naar rechercheteams en andere onderdelen van de politieorganisatie. In ons onderzoek zijn wij vier verschillende vormen van verstrekken van criminele inlichtingen tegengekomen te weten (1) de schriftelijke verstrekking door middel van een proces-verbaal (subsectie 4.3.1), (2) de schriftelijke verstrekking door middel van een informatierapport (subsectie 4.3.2), (3) de elektronische verstrekking door rechtstreekse toegang tot de informatiesystemen (subsectie 4.3.3) en (4) de mondelinge verstrekkingen (subsectie 4.3.4).

4.3.1 Verstrekking bij proces-verbaal

Het proces-verbaal als verstrekkingsvorm wordt voornamelijk gebruikt om inlichtingen te verstrekken aan de recherche. Het proces-verbaal is bedoeld om de informatiestroom van de CIE naar de recherche transparant en controleerbaar te maken. Het College van Procureurs-generaal heeft deze informatiestroom gestandaardiseerd via een landelijk model voor CIE processenverbaal.[111] Het proces-verbaal vermeldt naast de informatie ook de mate van juistheid en betrouwbaarheid. Vrijwel altijd wordt dat in algemene bewoordingen gedaan omdat het met een uitgebreide toelichting moeilijker wordt de informant af te schermen. In het proces-verbaal wordt verder een selectie gemaakt van de voor het rechercheonderzoek relevante informatie. Bij die

111 Openbaar ministerie, Aanwijzingen opsporingsbevoegdheden, te raadplegen via <www.om.nl>.

selectie wordt naast de inschatting van mogelijke relevantie ook gekeken naar de afbreukrisico's voor de informant. De afbreukrisico's spelen vooral een rol wanneer de informatie operationeel zal worden ingezet (Feenstra-Schellekens e.a., 2007). Uit ons veldwerk (zie hoofdstuk 5) kwam naar voren dat het behoud van een informant bij de CIE in beginsel als zwaarste belang wordt meegewogen. In het uiterste geval wordt dan de relevante informatie in het geheel niet opgenomen in het proces-verbaal. Het komt evenwel relatief vaak voor dat de informatie wordt veralgemeniseerd of dat slechts een gedeelte van de informatie in het proces-verbaal wordt opgenomen. Hiermee wordt beoogd de kans op herleidbaarheid van de informant te verkleinen. De aanwijzingen voor de opsporingsbevoegdheden die zijn opgesteld door het College van procureurs-generaal bepalen dat uitsluitend de CIE-chef of diens plaatsvervanger informatie uit de CIE-bestanden kan verstrekken aan andere opsporingsambtenaren. Dit zijn binnen de organisatie de politieambtenaren die de processen-verbaal ondertekenen en daarmee verantwoordelijk zijn voor de verstrekking van informatie. Naast het besproken CIE proces-verbaal wordt er gebruik gemaakt van het proces-verbaal voor de bijvangst. Het gaat daarbij om informatie die niet voldoet aan de opnamecriteria van het register zware criminaliteit omdat het bijvoorbeeld gaat om minder ernstige misdrijven. Deze informatie wordt niet geregistreerd in de registers van de CIE, maar rechtstreeks via een proces-verbaal verzonden naar de betreffende afdeling binnen de politie (Kieviet e.a., 2004).

4.3.2 Verstrekking via informatierapport

De tweede vorm van verstrekken is het schriftelijke informatierapport, ook wel aangeduid met het 4x4-tje. In art. 6 lid 1 CIE-regeling wordt bepaald dat de CIE-en gevraagd en ongevraagd onderling criminele inlichtingen uitwisselen indien dit van belang is voor de uitvoering van de politietaak. Bij deze uitwisseling moet gebruik worden gemaakt van het standaard informatierapport. Bij de uitwisseling in deze vorm wordt in beginsel zowel operationeel bruikbare informatie als informatie met een (hoog) afbreukrisico uitgewisseld. Het informatierapport bevat tevens de coderingen die iets zeggen over de inschatting van de verstrekkende CIE met betrekking tot de juistheid en de betrouwbaarheid van de informatie. Deze codering wordt overigens ook gebruikt om de informatie op een proces-verbaal te duiden. In tabel 4.1 en tabel 4.2 geven wij het landelijk geldende model van coderingen weer.[112]

112 Openbaar ministerie, Aanwijzingen opsporingsbevoegdheden, te raadplegen via <www.om.nl>.

Code	betekenis	toelichting
A	betrouwbaar	De bron vervult een maatschappelijke rol of een ambt die of dat met zich meebrengt dat aan integriteit en zuiverheid van waarnemingsvermogen of oordeelsvorming niet behoeft te worden getwijfeld.
B	meestal betrouwbaar	De bron heeft in het verleden eerder, en herhaaldelijk, informatie verschaft die bij nader onderzoek in de meeste gevallen juist bleek te zijn.
C	minder betrouwbaar tot niet betrouwbaar	De bron heeft in het verleden eerder, en herhaaldelijk, informatie verschaft die bij nader onderzoek in de meeste gevallen niet juist bleek te zijn.
X	niet te beoordelen	De bron heeft de CIE in kwestie niet eerder van informatie voorzien of het is niet mogelijk vast te stellen of de bron in dit geval te goeder trouw is dan wel werkelijk kan beschikken over de informatie die hij of zij pretendeert te hebben.
1	waargenomen	De informatie is door de informant zelf waargenomen.
2	gehoord	De informatie heeft de informant gehoord van iemand die er bij is geweest.
3	indirect gehoord	De informant heeft de informatie via via verkregen.

Tabel 4.1: Beoordelingscoderingen.

Verder wordt op het informatierapport aangetekend of, en zo ja onder welke voorwaarden, de aangedragen informatie door de ontvangende CIE ter beschikking van de recherche kan worden gesteld. Daarvoor wordt gebruik gemaakt van de afhandelingscodes die in tabel 4.2 gegeven zijn.

Code	betekenis
11	De informatie is operationeel te gebruiken.
01	De informatie mag alleen worden gebruikt na overleg met de afzender.
00	De informatie kan niet worden gebruikt dan met zware beperkingen.
200	De informatie kan vanwege een verhoogd afbreukrisico niet operationeel worden gebruikt, maar kan onder bepaalde voorwaarden wel voor coördinatie- en analysedoeleinden worden gebruikt.
300	De informatie kan vanwege bronbeschermingsbelangen niet operationeel gebruikt worden, maar kan onder bepaalde voorwaarden wel voor coördinatie- en analysedoeleinden worden gebruikt.

Tabel 4.2: Afhandelingscoderingen.

Bij registratie van de inlichtingen in de informatiesystemen moeten bij de mutatie (dat wil zeggen de toevoeging van nieuwe informatie of de wijziging van bestaande informatie) de afhandelingscode vermeld worden. Uit ons veldwerk is naar voren gekomen dat er regionaal aanzienlijke verschil-

len bestaan met betrekking tot de interpretaties en het gebruik van de afhandelingscodes. In meer dan de helft van de onderzochte regio's werd aangegeven dat er geen gebruik werd gemaakt van de coderingen 200 en 300 omdat de informatiesystemen niet zijn ingesteld op het gebruik van deze codering. Verder viel op dat er in een aantal regio's geen onderscheid wordt gemaakt tussen de 11 en de 01 coderingen. De reden die werd gegeven voor die ontstane praktijk was dat in de betreffende regio altijd overleg zou moeten plaatsvinden met de afzender alvorens de informatie operationeel mag worden ingezet.

De informatierapporten zijn uitsluitend bedoeld voor de uitwisseling van informatie tussen de CIE-en onderling en mogen niet worden doorverstrekt aan de recherche of andere onderdelen binnen de politieorganisatie.[113] Het is daarom niet de bedoeling dat informatierapporten worden toegevoegd aan een strafdossier. Wanneer de ontvangende CIE de informatie toch wil gaan inzetten voor operationele doeleinden dan wordt aan de verstrekkende CIE gevraagd om de informatie uit het informatierapport opnieuw te verstrekken via een proces-verbaal. Evenals voor de processen-verbaal, geldt dat uitsluitend de CIE-chef of zijn plaatsvervanger bevoegd is informatie in deze vorm te verstrekken. In de praktijk is het informatierapport de meest voorkomende vorm van informatie-uitwisseling tussen CIE-en onderling. Dat heeft te maken met het feit dat de verstrekkende CIE een controle kan uitoefenen op de informatie die wordt verstrekt. Wanneer de CIE-chef inschat dat aan verstrekking van bepaalde informatie te grote risico's kleven dan wordt het niet opgenomen in een informatierapport.

Uit de gesprekken die in het kader van het veldwerk zijn gevoerd met diverse CIE-ers (zie hoofdstuk 5) komt verder naar voren dat er ook een aantal nadelen kleven aan deze vorm van verstrekken. Het gaat dan ten eerste om de tijd die nodig is om uiteindelijk een verstrekking daadwerkelijk tot stand te laten komen. Het uitwisselingsproces is nauwelijks geautomatiseerd waardoor het grotendeels handmatig wordt gedaan. Het proces van uitwisselen komt over het algemeen pas tot stand na telefonisch overleg waarbij door de ene CIE aan de andere CIE wordt gevraagd of er bij hen informatie aanwezig is over een bepaald subject. De bevraagde CIE zal daarop gaan zoeken in de eigen registers. Vervolgens wordt de vermoedelijk relevante informatie geselecteerd en geprint. Het document wordt ter beoordeling voorgelegd aan de CIE-chef die vervolgens moet beoordelen of de informatie verstrekt mag gaan worden. Wanneer de CIE-chef akkoord is wordt de informatie gefaxt of per post verstuurd. De ontvangende CIE beoordeelt daarna of de informatie inderdaad relevant is en zo ja, dan wordt het informatierapport overgetypt en opgeslagen in het eigen informatiesysteem. Wanneer de informatie nodig blijkt voor recherche-onderzoek zal er een

113 Zie aanwijzingen opsporingsbevoegdheden.

terugkoppeling plaatsvinden waarin aan de verstrekkende CIE gevraagd wordt om een proces-verbaal van de informatie te maken.

4.3.3 Elektronische verstrekking

De derde verstrekkingsvorm is het elektronisch verstrekken van gegevens. Deze wijze van verstrekken vindt in de praktijk voornamelijk plaats tussen de CIE-en onderling. Wij onderscheiden drie verschillende vormen van elektronische verstrekkingen.

De eerste verstrekkingsvorm is de elektronische verstrekking via autorisatie tot registers van andere CIE-en. Via een autorisatie tot het informatiesysteem van een regionale CIE is het mogelijk om te zoeken in het register zware criminaliteit van die regio. Zo konden in de periode dat wij in het kader van dit onderzoek veldwerk hebben verricht (oktober 2004 – juni 2006) de ambtenaren van de drie noordelijke CIE-en in elkaars systemen inloggen en alle daarin opgeslagen informatie doorzoeken en opvragen. Ook de 00-informatie kon op deze manier worden uitgewisseld. Het voordeel daarvan is dat zonder tussenkomst van een CIE-chef rechtstreeks informatie wordt verstrekt aan een medewerker van een andere CIE.

In de gesprekken die wij hebben gevoerd met CIE-ambtenaren van de noordelijke regio's (Friesland, Groningen en Drente) werd benadrukt dat deze wijze van elektronisch verstrekken uitsluitend gebaseerd was op een wederzijds regionaal vertrouwen. Met name waar het gaat om het elektronisch uitwisselen van informatie waarop een zware beperking rust, de zogenaamde 00-informatie, kan het gebrek aan wederzijds vertrouwen een obstakel vormen in de uitwisseling.

De tweede verstrekkingsvorm is de elektronische verstrekking van gegevens door middel van het VROS-systeem (Eling e.a., 2003). De elektronische uitwisseling door middel van dit systeem heeft vooral een signaleringsfunctie. Er wordt uit alle regionale CIE-informatiesystemen en de recherche informatiesystemen wekelijks een *dataset* aangeleverd van CIE-subjecten en subjecten die onderwerp zijn van een rechercheonderzoek. Deze gegevens worden één keer per week onderling en met elkaar vergeleken om vast te stellen of één subject in meerdere regio's onderwerp is van een CIE-onderzoek en/of van een ander rechercheonderzoek. De resultaten van deze gegevensvergelijking worden vervolgens naar de verantwoordelijke CIE-ambtenaar of rechercheur in de regio verzonden. Naast deze signaleringfunctie voor overlappen in lopende onderzoeken wordt het VROS geraadpleegd om in geval van nieuwe subjecten na te gaan of deze al eerder in een andere regio onderwerp van onderzoek zijn geweest. Het VROS is daarmee vooral een verwijzingssysteem dat bedoeld is om politieambtenaren door de sluizen naar mogelijk relevante informatie.

De derde verstrekkingsvorm is een elektronische uitwisseling van informatie die plaatsvindt via het Platform Zwacri Uitwisseling (PZU). Deze vorm van elektronisch verstrekken vormt een uitwerking van de wederzijdse autorisatie. Het PZU-systeem koppelt namelijk de regionale informatiesystemen waardoor de informatie kan worden ontsloten. Het PZU-systeem ontsluit slechts de operationeel bruikbare informatie, dus informatie met de afhandelingscode 11 en 01 zichtbaar. Het systeem is daarmee een 'afgeslankte' technische uitwerking van de plicht om twee medewerkers van iedere regionale CIE te autoriseren in de registers zware criminaliteit van de overige CIE-en.[114] Het PZU-systeem beoogt een snellere en effectievere uitwisseling van relevante inlichtingen mogelijk te maken. De geautoriseerde medewerker kan via het systeem alle regionale registers zware criminaliteit bevragen waarbij hij de gevonden informatie rechtstreeks via een computerscherm verstrekt krijgt. Er is met betrekking tot deze wijze van verstrekken een protocol[115] vastgesteld waarin onder meer wordt geregeld dat wanneer er relevante informatie wordt gevonden, er altijd een telefonische terugkoppeling dient plaats te vinden met de bevraagde CIE. In die terugkoppeling moet worden aangegeven:

– welke informatie gezocht werd;
– welke informatie gevonden is;
– welke informatie gebruikt gaat worden;
– het doel waarvoor de informatie gebruikt gaat worden.

De bevraagde CIE geeft dan binnen twee werkdagen aan of dit akkoord is en of er binnen zijn eenheid nog meer informatie voor handen is. De medewerker die de informatie heeft vergaard maakt vervolgens een samenvatting van de informatie die mag worden gebruikt. Gedurende de periode dat wij het veldwerk hebben verricht (oktober 2004 – juni 2006) bleek evenwel dat in de CIE-praktijk nog nauwelijks gebruik wordt gemaakt van het systeem. De belangrijkste oorzaak die daarvoor werd aangegeven was dat via het PZU-systeem slechts de operationeel bruikbare informatie wordt ontsloten (informatie met afhandelingscode 11 en 01) terwijl het merendeel van de opgeslagen informatie (00-informatie) niet wordt ontsloten. Het gevolg daarvan is dat je met de via PZU gevonden informatie nog altijd niet alle beschikbare informatie voor handen hebt. Zodoende kan geen volledig beeld gevormd worden over een bepaald subject. Naast de zoekresultaten uit PZU moet dus vaak alsnog telefonisch contact worden opgenomen met de verschillende regio's om na te gaan of er ook relevante 00-informatie beschikbaar is. De keuze voor het niet ontsluiten van 00-informatie is zoals hiervoor reeds aangegeven gelegen in het gebrek aan interregionaal vertrouwen.

114 Art. 6 lid 2 CIE-regeling.
115 Protocol Uitwisselen Zwacri informatie.

4.3.4 Mondelinge verstrekking

De vierde verstrekkingsvorm die wij onderscheiden betreft de mondelinge verstrekking. Uit het veldwerk kwam naar voren dat CIE-ers zich in het algemeen terughoudend opstellen ten aanzien van het mondeling verstrekken van inlichtingen, zeker wanneer het gaat om verstrekkingen aan de recherche. Mondelinge verstrekkingen komen wel voor, maar dat blijft veelal beperkt tot de spoedeisende gevallen en dan wordt de verstrekking zo snel mogelijk schriftelijk bevestigd via een proces-verbaal. Evenals bij de schriftelijke verstrekkingen geldt ook hier dat de CIE-chef of zijn plaatsvervanger controle wil houden op de informatiestroom. Er werd echter ook aangegeven dat deze controle in de praktijk niet altijd mogelijk blijkt, bijvoorbeeld in gevallen waarin CIE-ambtenaren (veelal runners) meelopen met recherche-onderzoeken. Dat houdt in dat zij deel uitmaken van het rechercheteam om zodoende een inschatting te maken van de informatiebehoefte en daarnaast ook de informatiepositie van de eigen CIE willen verbeteren. Vaak beschikken deze medewerkers over meer informatie dan de rechercheurs, maar geldt intern de afspraak dat zij die niet mogen verstrekken. Het komt regelmatig voor dat dit toch wordt meegedeeld aan het rechercheteam hetgeen binnen de politie wordt aangeduid met de term 'fluisteren'. Hoewel het merendeel van de geïnterviewde CIE-chefs aangaf dat zij intern de afspraak hebben dat 'fluisteren' absoluut verboden is, gaven zij ook aan dat dit in de praktijk moeilijk te voorkomen is. De betreffende CIE-medewerkers zijn immers nauw betrokken bij het onderzoek en zij maken zichzelf populair bij hun collega's van de recherche wanneer zij informatie verstrekken. Het grote nadeel van deze verstrekkingsvorm is het gebrek aan transparantie waardoor de verstrekking nauwelijks controleerbaar is. Er wordt immers min of meer heimelijk verstrekt en er vindt geen schriftelijke bevestiging via een proces-verbaal plaats. Bovendien wordt van de verstrekking geen aantekening gemaakt in het register zware criminaliteit. Datzelfde geldt voor een groot gedeelte van de mondelinge verstrekkingen tussen de CIE-ers onderling tijdens het vaststellen van de wederzijdse informatiebehoeften. Tijdens het stellen van de zoekvragen moet vrijwel altijd een gedeelte van de eigen informatie worden verstrekt voordat een andere regio kan vaststellen of zij mogelijk relevante informatie hebben. Bij zo'n overleg is het gebruikelijk dat achtergronden en reeds bekende informatie wordt uitgewisseld door de verzoeker. Wanneer naar aanleiding van zo'n overleg informatie wordt uitgewisseld gebeurt dat in de regel schriftelijk en wordt daarvan ook aantekening bijgehouden in het register zware criminaliteit.

4.4 Tussenconclusies

Ten eerste hebben wij het ontstaan van de CIE-en onderzocht. Daaruit is naar voren gekomen dat bij de bestrijding van bepaalde vormen van criminaliteit (de handel in verdovende middelen en recent de bestrijding van terrorisme) binnen het opsporingsapparaat van politie en justitie in toenemende mate behoefte is ontstaan aan proactieve opsporingsmethoden. De CIE voorziet voor een belangrijk deel in deze behoefte.

Ten tweede hebben wij vastgesteld dat een adequate informatie-uitwisseling voor deze proactivering van de opsporing van groot belang is. Informatie-uitwisseling stelt andere onderdelen binnen de politieorganisatie immers in staat tot het effectief anticiperen op de beschikbare CIE-informatie. Van een adequate informatie-uitwisseling was echter lange tijd geen sprake. De informatie-uitwisseling werd belemmerd door een eilandenrijk aan verschillende informatiesystemen waartussen technisch nauwelijks uitwisseling mogelijk was. Daarnaast kende de organisatiecultuur binnen de CIE (voorheen CID) een sterke geslotenheid waardoor tot het eind van de jaren negentig nauwelijks maatregelen werden genomen om de informatie-uitwisseling te verbeteren.

Ten derde komen wij tot de conclusie dat vanaf het begin van 2000 langzaam maar zeker gewerkt wordt aan een cultuuromslag binnen de CIE. Het uitwisselen van CIE-informatie is niet meer uitsluitend een regionale aangelegenheid. Steeds meer ICT-toepassingen (VROS, PZU) voorzien in mogelijkheden om de CIE-informatie ook interregionaal uit te wisselen. Wij constateren dat deze ontwikkelingen langzaam gaan en dat er nog altijd een grote terughoudendheid bestaat ten aanzien van het elektronisch uitwisselen van 00-informatie. Toch menen wij dat het einde van de trend nog niet bereikt is. De komende jaren zal er hoe langer hoe meer behoefte ontstaan aan elektronische uitwisseling van CIE-informatie en daarmee ook aan betrouwbare en controleerbare systemen.

5 Knelpunteninventarisatie

In dit hoofdstuk geven wij een inventarisatie van de belangrijkste knelpunten met betrekking tot het uitwisselen van politiegegevens. Dit onderwerp vormt het eerste onderdeel van de derde onderzoeksvraag (OV 3). De knelpunteninventarisatie vormt het vertrekpunt voor de nadere organisatieanalyse in hoofdstuk 6 waar beide onderdelen van de derde onderzoeksvraag zullen worden beantwoord. De nadruk in dit hoofdstuk ligt op de uitwisseling van politiegegevens binnen de CIE. Daartoe wordt in sectie 5.1 een overzicht gegeven van de resultaten van vijf onderzoeken naar de uitwisseling van politiegegevens. In sectie 5.2 bespreken wij de resultaten van ons eigen veldwerk en vergelijken wij onze resultaten met de knelpunten die wij geïnventariseerd hebben in sectie 5.1. Op basis daarvan formuleren wij in sectie 5.3 vier tussenconclusies.

5.1 Onderzoeken naar informatie-uitwisseling

Sinds het midden van de jaren negentig is de uitwisseling van politiegegevens en de daarop betrekking hebbende regelgeving, regelmatig onderwerp van onderzoek geweest.[116] Ingrijpende maatschappelijke gebeurtenissen, zoals de aanslagen in New York (2001) en Madrid (2004), maar ook nieuwe ontwikkelingen op het gebied van de politiële automatisering vormden telkens aanleiding voor nieuw onderzoek. In deze sectie bespreken wij chronologisch een selectie van vijf onderzoeken en maken wij een inventarisatie van de geconstateerde knelpunten met betrekking tot de uitwisseling van politiegegevens waarbij wij zoveel mogelijk ingaan op uitwisseling door en met de CIE-en.

In subsectie 5.1.1 bespreken wij het evaluatieonderzoek (1996) van de Wpolr en Bpolr. Subsectie 5.1.2 gaat in op de hoofdconclusies van een onderzoek (1998) naar de gegevensuitwisseling tussen het CRI en de politieregio's. In subsectie 5.1.3 wordt een overzicht gegeven van de bevindingen van een onderzoek (2002) naar de uitwisseling van opsporings- en terrorisme-informatie. Vervolgens bespreken wij in subsectie 5.1.4 een onderzoek dat in 2004 is gehouden door de Inspectie Openbare Orde en Veiligheid (Inspectie OOV) naar de landelijke coördinatie en uitwisseling van politie-informatie. Daarna volgt in subsectie 5.1.5 een korte bespreking van het evaluatieonderzoek uit 2005 naar de Wet bijzondere politieregisters.

116 Zie rapporten van de Algemene Rekenkamer van 1998, 2002 en 2003.

5.1.1 Onderzoek 1996: Wpolr en Bpolr

Bij de invoering van de Wet en het Besluit Politieregisters in 1991 was door de regering toegezegd om de regelgeving twee jaar na de invoering te evalueren en na te gaan waar mogelijke aanpassingen noodzakelijk zouden zijn.[117] Het evaluatieonderzoek, dat liep van september 1994 tot mei 1995, richtte zich vooral op het inventariseren van knelpunten waarbij de centrale vraagstelling luidde:

> "Waar komt het werk van de politie in het gedrang als gevolg van de met het oog op de bescherming van de privacy ingevoerde regels?" (Cozijn e.a., 1996, p. 15).

De algemene conclusie die werd getrokken als antwoord op deze vraagstelling was dat niet is gebleken dat de opsporingstaak van de politie als gevolg van de nieuwe regelgeving in het gedrang is gekomen. Wel wezen de onderzoekers erop dat er door de politie vier knelpunten werden ervaren.

Het eerste knelpunt betrof de *protocolplicht*. Deze werd door de politie gekwalificeerd als ondoelmatig, ondoeltreffend en overbodig. De protocolplicht hield in dat van iedere verstrekking aantekening werd bijgehouden. Uit het onderzoek kwam naar voren dat de protocolplicht met name voor verstrekkingen langs geautomatiseerde weg leidde tot onwerkbaar grote logbestanden. De vrijstellingsregeling voor geautomatiseerde verstrekkingen bood daarbij nauwelijks een oplossing omdat inlogprotocollen, die in de plaats kwamen van protocollen voor de afzonderlijke verstrekkingen, drie maanden moesten worden bewaard waardoor eveneens onwerkbaar grote bestanden ontstonden.

Het tweede knelpunt zag op de belemmerende werking van het *gesloten verstrekkingenregime* van de Wpolr en de Bpolr. Door de geslotenheid van het regime werd de politie geremd in de ontwikkeling van nieuwe en vooral op preventie gerichte initiatieven in de samenwerking met partners buiten de politieorganisatie. Het gaat hierbij om informatie-uitwisseling met lagere overheden (gemeenten), woningcorporaties, sociale diensten en hulpverleningsinstanties, zoals de bureaus jeugdzorg.

Het derde knelpunt werd ervaren in de *reglementering van de verschillende politieregisters*. In het bijzonder werd daarbij gewezen op de geïntegreerde systemen, zoals het RBS, waarin verschillende politieregisters worden gevoerd die elk onder een eigen afzonderlijk privacyregime vallen en waarvoor dus evenzoveel reglementen moeten worden opgesteld.

---

117 Besluit van 14 februari 1991, houdende bepalingen ter uitvoering van de Wet politieregisters. Stb. 56, 1991.

Het vierde knelpunt zag op de *onbekendheid van politieambtenaren met de wettelijke regelingen*. Uit een enquête onder het politiepersoneel bleek dat een kwart van de ondervraagden niet op de hoogte was van het bestaan van de Wpolr en de Bpolr. In aanvulling daarop concludeerden de onderzoekers dat er bij politieambtenaren ruimte was voor verbetering van kennis van de verschillende privacyregelingen.

Constatering 1
Bij dit onderzoek merken we op dat de resultaten gerelativeerd moeten worden vanwege de gedateerdheid van het onderzoek na de inwerkingtreding van de Wpolg en de Bpolg op 1 januari 2008. Bovendien vond het evaluatieonderzoek plaats in de periode na de invoering van de Politiewet 1993 die leidde tot een ingrijpende reorganisatie van de politiekorpsen. Door deze reorganisatie werd de implementatie van de Wpolr en Bpolr in veel regio's vertraagd, hetgeen de resultaten van het evaluatieonderzoek kleurt. Desondanks menen wij dat de resultaten van het onderzoek wel van belang zijn omdat deze geplaatst kunnen worden in een bredere ontwikkeling.

5.1.2 Onderzoek 1998: Uitwisseling recherche-informatie

In 1997 deed de Algemene Rekenkamer onderzoek naar de divisie Centrale Recherche Informatie (CRI) en de uitwisseling van informatie tussen de CRI en de politieregio's.[118] De CRI was in die periode ondergebracht bij het KLPD (thans is de CRI opgegaan in de Dienst Nationale Recherche Informatie (DNRI)). Het toenmalige CRI had tot belangrijkste doel de ondersteuning van politie en justitie bij de bestrijding van zware georganiseerde criminaliteit. Voor de uitvoering daarvan onderhield het CRI contacten met diverse justitiële en politiële instellingen in binnen- en buitenland. Op recherchegebied vormden de toenmalige CID-en de belangrijkste contacten voor informatie-uitwisseling met de divisie CRI. De DNRI is van belang omdat het ook nu nog een centrale rol vervult in de interregionale uitwisseling van criminele inlichtingen.

De algemene conclusie van het onderzoek luidde dat er ernstige gebreken waren in de gehele recherche-informatieketen, zowel (1) de informatieverstrekking aan de CRI, als ook (2) de informatieveredeling door het CRI, en (3) de informatieverstrekking van de CRI aan de regio's vertoonden gebreken. De Algemene Rekenkamer onderscheidde in het onderzoek vier aandachtsgebieden die wij hier verder zullen duiden als knelpunten. Het zijn: (1) een gebrekkige kwaliteit van de gegevens, (2) onduidelijke privacyregels, (3) onvoldoende standaardisatie, en (4) onvoldoende onderling vertrouwen.

118 *Kamerstukken II* 1998/99, 26 215, nr. 2.

(1) *Gebrekkige kwaliteit:* De Rekenkamer constateerde dat de kwaliteit (juistheid, volledigheid en tijdigheid) van de geregistreerde recherche-informatie manco's vertoonde. Het ging daarbij zowel om de informatie die door de regio's werd aangeleverd als de recherche-informatie die door de CRI beschikbaar werd gesteld aan de regio's. De Rekenkamer wees erop dat dit onder andere te maken had met de matige tot slechte kwaliteit van de aangeleverde onderliggende informatie en het slecht doorgeven van mutaties. Daarnaast ontbrak het ook aan het systematisch terugkoppelen van gegevens met de regio's. Het gevolg daarvan was dat er veel onjuistheden en onvolledigheden zaten in de registraties van rechercheonderzoeken bij de CRI. Bovendien schoot de effectiviteit van de landelijke informatiecoördinatie van het CRI tekort.

(2) *Onduidelijke privacyregels*: De Rekenkamer constateerde verder dat de organisatorische en de juridische situatie rond het doorgeven van recherche-informatie onvoldoende helder waren. Zo waren de taken en plichten van de verschillende actoren onvoldoende vastgelegd en ontbrak een helder juridisch kader.

(3) *Onvoldoende standaardisatie:* De Rekenkamer constateerde vervolgens dat er ernstige complicaties voortvloeien uit de grote regionale verschillen op het gebied van automatisering. Deze complicaties werden mede veroorzaakt door onvoldoende standaardisatie en afstemming tussen de regio's.

(4) *Onvoldoende onderling vertrouwen:* Ten slotte constateerde de Rekenkamer een gebrek aan vertrouwen tussen politieambtenaren onderling. Dit gebrekkige vertrouwen had tot gevolg dat er weinig wil was tot samenwerking binnen de Nederlandse politie waar het ging om informatieuitwisseling. De Rekenkamer wees erop dat dit deels kwam doordat politieambtenaren zich onvoldoende bewust waren van het belang van hun informatie voor andere politieregio's.

Constatering 2
Wanneer wij deze resultaten vergelijken met het onderzoek van Cozijn e.a. (1996) dan valt op dat ook Cozijn een relatieve onbekendheid van politieambtenaren met de privacyregelingen constateerde. Onduidelijkheid en onbekendheid zijn daarbij elkaar versterkende factoren. Wanneer regels onduidelijk zijn, ligt het voor de hand dat politieambtenaren daarmee sneller onbekend zijn omdat de regels niet worden begrepen.

5.1.3 Onderzoek 2002: Uitwisseling van opsporingsinformatie

In aanvulling op het in de vorige subsectie besproken onderzoek deed de Algemene Rekenkamer van juni tot september 2001 aanvullend onderzoek

naar de uitwisseling van opsporings- en terrorisme-informatie.[119] Wij merken op dat er op organisatorisch niveau ten opzichte van de situatie in 1998 een en ander ingrijpend gewijzigd is. De belangrijkste wijziging betreft het opgaan van de CRI in de Dienst Nationale Recherche Informatie (DNRI). Deze dienst coördineerde opsporingsprocessen van het openbaar ministerie en de regionale politiekorpsen waarbij in het bijzonder de aandacht uitgaat naar de zware, de georganiseerde en de bovenregionale criminaliteit. Vanaf 9 april 2008 is de DNRI samengevoegd met de Dienst Internationale Politiesamenwerking[120] van het KLPD onder de naam Dienst IPOL. De taken van het DNRI (thans dus de Dienst IPOL) zijn voor wat betreft de bovenregionale gegevensverwerking dezelfde gebleven:

(1) het verzamelen, vastleggen, bewerken, analyseren, en verstrekken van gegevens en informatie;
(2) het ontwikkelen, delen, toepassen, en evalueren van expertise en kennis ten behoeve van de bestrijding van de zwaardere vormen van criminaliteit;
(3) de coördinatie en beleidsadvisering over de bestrijding van criminaliteit.

Organisatorisch was de DNRI onderverdeeld in negen diensteenheden (units) met een duidelijk afgebakend expertisegebied.[121] Voor de uitwisseling van criminele inlichtingen zijn de Unit Recherche Informatie Uitwisseling (RIU) en de Unit Nationaal Inzicht (NI) van belang.

De RIU is verantwoordelijk voor de samenwerking en verbetering van de uitwisseling van informatie tussen de opsporingsdiensten enerzijds en de DNRI anderzijds. De RIU heeft daartoe medewerkers gehuisvest in de directe nabijheid van de informatiedesks en de CIE-en van de regionale korpsen. Deze medewerkers moeten de schakel vormen tussen de regionale korpsen en de KLPD waarbij zij zich richten op het verzamelen en verstrekken van recherche-informatie die van bovenregionaal belang is.

De unit NI is verantwoordelijk voor het proces van vastleggen, bewerken en analyseren van de door de RIU aangeleverde informatie. De gegevens worden vastgelegd in gestandaardiseerde applicaties zodat de informatie ont-

119 *Kamerstukken II* 2002/03, 28 845, nr. 2.
120 De Dienst Internationale Politiesamenwerking verzorgde de samenwerking in brede zin tussen de Nederlandse Politie en buitenlandse politiediensten. Onder meer Interpol en Europol en het Nederlandse deel van het Schengen Informatie Systeem (SIS) zijn binnen de dienst georganiseerd.
121 De negen diensteenheden zijn: (1) Unit Recherche Informatie Uitwisseling, (2) Unit Nationaal Inzicht, (3) Unit Recherche Ondersteuning en Advies, (4) Unit Financiële Criminaliteit, (5) Unit Milieu Criminaliteit, (6) Unit Services en Migratiecriminaliteit, (7) Unit Ontwikkeling Kennis en Recherchetechnologie, (8) Unit Dactyloscopie en Identificatie, en (9) Unit Kennis en Onderzoek.

sloten kan worden voor de overige gebruikers. De Nationale Criminele Inlichtingeneenheid (NCIE) is onderdeel van de unit NI.

Zoals gezegd deed de Algemene Rekenkamer in 2001 opnieuw onderzoek naar de uitwisseling om te bezien in hoeverre de in 1998 geconstateerde knelpunten waren aangepakt. Zij kwam tot onder meer de volgende drie conclusies.

(1) *Onvoldoende standaardisatie:* De Rekenkamer stelde vast dat de verzameling en uitwisseling van criminele activiteiten binnen de politieorganisatie in 2002 nog steeds tekortkomingen vertoonde. Datzelfde gold voor de verzameling en uitwisseling van informatie op het gebied van terrorismebestrijding. Dat laatste was voor een belangrijk deel terug te voeren op het ontbreken van geautomatiseerde afstemming tussen het KLPD en de AIVD.

(2) *Onvoldoende verstrekkingen:* De Rekenkamer concludeerde dat ook in 2002 de aanlevering van informatie vanuit de regio's evenals de centrale verwerking van die informatie onvoldoende van de grond was gekomen. Hierdoor bleef het risico bestaan op overlapping en het onvoldoende afstemmen van opsporingsonderzoeken.

(3) *Gebrekkige kwaliteit:* De Rekenkamer constateerde dat er nog altijd sprake is van een matige kwaliteit van de basisregistraties. Dit had voor een deel ook te maken met de diversiteit van de basisregistratiesystemen waardoor geautomatiseerde aanlevering van gegevens nog altijd niet mogelijk was.

Constatering 3
Hoewel de Rekenkamer daar niet expliciet op wees kan uit de onderzoeksresultaten een juridische tekortkoming in het regelgevend kader voor de informatie-uitwisseling worden afgeleid. De regionale politiekorpsen dragen de verantwoordelijkheid om informatie door te geven aan het NRI. Deze verantwoordelijkheid kent evenwel geen wettelijke basis. De Regeling Opsporingsinformatie Regionale Politiekorpsen en de CIE-regeling leggen weliswaar de verplichting op de regionale korpsen om de relevante opsporingsgegevens te registreren en aan het KLPD ter beschikking te stellen. Het probleem is echter dat de DNRI geen bevoegdheden heeft om in te grijpen wanneer de regiokorpsen dit nalaten. De DNRI is daarmee in grote mate afhankelijk van de vrijwillige medewerking van de korpsen.

Wanneer wij de drie genoemde conclusies vergelijken met de conclusies van de Algemene Rekenkamer uit 1998 dan valt op dat er sprake is van grote overlap in knelpunten waarop de conclusies gebaseerd zijn. Dit betekent dat de politieorganisatie in de tussenliggende periode kennelijk niet in staat is geweest om deze punten op te lossen.

5.1.4 Onderzoek 2004: Uitwisseling politie-informatie

Mede naar aanleiding van het hiervoor besproken onderzoek door de Algemene Rekenkamer deed de Inspectie OOV een evaluatieonderzoek naar de maatregelen die zijn genomen om de problemen in de informatie-uitwisseling tussen de regio's en de NRI aan te pakken (Koolen en Moonen, 2004). Een van de maatregelen naar aanleiding van de besproken onderzoeken van de Rekenkamer was het starten van het project Landelijke Informatie Coördinatie (LIC) waarin een nieuwe informatiestructuur voor de politieorganisatie werd opgezet. De inspectie OVV keek in dat licht vooral naar wat het LIC-project opleverde en welke verbeteringen op het gebied van de informatie-uitwisseling op landelijk en regionaal niveau werden gerealiseerd.

Voor een goed begrip van deze evaluatie is het van belang om de wijzigingen die met het LIC-project zijn doorgevoerd in de organisatie rondom de informatiestromen kort te bespreken.

De gewijzigde structuur is opgebouwd uit een Nationaal Informatie Knooppunt (NIK), een Regionaal Informatie Knooppunt (RIK) en Districtelijke Informatie Knooppunten (DIK). De gedachte achter de opzet van deze drie knooppunten is dat deze functioneren als gelegenheidsorganisatie. Onder normale omstandigheden is er sprake van een zogenaamde 'waakvlamfunctie' maar bij een acute dreiging moet lokaal en regionaal aanwezige informatie via de knooppunten worden doorgeleid naar nationaal niveau. Op nationaal niveau komt alle informatie samen bij de Nationaal Coördinator Bewaking en Beveiliging (NCCB) of het Nationaal Coördinatie Centrum (NCC). Deze organisaties coördineren op basis van alle beschikbare de informatie de eventuele te nemen acties.

Hoewel deze structuur op zichzelf eenvoudig is constateerde de Inspectie OOV dat er naast de LIC-structuur voor de informatie-uitwisseling diverse andere communicatielijnen gebruikt werden waardoor uiteindelijk onduidelijk is langs welke organisatielijnen gecommuniceerd moet worden. De Inspectie OOV constateerde naast de informatie-uitwisseling via de structuur van districtelijke en regionale knooppunten onder meer de volgende communicatielijnen:

- de Regionale Inlichtingen Diensten (RID) bij de politiekorpsen hebben een aparte lijn met de Algemene Inlichtingen en Veiligheidsdienst (AIVD);
- de Criminele Inlichtingen Eenheden (CIE) bij de regiokorpsen leveren hun informatie via een speciale lijn rechtstreeks aan de Nationale CIE bij de DNRI;

- de Nationaal Coördinator Bewaken en Beveiligen (NCBB) en het Nationaal Coördinatie Centrum (NCC) communiceren ook via de bestuurlijke lijn (Commissaris van de Koningin, de burgemeester/korpsbeheerder) of hebben eigen contactpersonen bij de korpsen;
- Veel bilateraal contact vindt plaats binnen persoonlijke netwerken tussen ambtenaren op nationaal en regionaal niveau.

De Inspectie OOV was naar aanleiding van haar evaluatieonderzoek allereerst van oordeel dat de Nederlandse politie een goede weg is ingeslagen met de ontwikkeling van een landelijke informatiecoördinatie. Zij overwoog daarbij dat:

> "De richting naar een cultuur van informatie delen en samenwerken, naar een informatiegestuurde werkwijze in en tussen de korpsen en meer landelijke afstemming en uniformering op het gebied van informatie, registratie en ICT, is de juiste." (Koolen en Moonen, 2004, p. 19)

De Inspectie OOV merkt daarnaast echter op dat het systeem van informatie-uitwisseling zich weliswaar in de goede richting ontwikkelde maar dat het desondanks nog niet optimaal werkte. Evenals de Algemene Rekenkamer constateerde ook de inspectie een aantal knelpunten die moesten worden opgelost. Hieronder bespreken wij zes knelpunten.

(1) *Onvoldoende regie:* De inspectie stelde dat meer aandacht gegeven moet worden aan een vereenvoudiging van de algehele bestuurlijke structuur van de informatie-uitwisseling. Er moest een duidelijke regie worden gevoerd op de samenhang tussen de verschillende ontwikkelingen die gaande zijn op zowel het gebied van de automatisering als op organisatorisch niveau met betrekking tot het inrichten van werkprocessen. Zonder een dergelijke regie is volgens de inspectie het risico aanwezig dat de verschillende ontwikkelingen elkaar tegenwerken en/of vertragen.

(2) *Onduidelijke doelstelling:* Er bestond nog altijd onduidelijkheid over de vraag of de RIK- en NIK-lijnen uitsluitend bedoeld zijn voor de zeer ernstige zaken of voor alle zaken. Deze onduidelijkheid hindert een effectief gebruik van het LIC-systeem.

(3) *Complexe verantwoordelijkheidsstructuur:* De Inspectie OVV zette verder vraagtekens bij de verantwoordelijkheidsstructuur van het LIC-systeem. Daarin wordt een rol vervuld door de Raad van Hoofdcommissarissen, door de Board Opsporing die daaronder functioneert, door de strategische beleidsgroep die onderdeel uitmaakt van de Board, en de expertgroep die weer onderdeel uitmaakt van de strategische beleidsgroep. Daarnaast spelen de KLPD en de DNRI een rol. De Inspectie OOV stelde dat in dit 'woud' van betrokkenen het niet duidelijk is welk orgaan verantwoordelijk is voor het monitoren of doorontwikkelen van het sys-

teem. Bovendien ontbreken beoordelingscriteria aan de hand waarvan kan worden vastgesteld of het systeem naar behoren werkt. De Inspectie OOV meent in dit verband dat de DNRI een grotere voortrekkersrol moet gaan vervullen en meer aandacht moet besteden aan de coördinatie en controle op wat er binnen de NIK- en RIK-lijn gebeurt.

(4) *Onvoldoende standaardisatie:* De Inspectie OOV stelde voorts vast dat er binnen de politieorganisatie nog altijd een grote diversiteit in informatiesystemen bestaat. Uit het onderzoek blijkt dat ook de verschillende korpsen het ontbreken van een uniforme informatiehuishouding beschouwen als een belemmering voor een voortvarende informatie-uitwisseling. Wij hebben in subsectie 4.1.2 ten aanzien van de interregionale informatie-uitwisseling tussen de CIE-en geconstateerd dat het gebruik van verschillende soorten informatiesystemen binnen de regionale CIE-en sinds de jaren negentig aanzienlijk is teruggedrongen. Om die reden speelt de onvoldoende standaardisatie een minder grote rol bij de uitwisseling van informatie tussen CIE-en onderling maar doet dit knelpunt zich vooral voelen in de informatie-uitwisseling met ketenpartners.

(5) *Onvoldoende vertrouwen:* De Inspectie OVV wees vervolgens op het ontbreken van een adequaat terugkoppelingsmechanisme van de DNRI naar de regiokorpsen. Dit heeft tot gevolg dat het onderlinge vertrouwen wordt ondermijnd en de DNRI vooral gezien wordt als een organisatie die alleen maar informatie inwint in plaats van uitwisselt.

(6) *Gesloten cultuur:* De Inspectie OOV constateerde ten slotte dat er nog altijd sprake was van een gesloten politiecultuur waarin informatie-uitwisseling niet vanzelfsprekend is. Deze cultuur is terug te vinden op alle organisatieniveaus. Dat wil zeggen dat deze cultuur een rol speelt in de informatie-uitwisseling tussen politieregio's met de NRI maar ook tussen regio's onderling en zelfs tussen verschillende teams en diensten binnen een regio.

Constatering 4
Wanneer wij deze zes knelpunten vergelijken met de knelpunten die de Algemene Rekenmaker in 2002 constateerde dan valt opnieuw op dat er een grote overlap bestaat tussen de knelpunten. Het onvoldoende vertrouwen in de regio's onderling, de daarmee samenhangende gesloten politiecultuur als het gaat om informatie-uitwisseling en de onvoldoende standaardisatie van informatiesystemen, de input en output, blijven ook in 2004 knelpunten. Opvallend is dat de Inspectie OOV meer dan de Rekenkamer aandacht besteedt aan de mogelijke oorzaak van het voortbestaan van deze knelpunten. Zij wijzen op (1) onvoldoende regie bij het oplossen van de knelpunten, (2) op onduidelijke doelstellingen en (3) een complexe verantwoordelijkheidsstructuur.

5.1.5 Onderzoek 2005: Evaluatie Wet bijzondere politieregisters

In art. 30a van de Wet bijzondere politieregisters was bepaald dat vier jaar na de inwerkingtreding van deze wet er een evaluatie diende plaats te vinden naar de gevolgen en doeltreffendheid van de wet. Het evaluatieonderzoek werd uitgevoerd van april 2003 tot en met mei 2004. In ons onderzoek concentreren wij ons op de bevindingen van Schreuders e.a. (2005) met betrekking tot het verstrekken van informatie uit de registers zware criminaliteit en de voorlopige registers. We bespreken vier bevindingen die wij duiden als knelpunten.

(1) *Geen geformaliseerd beleid voor verstrekkingen:* Schreuders e.a. (2005) onderzochten de instructies en de bekendheid daarmee ten aanzien van het verstrekken van gegevens uit de genoemde registers:

> "(…) over instructies en de bekendheid daarmee is ten aanzien van het verstrekken van gegevens uit bijzondere politieregisters reeds opgemerkt dat er van een geformaliseerd schriftelijk vastgelegd beleid over in- en externe verstrekkingen ten aanzien van CIE-informatie geen sprake is en dat de aanwezige documenten voor de gebruikers vaak niet meer inzichtelijk of verouderd waren." (Schreuders e.a., 2005, p. 110).

Overigens zij opgemerkt dat dit knelpunt in andere onderzoeken al eerder naar voren was gekomen. Wij noemen het onderzoek van Van Ruth en Gunther Moor (1997) naar informatie-uitwisseling binnen de politieorganisatie. Zij signaleerden eveneens een relatieve onbekendheid van de verschillende privacyregelingen binnen de politie-organisatie.

> "Politiefunctionarissen op verschillende niveaus en van hoog tot laag, zijn niet of slechts in beperkte mate op de hoogte van de inhoud. Deze onbekendheid met de privacyregelingen heeft verschillende gevolgen. In de eerste plaats vervullen de regelingen niet die machtsfactor die zij in de praktijk ten aanzien van de informatiehuishouding hadden moeten vervullen. Men wordt in het dagelijks handelen meer geleid door een vaag en algemeen besef van 'geheimhouding' en het 'eigen geweten', dan door de regelgeving. In de tweede plaats leidt het vage bewustzijn ook tot vormen van ongewenst gedrag. Gebrekkige kennis leidt in de praktijk tot een teruggrijpen op informele methoden en onderhands gedrag: waarom risico's lopen als het immers ook anders kan? In zoverre werkt het bestaan van de regelgeving informele vormen van uitwisseling juist in de hand. Daarnaast wordt de regelgeving soms wel in stelling gebracht om 'bureaupolitiek' te bedrijven: informatie wordt niet verstrekt hoewel dit strikt genomen wel zou kunnen/moeten (Van Ruth en Gunther Moor, 1997, p. 98)."

De wetgever was zich in 1997 echter bewust van de ingewikkeldheid van de regelgeving. Dat blijkt onder meer uit hetgeen de Minister van Binnenlandse Zaken ten tijde van de totstandkoming van de Wet bijzondere politieregisters opmerkte:

> "Wij erkennen in de eerste plaats dat regelgeving op het gebied van de bescherming van de persoonlijke levenssfeer zich gezien de aard van dit rechtsgebied in het algemeen niet kenmerkt door eenvoud en overzichtelijkheid. (…) Met name bij de bescherming van de persoonlijke levenssfeer in verband met de uitvoering van de politietaak heeft deze belangenafweging geresulteerd in relatief complexe regelgeving."[122]

(2) *Complexiteit en gedetailleerdheid regelgevin*g: Schreuders e.a. wezen er verder op dat het verstrekkingenregime erg gedetailleerd was vormgegeven waardoor het op onderdelen voor ambtenaren die werkzaam zijn in de praktijk van alledag, te lastig is om deze regels te doorgronden. In het verlengde daarvan wordt gewezen op het feit dat het een moeilijke en moeizame opgave blijft om het benodigde kennisniveau over deze regelgeving vast te houden.

(3) Protocolplicht: Daarnaast vormde het protocolleren van de verstrekkingen langs geautomatiseerde weg een probleem doordat de systemen daar niet op zijn toegesneden. De onderzoekers merken daarbij op dat er onduidelijkheid bestaat met betrekking tot de vraag in hoeverre de protocollering wordt gebruikt voor controle en toezicht op de naleving van de wettelijke regels ten aanzien van het verstrekken van gegevens.

(4) Onvoldoende standaardisatie: Ten slotte constateerden de onderzoekers dat de wijze varieert waarop de informatiehuishouding binnen de korpsen georganiseerd is. Dat is met name het geval als het gaat om de organisatorische inbedding van de verhouding tussen CIE, een infodesk en een afdeling belast met misdaadanalyse. Dit vloeit voor een deel voort uit het feit dat het niet altijd duidelijk is of de analysetaak moet worden uitgevoerd door (1) de CIE zelf, (2) door een bureau Misdaadanalyse of (3) door analisten van een Infodesk.

> "De bevindingen wijzen ook uit dat vanwege de complexiteit en diversiteit aan regelgeving op het gebied van organisatie en informatiehuishouding van de politie afstemming tussen de daarmee samenhangende uitvoeringsregelingen te wensen over laat. Dit klemt des te meer, nu de landelijke ontwikkelingen op het terrein van het delen van politie-informatie, steeds meer aandacht vragen voor een effectief en efficiënt beheersen van de integriteit, exclusiviteit en beschikbaarheid van politie-informatie (Schreuder e.a. 2005)."

Constatering 5

Wanneer wij deze bevindingen vergelijken met de eerder besproken onderzoek dan constateren wij opnieuw dat er sprake is van terugkerende knelpunten. Met name in het onderzoek van Cozijn e.a. (1996) werden de genoemde knelpunten al eerder geconstateerd. Nieuw is de conclusie dat het ontbreekt aan een geformaliseerd beleid voor de verstrekkingen.

122 *Kamerstukken II* 1997/98, 25 398, nr. 6.

5.2 Onderzoek 2005-2006: Eigen veldwerk

In het kader van dit promotieonderzoek hebben wij binnen het ANITA-project vanaf februari 2005 tot en met januari 2006 negen gesprekken gevoerd met politieambtenaren van de CIE. Zoals wij uiteengezet hebben in subsectie 1.7.2 hadden de gesprekken primair tot doel inzicht te verkrijgen in de wijze waarop de informatie-uitwisseling in de praktijk verloopt en na te gaan in hoeverre de hiervoor geconstateerde knelpunten een probleem vormen in de CIE-praktijk. De resultaten van ons veldwerk hebben wij ter nadere validatie voorgelegd aan organisatiedeskundige van de politie, de heer Johan Oostveen. Onze bevindingen zijn:

(1) Onvoldoende standaardisatie: In de gesprekken kwam naar voren dat de pluriformiteit van de informatiesystemen niet meer het belangrijkste technische knelpunt vormt voor de uitwisseling van informatie tussen CIE-en onderling. Wel worden binnen andere onderdelen van de politieorganisatie, zoals de recherche en de RID, verschillende informatiesystemen gebruikt. Datzelfde geldt voor ketenpartners. Het gebrek aan standaardisatie vormt daarmee vooral een knelpunt bij de elektronische uitwisseling van informatie met andere organisatie-onderdelen en ketenpartners.

(2) G*ebrekkige functionaliteiten informatiesystemen:* Dit knelpunt ziet op de belemmeringen die voortvloeien uit de technische mogelijkheden van de informatiesystemen. In de gesprekken werd gewezen op een aantal technische nadelen van de systemen. We noemen de vier meest in het oogspringende nadelen die tezamen geduid kunnen worden als een knelpunt met betrekking tot de functionaliteit van de informatiesystemen.
   (a) Er werd gewezen op het feit dat het *invoeren* van gegevens in de systemen een omslachtige en tijdrovende bezigheid is (zie ook: Klerks e.a., 2002).
   (b) Verder kunnen de geregistreerde gegevens niet optimaal worden *teruggevonden* doordat bepaalde velden in het systeem niet geïndexeerd zijn voor de zoekmachine in het systeem. Het gevolg daarvan is dat het niet valt uit te sluiten dat cruciale informatie misschien wel in het systeem zit, maar er niet gericht kan worden uitgehaald, althans niet via de huidige zoekmogelijkheden.
   (c) De systemen zijn over het algemeen niet of onvoldoende geschikt voor het *systematisch bevragen* voor analyse- en managementdoeleinden. Zo blijkt het niet mogelijk om informatie op bepaalde categorieën (bijvoorbeeld nationaliteit) te filteren.
   (d) Op het gebied van de prestatie van de systemen kan nog veel verbeterd worden, zeker waar het gaat om de *snelheid en gebruiksvriendelijkheid* van communicatie tussen de systemen.

Om het laatste knelpunt te verbeteren zijn verschillende oplossingen ontwikkeld waaronder een separaat gevoerd centraal indexsysteem VROS. Dit systeem vergelijkt echter slechts één keer per week de uit de registers aangeleverde subjecten waardoor de informatie niet up-to-date is. Daarnaast ontsluit dit systeem geen detailinformatie en voorziet het niet in de mogelijkheid om complexere zoekvragen te beantwoorden. Voor een deel werden deze beperkingen opgelost door het implementeren van het PZU-SYSTEEM.

(3) *Gesloten cultuur:* Uit de gesprekken kwam naar voren dat er nog altijd sprake is van een cultuur van geslotenheid rondom CIE-informatie. Hoewel de uitwisselingscultuur tussen de eenheden zelf langzaam maar zeker verbetert, zijn de CIE-en met name waar het gaat om de verticale uitwisseling met de verschillende ketenpartners, nog altijd zeer terughoudend. Regionale CIE-en laten bij de belangenafweging die ten grondslag ligt aan de uitwisseling vaak het belang van lokale afscherming van bronnen zwaarder wegen dan het belang van hun inlichtingen voor de opsporing.

(4) Arbeidsintensief proces: In de gesprekken werd gewezen op de arbeidsintensiviteit van het uitwisselingsproces. De noodzaak die door CIE-chefs wordt gevoeld om iedere verstrekking van informatie te controleren maakt dat de capaciteit om informatie uit te wisselen zeer beperkt is. Daarbij komt dat de hoeveelheid aanwezige informatie te groot is om daarover goed overzicht te hebben. Ter illustratie: uit een onderzoek van het Cbp in 2004 bleek dat er destijds ongeveer 50.000 subjecten geregistreerd stonden bij de verschillende korpsen. Iedere regio heeft met andere woorden gemiddeld zo'n 2.000 subjecten in het lokale zwacri-register staan. Dit betekende dat er binnen een CIE geen van de politieambtenaren een volledig overzicht heeft betrekking tot de geregistreerde subjecten. Er staat zodoende veel informatie geregistreerd zonder dat daar verder iets mee wordt gedaan. Een beperkte personele capaciteit heeft daarnaast gevolgen voor de verificatie van de betrouwbaarheid en kwaliteit, maar kan er ook toe leiden dat informatie onterecht of te lang in het register blijft opgeslagen.[123]

(5) Ontoereikende privacywaarborgen: In de verschillende gesprekken hebben wij ook gevraagd naar het functioneren van de (onafhankelijke) toezicht- en controlemechanismen ten aanzien van de privacyregelgeving. In de praktijk hebben de CIE-en vooral te maken met (1) de CIE-officier van justitie, (2) de privacyfunctionaris en (3) het Cbp.

123 Dit houdt in dat gegevens worden opgeslagen onder afhandelingscode 00, wat zoveel betekent als 'niet geschikt voor operationele doeleinden', en daarmee dat deze informatie niet gedeeld mag worden met anderen.

In de gesprekken werd door de geïnterviewden CIE-hoofden aangegeven dat regelmatig (veelal wekelijks) overleg plaatsvindt met de officier van justitie. Daarbij worden de twijfelgevallen besproken. Het gaat met betrekking tot de gegevensverwerking dan om de vraag of bepaalde informatie wel of niet geregistreerd mag worden en of bepaalde informatie al dan niet uitgewisseld kan worden. Enkele regio's gaven aan dat de officier van justitie ook actief de registraties controleert door steekproefsgewijs na te gaan wat er per subject geregistreerd staat. In sommige regio's controleert de officier achteraf *alle* geregistreerde subjecten.

De informatieverwerking kan verder gecontroleerd worden door een privacyfunctionaris. Uit de gesprekken kwam evenwel naar voren dat de privacyfunctionaris niet of nauwelijks functioneert als controlemechanisme voor de CIE. Zo heeft hij geen toegang tot de registratiesystemen en wordt hij in de praktijk niet geraadpleegd door CIE-ambtenaren. Kenmerkend is de volgende uitspraak van één van de geïnterviewde CIE-ers:

> *"Aan hem (de privacyfunctionaris) wordt geen informatie verstrekt, dat is in zijn eigen belang. Kennis van de inhoud kan hem toch alleen maar belasten."*

Dit lijkt een duidelijke aanwijzing te zijn dat het toezicht op de naleving van de privacyregels door de privacyfunctionaris tekortschiet omdat hij eenvoudigweg geen controle kan uitoefenen op registraties waartoe hij geen toegang heeft.

Ten slotte dient toezicht op de naleving van de privacywetgeving uitgeoefend te worden door het Cbp. Uit de gesprekken kwam naar voren dat in de dagelijkse CIE-praktijk het toezicht door het Cbp eveneens tekortschiet. De geïnterviewden CIE-ers gaven aan dat het Cbp maar zeer sporadisch de gegevensverwerkingen controleerde. Enkele CIE-en hadden nog nooit een controlebezoek van het Cbp gehad en bij anderen was dat ruim twee jaar geleden. Illustratief is hetgeen een van de geïnterviewden CIE-ers over de sporadische controles van het Cbp opmerkte.

> *"Het Cbp is hier twee jaar geleden geweest voor een bezoek. Het is te manipuleren, je weet wat je laat zien en je laat dus niet de registraties zien waarover je twijfelt of waarvan je weet dat ze niet kloppen. Je laat alleen die registraties zien die kloppen. Dat kan ook makkelijk omdat ze geen verstand van zaken hebben. Ze weten niet wat we precies doen en hoe de systemen werken."*

Het voorgaande citaat lijkt kenmerkend voor de wijze waarop het Cbp de controle uitvoert en dat betekent dat juist het onafhankelijke controle- en het toezichtsysteem ten aanzien van de naleving van privacyregels niet toereikend is. In de praktijk vindt de controle dan uitsluitend plaats door de officier van justitie. De overige onafhankelijke controle- en toezichtmechanismen zijn niet, althans onvoldoende toereikend.

5.3 Tussenconclusies

Wanneer wij de conclusies van de verschillende onderzoeken en ons eigen veldwerk vergelijken dan kan gesproken worden van een grote mate van overlap in de bevindingen ook al is er een tijdsverschil. Wij constateren met name vijf terugkerende knelpunten. Om die reden duiden wij deze aan als de hoofdknelpunten in de informatie-uitwisseling.

1. *Moeilijk toegankelijke juridische kennis:* Complexe wet- en regelgeving voor de verwerking van politiegegevens bemoeilijkt de naleving daarvan door politieambtenaren bij onder meer de uitwisseling.
2. *Ontoereikende gegevenscontrole*: Het gaat dan om onvoldoende controle op de juistheid, tijdigheid en volledigheid van de gegevens waardoor de kwaliteit van de opgeslagen gegevens te wensen over laat.
3. *Onvoldoende standaardisatie:* Diversiteit van de informatiesystemen en onvoldoende standaardisatie belemmeren de interne uitwisseling van gegevens en de externe uitwisseling met ketenpartners.
4. *Gesloten bedrijfscultuur:* Onvoldoende vertrouwen van politieambtenaren in elkaar heeft geleid tot een gesloten politiecultuur waarin het delen van informatie alles behalve vanzelfsprekend is.
5. *Ontoereikende privacywaarborgen:* De onafhankelijke controle- en toezichtmechanisme via de privacyfunctionaris en het Cbp schieten in de dagelijkse praktijk tekort waardoor er binnen de CIE nauwelijks prikkels zijn om privacyregels na te leven.

De overige geconstateerde knelpunten hebben niet zozeer met de organisatie of het juridisch kader te maken maar met het beleid dat wordt gevoerd bij de aanpak van de knelpunten. Voor de organisatieanalyse laten wij deze verder buiten beschouwing.

Wij signaleren voorts dat in samenhang met de in hoofdstuk 4 beschreven ontwikkeling van de informatie- en registratiesystemen binnen de CIE ook steeds hogere eisen gesteld worden aan de informatie-uitwisseling. Naarmate de technische mogelijkheden toenemen om elektronisch informatie te delen, nemen ook de eisen toe en wordt er van de politieorganisatie verwacht, en tot op zekere hoogte ook geëist, dat zij mee ontwikkelen met de technische mogelijkheden. Daarmee is sprake van een technologiegedreven ontwikkeling die ons inziens op termijn vrijwel zeker leidt tot het in het gedrang raken van het recht op de bescherming van de persoonlijke levensfeer. Wanneer immers (1) de mogelijkheden tot geautomatiseerde verwerking en uitwisseling toenemen en (2) verwacht wordt dat de politie op grotere schaal techniek gaat inzetten bij deze verwerkingen, dan staat daarmee het recht op privacy onder grote druk.

In het technologiedebat (sectie 1.5) schaarden wij ons reeds eerder aan de zijde van de technologisch-deterministen die stellen dat techniek zich onder meer ontwikkelt volgens het autonome principe dat efficiëntie gaat voor moraliteit. Uitgaande van deze autonome wetmatigheid is het ons inziens van groot belang dat er nieuwe methoden worden onderzocht die het recht op privacy effectiever waarborgen. Bij de technologische ontwikkeling in het politiedomein zou daarom niet eenzijdig de aandacht moeten worden gericht op het belang van de rechtshandhaving (efficiëntie). Wij menen dat meer aandacht zou moeten worden besteed aan de inzet van techniek in het belang van de rechtsbescherming (moraliteit). Dat de techniek daarvoor goede mogelijkheden biedt hebben wij laten zien in hoofdstuk 2. Op welke wijze deze technieken ingezet kunnen worden in de politieorganisatie is onderwerp van hoofdstuk 7.

6 Organisatieanalyse

In dit hoofdstuk nemen wij de hoofdknelpunten die we beschreven hebben in hoofdstuk 5 als vertrekpunt voor onze organisatieanalyse. Voor deze analyse gebruiken wij de CommonKads-methode. Sectie 6.1 geeft een toelichting op CommonKads. Vervolgens wordt de organisatie rond het proces van uitwisselen in kaart gebracht; sectie 6.2: organisatiemodellen en sectie 6.3: taakmodellen. Daarna geven wij in sectie 6.4 een antwoord op de derde onderzoeksvraag (OV 3). De organisatieanalyse vormt de basis voor de conceptuele voorstellen die wij in hoofdstuk 7 doen ter verbetering van de informatie-uitwisseling, onder ander door toepassing van MAS-technieken.

6.1 CommonKads-methode

In dit hoofdstuk stellen wij de vraag aan de orde: op welke wijze is de huidige uitwisseling van criminele inlichtingen ingericht en wat zijn daarin de (juridische) knelpunten? Voor de beantwoording van deze vraag hebben wij in ons onderzoek met behulp van de CommonKads-methode geanalyseerd welke taken in het proces van uitwisselen een rol spelen en waar normatieve beperkingen kunnen worden ingebouwd wanneer deeltaken verder worden geautomatiseerd.

Alvorens dieper op CommonKads en de toepassing van de modellen in te gaan maken wij drie opmerkingen die met CommonKads en ons onderzoek te maken hebben.

(1) Ons onderzoek heeft tot doel op conceptueel niveau een ontwerp te verkennen van een normatief multi-agentsysteem dat beoogt bij te dragen aan de verbetering van de uitwisseling van politiegegevens.
(2) CommonKads houdt zich vooral bezig met het modelleren van kennis ten behoeve van de ontwikkeling van kennissystemen. Tegenwoordig zijn voor veel onderdelen van kennissystemen gespecificeerde webservices ontwikkeld. Waar nodig gebruiken we die. Daarbij hebben we ontdekt dat veel normatief communicatiegedrag of onderdelen daarvan nog niet in webservices zijn omgezet.
(3) CommonKads besteedt nog weinig aandacht aan softwareagenten en aan Internet. In ons onderzoek wordt dit stilzwijgend gecompenseerd. Agenten spelen bij ons een hoofdrol, evenals Internet.

CommonKads (*Common Knowledge Acquisition and Design Structure*) is een methode voor het ontwerpen van kennissystemen. De methode stamt uit het

midden van de jaren tachtig en is voortgekomen uit de behoefte om bij de ontwikkeling van industriële kennissystemen gebruik te maken van een vaste methode (Schreiber e.a., 2000). Sinds 1995 wordt de methode gezien als de Europese standaard voor het modelleren van kennis, met inachtneming van de bovengenoemde opmerkingen (2) en (3). De keuze voor deze methode vloeit voort uit het interdisciplinaire karakter van het ANITA-project. Voor de uitwisseling van kennis tussen de AI-onderzoekers en de rechtswetenschappelijke onderzoekers met betrekking tot de CIE-organisatie, is veel gebruik gemaakt van de CommonKads-modellen. Binnen het project werd daarom gekozen voor de CommonKads-methode boven alternatieve modelleringsmethoden zoals bijvoorbeeld de Nijssen's Information Analysis Methodology (NIAM) (Nijssen, 1977). Commonkads sloot het beste aan bij de manier waarop de AI-onderzoekers binnen het project de multi-agenttoepassingen ontwikkelden.

Met behulp van drie categorieën van modellen wordt structuur aangebracht in de kennis van zogenaamde domeindeskundigen. Het doel van het op deze wijze ordenen van kennis is het vastleggen van een decompositie van taken die door de deskundigen in een voorgeschreven volgorde moeten worden uitgevoerd om de eindtaak (in ons geval: het opstellen van een organisatieanalyse voor het incorporeren van een normatief communicatiegedrag bij het uitwisselen van politiegegevens) te bereiken. Het betreft hier met name het selecteren van kennis die nodig is bij het oplossen van een probleem of het uitvoeren van een bepaalde taak. Voor onze onderzoeksvragen tekenen we aan dat het niet mogelijk is om alle kennis uit een deskundige te halen, omdat de kennis vrijwel zeker te veel impliciete details bevat en bovendien niet volledig toegankelijk is (zie daarover: Mommers, Koelewijn en Kielman, 2007). De CommonKads-methode heeft het selectieproces van *knowledge engineering* gebaseerd op vier basisprincipes. Het eerste principe sluit nauw aan bij wat hierboven is opgemerkt.

> (1) "Knowledge engineering is not some kind of 'mining from the expert's head,' but consists of constructing different aspect models of human knowledge." (Schreiber e.a., 2000, p. 15)

Dit principe is voortgekomen uit het inzicht dat het willekeurig kennis onttrekken aan een deskundige een weinig effectieve manier van werken is bij de ontwikkeling van kennissystemen. In CommonKads wordt *knowledge engineering* dan ook benaderd als een modelleringsactiviteit waarbij het model een bruikbare abstractie dient te zijn van de werkelijkheid. Slechts de kennis die nodig is voor het doel van het kennissysteem dient daarom te worden gemodelleerd. In de context van ons onderzoek ligt daarom de focus op de kennis die samenhangt met de rechtmatigheid van de uitwisseling van politiegegevens. Het tweede principe staat bekend als het *knowledge-level* principe.

> (2) "In knowledge modelling, first concentrate on the conceptual structure of knowledge, and leave the programming details for later." (Schreiber e.a., 2000, p. 16)

Vaak bestaat er bij software-ontwikkelaars de neiging om het precies andersom te doen. Het computersysteem wordt dan als uitgangspunt genomen bij het analyseren en ontwerpen van de taken. In de CommonKads-benadering gebeurt dat niet en is eerst en vooral de menselijke kant van het model van belang. Dit vloeit voort uit de gedachte dat bij *knowledge engineering* de kennis en het gedrag van deskundigen zich bevinden in een reële omgeving. Het te ontwikkelen computersysteem, de gebruikers, en de deskundigen zijn opgenomen in een georganiseerde context die op zijn beurt van invloed is op de wijze waarop taken worden uitgevoerd. Het derde principe gaat over de interne structuur van kennis.

> (3) "Knowledge has a stable internal structure that is analyzable by distinguishing specific knowledge types and roles." (Schreiber e.a., 2000, p. 16)

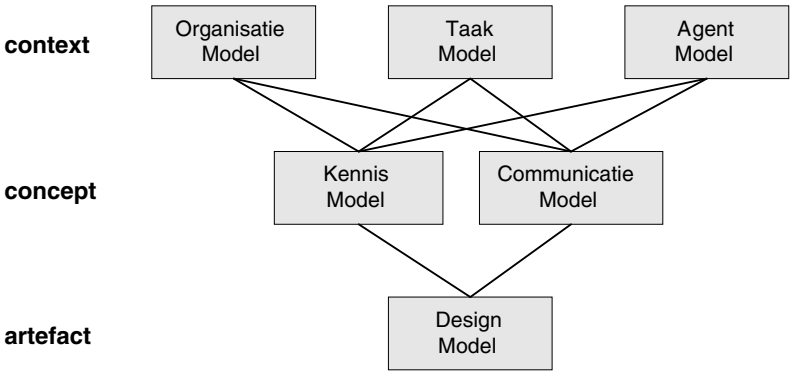
Hoewel kennis bijzonder complex kan zijn gaat de CommonKads methode er vanuit dat het nooit chaotisch is. Kennis blijkt een stabiele interne structuur te hebben die keer op keer dezelfde patronen laat zien. Conceptuele kennismodellen kunnen helpen bij het doorgronden van de wijze waarop mensen handelen bij het oplossen van problemen of het nemen van beslissingen in bepaalde situaties. Een belangrijk resultaat van onderzoek dat ziet op *knowledge engineering* is dat menselijke kennis nauwkeurig kan worden geanalyseerd in termen van generieke categorieën, patronen en structuren. Het vierde principe ziet op de projectmatige vormgeving van de methode.

> (4) "A knowledge project must be managed by learning from your experiences in a controlled 'spiral' way." (Schreiber e.a., 2000, p. 17)

In de CommonKads-methode is gekozen voor een uitgebalanceerd projectmanagement dat voorziet in het structureel ondernemen van stappen in het ontwikkelingsproces. De verschillende modellen vormen steeds de wegwijzer naar de volgende stap in het ontwikkelingsproces. In het onderhavige onderzoek hebben wij CommonKads gebruikt bij de analyse van de CIE-organisatie en het proces van informatie-uitwisseling. In hoofdstuk 7 borduren wij voort op deze organisatieanalyse en doen wij conceptuele voorstellen voor de toepassing van softwareagenten in het systeem van informatie-uitwisseling. In dit hoofdstuk wordt om die reden slechts gebruik gemaakt van de eerste fasen van de CommonKads-methode. Het is daarom niet van belang verder stil te staan bij het projectmanagement.

De methode voorziet verder in de hiervoor genoemde drie categorieën van modellen (zie figuur 6.1) die respectievelijk de volgende vragen beogen te beantwoorden.

(1) Context: Waarom moet het systeem gemaakt worden?
(2) Concept: Wat is de aard en de structuur van de benodigde kennis?
(3) Artefact: Hoe moet die kennis geïmplementeerd worden?



Figuur 6.1: Samenhang modellen.

De eerste categorie wordt gevormd door de context en daarin zitten drie modellen, een organisatiemodel, een taakmodel, en een agentmodel. Met behulp van deze modellen wordt een gestructureerde beschrijving gemaakt van de organisatorische context waarin de relevante taken van het bedrijfsproces worden uitgevoerd. In het agentmodel kan het in beginsel zowel gaan om menselijke actoren als om softwareprogramma's die een bepaalde taak uitvoeren. Wij gebruiken een royaal aangevuld agentmodel (zie nogmaals opmerking 2 en 3 hierboven) in hoofdstuk 7 om de verschillende rollen van de softwareagenten te beschrijven in het conceptueel model dat wij daarin voorstellen.

De tweede categorie bevat twee modellen: een kennismodel en een communicatiemodel. Zij zien beide op het conceptuele niveau van de te modelleren kennis. De modellen geven een analyse weer van de typen en de structuren van de benodigde kennis, en zij voorzien in een beschrijving van de communicatie tussen de betrokken agenten. Op deze wijze geven ze een conceptuele beschrijving voor de te gebruiken data en functies die nodig zijn om een taak uit te voeren.

De derde categorie wordt gevormd door het ontwerpmodel waarin wordt beschreven hoe de functies uit de kennis- en communicatiemodellen geïmplementeerd moeten worden. Dit model wordt beschreven in termen van architecturen en softwaremodulen. In ons onderzoek analyseren wij de mogelijkheden van softwareagenten bij de uitwisseling van criminele inlichtingen op conceptueel niveau. Dit houdt in dat er in dit onderzoek geen *design model* zal worden gemaakt en de verdere bespreking daarvan buiten beschouwing wordt gelaten (zie opmerking 1 hierboven).

Wij hebben voor de CommonKads-methode gekozen omdat het op deze wijze structureren en toepassen van kennis nauw aansluit bij de wijze waarop mensen dat in de praktijk doen. Mensen gebruiken een aantal cognitieve patronen waarmee ze hun waarnemingen organiseren en filteren. Deze cognitieve patronen zijn gericht op het verkrijgen van een bepaald resultaat of

op het trekken van conclusies. De CommonKads-methode beschrijft deze patronen om ze onder meer te kunnen gebruiken in redeneersystemen. Daarbij gaat het om redeneren over kennis en het aan de hand daarvan nemen van beslissingen. De benadering sluit goed aan bij het object van ons onderzoek. Het gaat immers in essentie over de vraag of bepaalde informatie al dan niet kan worden uitgewisseld.

6.2 Organisatiemodel

CommonKads gaat uit van het principe dat een kennissysteem bruikbaar is wanneer het bepaalde taken voor een gebruiker kan uitvoeren of wanneer het een gebruiker helpt bij het uitvoeren van bepaalde taken. Een kennissysteem kan zal echter pas succesvol zijn wanneer er oog is voor de organisatorische context en het geïntegreerd is in een bredere organisatorische context. Daarbij gaat CommonKads uit van de volgende zienswijze.

> "A knowledge system acts as one agent cooperating with many others, human and nonhuman, and it carries out just a fraction of the many tasks that are performed in the organization. Knowledge systems, like information systems in general, must thus be viewed as supporting components within the business processes of the organization – no less and no more." (Schreiber e.a., 2000, p. 25)

Vaak is het doel van de inzet van een kennissysteem de verbetering van bedrijfsprocessen. Dat is in feite iets anders dan de traditionele opvatting van het automatiseren van bepaalde taken. Het uitvoeren van kennisintensieve taken is veelal te complex om het volledig te automatiseren. Dat geldt ook voor het onderhavige onderzoeksdomein en daarom sluit de doelstelling van CommonKads goed aan bij de probleemstelling van dit onderzoek. Wij gebruiken derhalve voor de organisatie- en taakanalyse CommonKads en onderscheiden daarbij twee stappen.

1. Identificeer de knelpunten en de mogelijke oplossingen.
2. Verkrijg inzicht in de relaties tussen taken, agenten, en kennis.

Deze twee stappen worden door ons uitgewerkt in vier modellen. Bij de uitwerking hebben we ons, als gezegd, laten inspireren door Schreiber e.a. (2004). Zij hanteren een indeling in vijf modellen. Wij kiezen voor een iets andere aanpak vanwege onze specifieke zienswijze op het werk van de politie en volstaan daarom met vier modellen.

In subsectie 6.2.1 beschrijven wij het eerste organisatiemodel waarin de knelpunten en mogelijke oplossingen worden uitgewerkt. Subsectie 6.2.2 geeft een beschrijving van het tweede organisatiemodel waarin de relevante organisatorische context met betrekking tot de gegevensuitwisseling is opgenomen. Vervolgens geeft subsectie 6.2.3 een beschrijving van het derde organi-

satiemodel waarin het bedrijfsproces wordt ontleed in deeltaken en per deeltaak wordt aangegeven (1) in welke mate er kennis nodig is voor de uitvoering van die deeltaak en (2) welk soort kennis nodig is. Ten slotte wordt in subsectie 6.2.4 het vierde organisatiemodel beschreven waarin nader ingegaan wordt op de kenniselementen. Het gaat daarbij om de kennis die door de menselijke actoren of door software in een organisatie gebruikt worden bij de uitvoering van een deeltaak.

6.2.1 Organisatiemodel 1: knelpunten en oplossingen

In Organisatiemodel 1 concentreren wij ons op de knelpunten die zijn gesignaleerd in vijf onderzoeken en ons eigen veldwerk. Wij hebben daarin geconcludeerd dat er vijf hoofdknelpunten kunnen worden onderscheiden in het proces van elektronische informatie-uitwisseling. In tabel 6.1 categoriseren wij deze hoofdknelpunten naar de door ons in sectie 1.2 geconstateerde (1) juridische barrière, (2) bestuurlijke barrière en (3) technologische barrière in de elektronische informatie-uitwisseling. De hoofdknelpunten vormen de aanleiding en het vertrekpunt voor ons onderzoek naar de vraag in hoeverre MAS-technologie kan bijdragen aan het (gedeeltelijk) oplossen van de knelpunten en het verbeteren van de informatie-uitwisseling. Een korte beschrijving van Organisatiemodel 1 volgt hieronder.

Organisatiemodel 1	**Hoofdknelpunten**
Juridisch:	1. *Moeilijk toegankelijke juridische kennis*
	2. *Ontoereikende privacywaarborgen*
Bestuurlijk:	3. *Ontoereikende gegevenscontrole*
	4. *Gesloten bedrijfscultuur*
Technologisch:	5. *Onvoldoende standaardisatie*

Tabel 6.1: Hoofdknelpunten.

Moeilijk toegankelijke juridische kennis: Complexe wet- en regelgeving voor de verwerking van politiegegevens bemoeilijkt de naleving daarvan door politieambtenaren bij onder meer de uitwisseling. Hierdoor kunnen regionale verschillen ontstaan in de toepassing van de wettelijke regels hetgeen tot gevolg kan hebben dat juist te veel of juist te weinig informatie wordt gedeeld.

Ontoereikende privacywaarborgen: In het proces van geautomatiseerde gegevensuitwisseling schieten belangrijke onderdelen van de bestaande controle- en toezichtmechanismen (privacyfunctionaris en Cbp) tekort waardoor de waarborging van de rechtmatigheid van de elektronische gegevensverwerking en –uitwisseling, en daarmee dus het recht op privacy onder druk komt te staan.

Ontoereikende gegevenscontrole: Het gaat hier om de controle op de kwaliteit van de registraties. De kwaliteit wordt bepaald door de juistheid, tijdigheid,

en volledigheid van de geregistreerde gegevens. De controlemechanismen om die kwaliteit te waarborgen zijn onvoldoende toereikend gebleken.

Gesloten bedrijfscultuur: Onvoldoende onderling vertrouwen van politieambtenaren heeft geleid tot een gesloten politiecultuur waarin het uitwisselen van informatie alles behalve vanzelfsprekend is.

Onvoldoende standaardisatie: Diversiteit van de informatiesystemen en onvoldoende standaardisatie belemmeren de interne uitwisseling van gegevens tussen de CIE-en en andere onderdelen binnen de politieorganisatie en de externe uitwisseling van informatie met de verschillende ketenpartners.

In samenhang met deze hoofdknelpunten is voorts de organisatorische context (politieorganisatie) van de informatie-uitwisseling rondom de regionale CIE-en in kaart gebracht. Van belang is daarbij de door de Raad van Hoofdcommissarissen (RHC) geformuleerde missie en randvoorwaarden. Tot de organisatorische context rekent CommonKads ook externe factoren die van invloed zijn op de organisatie en de ontstane knelpunten. Daarom zijn voor de organisatorische context ook enkele strategische notities van belang, waarbij de ideeën van de RHC over de uitgangspunten voor de aanpak van de ontstane knelpunten worden uiteengezet.

Organisatiemodel 1	**Organisatorische context**
Relevante missie:	De ontwikkeling van de politieorganisatie tot een kennisintensieve organisatie die in een veranderende samenleving de vijf belangrijkste functies (handhaven, opsporen, noodhulp, signaleren en adviseren) adequaat kan blijven uitvoeren (zowel lokaal als nationaal).
Randvoorwaarde:	Voor het verwezenlijken van de missie is informatiegestuurd politiewerk (zie: Meesters, Kortekaas en Tragter, 2000) en informatie-uitwisseling in het gehele veiligheidsdomein noodzakelijk.
Externe factoren:	Wet- en regelgeving. Coördinatie en sturing op centraal en decentraal niveau. Bereidheid tot samenwerking van ketenpartners. Controle door toezichthouders. Tegenstrijdige belangen bij informatie-uitwisseling.
Strategische notities:[125]	De criminaliteitsbestrijding moet worden gederegionaliseerd en geïnternationaliseerd. De politie moet worden beschouwd als een coproducent in de openbare orde- en veiligheidsketen. De politie dient informatie zoveel mogelijk te personaliseren.

Tabel 6.2: Organisatorische context.

124 Raad van Hoofdcommissarissen, Wenkend perspectief. Strategische visie op politieel informatiemanagement en technologie 2006-2010, Projectgroep visie op de politiefunctie, 2006.

Ten slotte formuleren wij in Organisatiemodel 1 drie mogelijke oplossingsrichtingen via de inzet van kennissystemen en multi-agenttechnieken. De inzet van kennissystemen ziet erop om de betrokken politieambtenaren in het proces van informatie-uitwisseling te ondersteunen ten aanzien van het gebrek aan juridische kennis van de relevante wet- en regelgeving. Bovendien kan de toepassing van een kennissysteem in het proces van gegevensverwerking ook de kwaliteit van de registraties positief beïnvloeden. Daarbij kan gedacht worden aan korte adviezen van het systeem met betrekking tot de registratie van afhandelingscodes. Met name wanneer er informatiemutaties worden doorgevoerd ten aanzien van geregistreerde CIE-subjecten kan het systeem bevorderen dat de actualiteit van de afhandelingscodes wordt heroverwogen. In tabel 6.3 geven we drie mogelijke oplossingen.

Organisatiemodel 1	**Mogelijke oplossingen**
Registratie: Uitwisseling: Controle:	• Ondersteuning door registratiesysteem. • Automatiseer de standaard interne en externe uitwisseling. • Controleer geautomatiseerd de rechtmatigheid, juistheid, volledigheid en actualiteit.

Tabel 6.3: Mogelijke oplossingen.

Ondersteuning door registratiesysteem: Voor de informatie- en registratiesystemen is het ons inziens zinvol om applicaties in te zetten die de gebruiker ondersteunen bij het registreren van de gegevens. Daarbij kan worden gedacht aan verschillende toepassingen zoals een online assistent die de gebruiker attendeert op privacygevoeligheid van (delen van) de informatie of een applicatie die de gebruiker adviseert ten aanzien van de rechtmatigheid van de registratie. Dezelfde applicatie stelt de gebruiker bij de registratie van privacygevoelige informatie eerst enkele vragen die betrekking hebben op de noodzaak van de registratie van deze gevoelige gegevens en adviseert aan de hand van de antwoorden of de gegevens geregistreerd mogen worden. Bovendien kunnen de metadata (de vragen en de antwoorden) worden opgeslagen zodat achteraf door de toezichthouder (Cbp) de noodzaak van de registratie kan worden gecontroleerd.

Automatiseer de standaard interne en externe uitwisseling: Veel informatie-uitwisseling binnen de CIE-en vindt plaats ter verificatie van de eigen informatie. Voor een belangrijk deel kan deze uitwisseling worden geautomatiseerd. Zo zou het systeem bij de registratie van nieuwe subjecten of mutaties bij bestaande subjecten automatisch de nieuwe informatie kunnen verifiëren bij andere onderdelen binnen de politieorganisatie. Deze verificatie en uitwisseling zou volledig automatisch kunnen worden uitgevoerd door softwareagenten. Datzelfde geldt voor de verificatie met externe bronnen. Ook hier geldt dat softwareagenten ingezet zouden kunnen worden om na te gaan of aanvullende informatie kan worden gevonden via elektronische toegankelijke openbare bronnen op Internet. Via dergelijke bronnen kunnen in de toe-

komst mogelijk bruikbare relaties worden gelegd tussen geregistreerde CIE-subjecten. Wij merken op dat daarvoor wel een gestandaardiseerde uitwisselingstaal nog is (XML) en in veel gevallen ook de medewerking van het betreffende internetbedrijf. Deze dient immers de geregistreerde informatie aan te leveren in de standaardtaal.

Controleer geautomatiseerd de rechtmatigheid, juistheid, volledigheid en actualiteit: In de politiële informatiesystemen zouden softwareagenten kunnen worden ingezet die automatisch controles uitvoeren op de rechtmatigheid, juistheid, volledigheid, en actualiteit van de geregistreerde gegevens. Daarbij gaat het om (1) de controle op de bewaartermijnen en (2) de rechtmatigheid van gegevensverstrekkingen aan derden. Ook zouden softwareagenten extra controles kunnen uitvoeren op de juistheid en volledigheid van geregistreerde subjecten door geautomatiseerde verificatie van de gegevens met andere politiedatabases of de GBA. Datzelfde geldt voor de actualiteit van de gegevens met betrekking tot de woon- of verblijfplaats. Door middel van de toepassing van softwareagenten kan permanent worden nagegaan of ten aanzien van een CIE-subject op enig moment in een andere regio aanvullende informatie beschikbaar is die ook voor het andere onderzoek bruikbaar is.

6.2.2 Organisatiemodel 2: Beschrijving van organisatorische aspecten

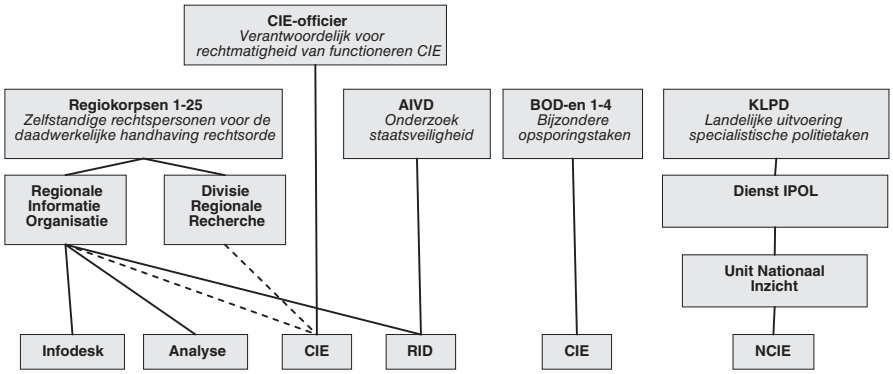
In Organisatiemodel 2 wordt gekeken (1) hoe een bedrijfsproces is gestructureerd, en (2) welke functies binnen de organisatie erbij betrokken zijn. Daartoe zijn in Organisatiemodel 2 vijf variabele factoren opgenomen die algemeen gelden als niet constant binnen een organisatie. Deze variabele factoren kunnen wijzigen als gevolg van het introduceren van een kennissysteem in de organisatie. Hieronder worden in tabel 6.4 de vijf variabele factoren beschreven.

Organisatiemodel 2	**Variabele factoren**
Structuur:	Figuur 6.2 en 6.3
Betrokken personen:	Figuur 6.3
Kennis:	Juridische kennis
Organisatiecultuur:	Kennis gebaseerd op ervaring
	Variabele kennis
	Hiërarchische organisatie
	Gesloten bedrijfscultuur

Tabel 6.4: Organisatorische aspecten.

Figuur 6.2 geeft inzicht in de organisatorische inbedding van de CIE-en binnen de politieorganisatie en de verhouding tot de belangrijkste interne en externe ketenpartners waarmee informatie wordt uitgewisseld. In het bijzonder gaat het daarbij om de hiërarchische verhouding tussen de verschil-

lende organisatieonderdelen binnen de politieorganisatie. Met elk van de organisatieonderdelen wordt op regionaal en nationaal niveau informatie uitgewisseld.



Figuur 6.2: Organisatorische inbedding CIE.

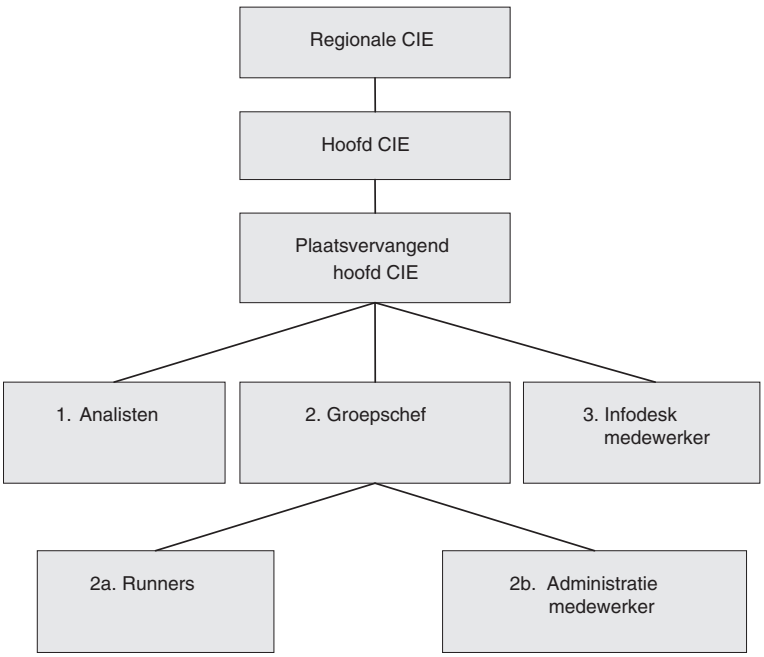
Het uitgangspunt voor de hiërarchische verhoudingen zijn de 25 zelfstandige politiekorpsen, de AIVD, de bijzondere opsporingsdiensten[125] (BOD-en) en het KLPD. De BOD-en en het KLPD hebben ieder een eigen CIE die zich richt op de verzameling en verwerking van informatie op specifieke deeltereinen van de opsporing van strafbare feiten. Deze CIE-en hebben ten aanzien van de informatieverwerking en uitwisseling dezelfde taken en kunnen dezelfde bevoegdheden uitoefenen als de regionale CIE-en.

Een bijzondere positie in de hiërarchie is toegekend aan de CIE-officier van justitie die vanuit het openbaar ministerie gezag uitoefent over alle werkzaamheden van de onder hem ressorterende CIE. Deze bepaalt de kaders waarbinnen de werkzaamheden moeten worden uitgevoerd en geeft aanwijzingen die door de CIE in acht moeten worden genomen. De AIVD verzamelt, verwerkt, en analyseert informatie in het belang van de nationale veiligheid.[126] Onder het gezag van de AIVD zijn regionale inlichtingendiensten (RID-en) geplaatst bij de regiokorpsen om regionaal informatie te verzamelen via het runnen van informanten en het onttrekken van informatie bij de andere diensten binnen het korps waaronder de CIE-en. De tweede gezagslijn naar de RID-en verloopt via de Regionale Informatie Organisatie (RIO). Concreet betekent dit dat de RID-en zowel worden aangestuurd vanuit de regiokorpsen (openbare orde) als vanuit de AIVD (staatsveiligheid). Bij de RIO binnen een regiokorps vindt de coördinatie van de verschillende informatiestromen binnen het korps plaats. Vanuit de RIO wordt de informatie uitgewisseld met andere korpsen en met de betrokken ketenpartners. Onder

125 FIOD-ECD, AID, SIOD, Inlichtingen en opsporingsdienst van het ministerie van VROM.
126 Zie art. 6 Wiv 2002

deze afdeling werkt de Infodesk. De infodesk vormt de belangrijkste schakel in de informatievoorziening aan individuele politieambtenaren. In enkele regionale korpsen is de CIE niet onder het gezag van de RIO gebracht maar functioneert de CIE nog onder het rechtstreekse gezag van de divisie recherche. In figuur 6.2 zijn deze twee verschillende organisatorische gezagsrelaties aangeduid met een stippellijn.

Een vergelijkbare taak als de RIO heeft de Dienst IPOL bij de KLPD met dat verschil dat het gaat om de informatiecoördinatie op nationaal niveau. Onderdeel van de Dienst IPOL vormt de Unit Nationaal Inzicht die zich bezighoudt met informatieverzameling en analyse van zware criminaliteit die zich bovenregionaal afspeelt. Onderdeel van deze unit is de Nationale Criminele Inlichtingeneenheid (NCIE) waaraan Regionale CIE-en informatie verstrekken die van nationale of van internationale betekenis zijn.



Figuur 6.3: Interne organisatie Regionale CIE.

In figuur 6.3 is de interne organisatie van een regionale CIE uitgewerkt. Hoewel er regionaal relatief kleine verschillen zijn in de organisatiestructuur hebben wij voor het onderzoek gebruik gemaakt van de meest voorkomende hiërarchische structuur. De leiding van een regionale CIE is in handen van het hoofd CIE. In enkele regiokorpsen is het leidinggeven aan de CIE een deeltaak van het hoofd van de Regionale Informatie Organisatie of de Divisie Recherche maar vaak wordt deze verantwoordelijkheid gedelegeerd aan een hoofd CIE of een plaatsvervangend hoofd CIE die op zijn beurt verant-

woordelijk is voor de dagelijkse taakuitvoering van de CIE. Met betrekking tot de opslag, verwerking en uitwisseling van informatie is het hoofd CIE eindverantwoordelijke. De teamchef bepaalt uiteindelijk of informatie al dan niet kan worden uitgewisseld. Hieronder geven beschrijven wij per functie de verschillende taken.

1. Analisten
De analisten met een CIE-status houden zich bezig het veredelen van informatie. Dat houdt in dat de informatie die een informant heeft gegeven op bepaalde punten wordt gecontroleerd op de juistheid. Het gaat om de juistheid van namen, adresgegevens, lokaties etc. Verder houden CIE-analisten zich bezig met het opstellen van zogenaamde strategische analyses. Daarin worden criminaliteitsbeelden opgesteld die in het driehoeksoverleg tussen de burgemeester, de hoofdofficier van justitie, en de korpschef kunnen worden gebruikt bij het stellen van beleidsprioriteiten in de regio. Verder worden deze criminaliteitsbeelden binnen de CIE gebruikt om vast te stellen aan welke informatie behoefte is zodat gerichter informatie kan worden ingewonnen.

2. Groepschef
De groepschef stuurt de runnerskoppels aan. Hij stelt in samenspraak met de runners welke informatie in aanmerking komt voor opname in het register zware criminaliteit en welke afhandelingscode de informatie moet krijgen. Daarnaast speelt hij een rol bij het maken van inschattingen omtrent de betrouwbaarheid van de informatie.

2a. Runners
De runners onderhouden binnen de CIE contacten met de informanten. Zij stellen naar aanleiding van gesprekken verslagen op, de zogenaamde bruto gespreksverslagen, die zoveel mogelijk een feitelijke weergave zijn van hetgeen gezegd is tijdens het gesprek. Zij registreren deze informatie in het informantenregister. Vervolgens bepalen zij in samenspraak met de groepschef welke informatie van het bruto gespreksverslag kan worden opgenomen in het register zware criminaliteit. Dit vormt het zogenaamde nettoverslag. De runners hebben verder een belangrijke stem in de beoordeling van de informatie op betrouwbaarheid en het vaststellen van de afhandelingscodes. Daarnaast overleggen zij met het hoofd CIE of informatie al dan niet kan worden uitgewisseld.

2b. Administratiemedewerker
De administratiemedewerker registreert de netto verslagen in het register zware criminaliteit. Hij of zij voert daarbij soms ook een (marginale) rechtmatigheidcontrole uit waarbij hij nagaat of de te registreren informatie voldoet aan de opnamecriteria. Deze medewerkers vormen binnen de organisatie de feitelijke gebruikers van het systeem. Zij voeren ook zoekopdrachten uit in de systemen voor het hoofd CIE wanneer deze een informatieverzoek via een van de ketenpartners binnen krijgt.

3. Infodeskmedewerker
De infodeskmedewerker is het aanspreekpunt van alle politieambtenaren in de regio. Alle informatieverzoeken komen bij de infodesk binnen en wanneer blijkt dat er informatie gevraagd wordt over een CIE-subject kan deze medewerker dergelijke verzoeken, al dan niet in overleg met het hoofd CIE, afhandelen. Vaak zijn daarover binnen de regio afspraken gemaakt zodat de medewerker op basis van de afhandelingscodes weet welke informatie hij wel en niet mag verstrekken.

6.2.3 Organisatiemodel 3: Bedrijfsproces informatie-uitwisseling

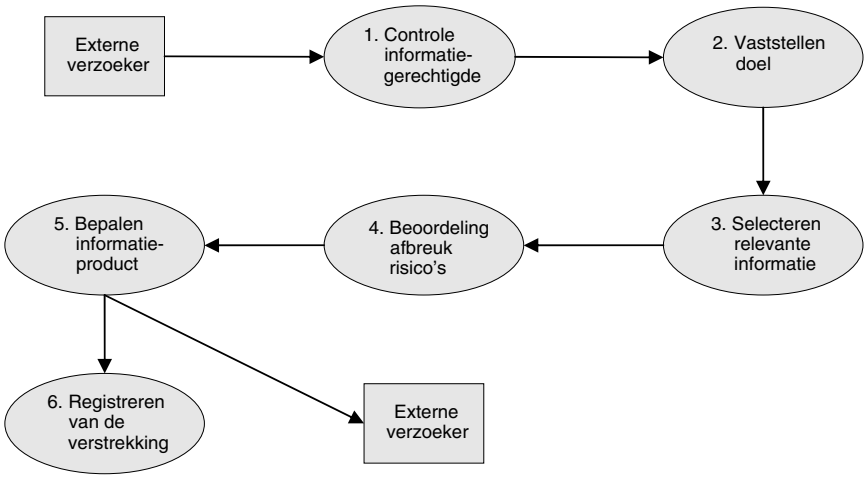
In Organisatiemodel 3 worden zes deeltaken met betrekking tot het bedrijfsproces rond de informatie-uitwisseling nader uitgewerkt. In het model wordt aangegeven welke functie binnen de regionale CIE verantwoordelijk is voor de uitvoering van de deeltaak. De uitvoerder van de deeltaak wordt bepaald volgens de functies die in figuur 6.3 zijn onderscheiden. In het model wordt voorts de lokatie waar de taak wordt uitgevoerd gespecificeerd. Hierbij moet worden bedacht dat de politieorganisatie is opgebouwd uit 25 regionale politiekorpsen. Dat houdt in dat er ook 25 geografisch gespreide CIE-en zijn waartussen informatie-uitwisseling plaatsvindt. Verder is per deeltaak de benodigde kennis gespecificeerd waarbij onderscheid is gemaakt tussen juridische kennis, kennis gebaseerd op ervaring en variabele kennis. De juridische kennis volgt primair uit de wet- en regelgeving en secundaire rechtsbronnen zoals relevante jurisprudentie en de literatuur (handboeken). De variabele kennis van het verzoek moet worden ontleend aan de informatieverzoeker. Daarnaast is uit ons veldwerk gebleken dat veel kennis die wordt gebruikt bij de uitwisseling van gegevens voortvloeit uit

Organisatiemodel 3	**Uitvoerder**	**Benodigde kennis**	**Kennis-intensiteit**
Controle informatie-gerechtigde (1)	Hoofd CIE	Verstrekkingsbepalingen	Hoog
Vaststellen doel (2)	Hoofd CIE	Doel informatieverzoek	Middel
Selecteren relevante informatie (3)	Analist	Doel informatieverzoek Betrouwbaarheidscodes	Laag
Beoordeling afbreuksrisico's (4)	Hoofd CIE en runner	Afhandelingscodes Impliciete kennis Verstrekkingsbepalingen	Hoog
Bepalen informatieproduct (5)	Hoofd CIE	Doel informatieverzoek	Laag
Registreren van de verstrekking (6)	Administatie-medewerker	Doel informatieverzoek Protocolbepalingen	Laag

Tabel 6.5: Deeltaken.

de ervaring van de betrokken CIE-ambtenaren. Wij duiden dat als impliciete kennis. In het model is daarnaast aangegeven of de taakuitvoering kennisintensief is. Daarbij gaat het om de mate waarin juridische kennis nodig in voor de uitvoering van de deeltaak. Wij onderscheiden (1) een hoge kennisintensiteit waarin relatief veel juridische kennis vereist is, (2) een gemiddelde kennisintensiteit waarbij het gaat om juridische kennis op basisniveau en (3) een lage kennisintensiteit waarbij niet of nauwelijks juridische kennis is vereist voor de uitvoering van de deeltaak.

In figuur 6.4 worden de deeltaken schematisch weergegeven. Vanzelfsprekend kent ons onderscheid in de verschillende deeltaken een hoog abstractieniveau en is de praktijk van gegevensuitwisseling aanzienlijk complexer. Waar het echter in onze vereenvoudigde weergave om gaat is dat inzichtelijk wordt waar in het proces van gegevensuitwisseling een beoordeling plaatsvindt, althans behoort plaats te vinden, van de rechtmatigheid van de uitwisseling. De ontleding van het proces in deeltaken wordt schematisch weergegeven in figuur 6.4.



Figuur 6.4: Deeltaken informatieverstrekking CIE.

In de schematische weergave wordt ervan uitgegaan dat het proces aanvangt met een concreet informatieverzoek. Hoewel in de CIE-regeling is vastgelegd dat een onderdeel van de CIE-taak bestaat uit het ongevraagd uitwisselen van informatie, is uit ons veldwerk gebleken dat het merendeel dat informatie pas wordt uitgewisseld naar aanleiding van een concreet informatieverzoek. Het proces naar aanleiding van zo'n informatieverzoek ontleden wij in zes deeltaken die zijn weergegeven in het stroomschema van figuur 6.4. Hierna geven wij een korte beschrijving van de zes onderscheiden deeltaken.

1. Controle informatiegerechtigde
In de huidige CIE-praktijk komt een informatieverzoek telefonisch of via een e-mail binnen bij het hoofd CIE of diens plaatsvervanger. Deze eerste stap in het proces van informatie-uitwisseling bestaat dan uit een controle ten aanzien van de vraag of de verzoeker van informatie ook daadwerkelijk de informatiegerechtigde is. In de praktijk wordt CIE-informatie vrijwel altijd uitgewisseld via de regionale CIE-en en is er ten aanzien van de informatie-uitwisseling sprake van een sterk ontwikkelde ons-kent-ons-cultuur. De door ons onderscheiden deeltaak die ziet op de controle van de informatiegerechtigde is daarom in de praktijk niet of nauwelijks geformaliseerd.

2. Vaststellen doel
De volgende deeltaak is het vaststellen van de achtergrond van het informatieverzoek waarbij in het bijzonder het doel van het informatieverzoek moet worden nagegaan. Deze vaststelling van het doel is vanuit het privacyrechtelijk perspectief van belang omdat in de Wpolg de verschillende wettelijke doelen waarvoor informatie mag worden verwerkt, zijn vastgelegd. Verwerking en verstrekking van informatie in strijd met deze doelen is in beginsel onrechtmatig. Daarnaast is de vaststelling van het informatiedoel ook vanuit pragmatisch oogpunt van belang omdat het gebruikt kan worden voor een nadere precisering van de gezochte informatie.

3. Selecteren relevante informatie
Aan de hand van het geaccepteerde informatieverzoek wordt het register zware criminaliteit geraadpleegd en wordt de relevante informatie geselecteerd. Zoals hiervoor aangegeven speelt het doel van het informatieverzoek daarbij een belangrijke rol. De zorgvuldige selectie van relevante informatie is immers ook vanuit het perspectief van rechtsbescherming van belang. De eis van proportionaliteit brengt mee dat niet meer informatie wordt verstrekt dan nodig is met het oog op het doel waarvoor de informatie wordt gevraagd.

4. Beoordeling afbreukrisico's
De afbreukrisico's worden op basis van de gevonden informatie beoordeeld. In de praktijk wordt deze beoordeling uitgevoerd door het hoofd CIE. De beoordeling vindt in beginsel plaats op basis van de afhandelingscodes. Afhankelijk van het doel waarvoor de informatie wordt gevraagd en de inschatting van de afbreukrisico's wordt nagegaan of de informatie al dan niet kan worden verstrekt. Soms worden er door het hoofd CIE voorwaarden verbonden aan de uitwisseling of is eerst overleg nodig met de CIE-Officier van Justitie.

5. Bepalen informatieproduct
Aan de hand van het doel waarvoor de informatie wordt gevraagd maakt het hoofd CIE vervolgens een keuze uit de verschillende wijzen waarop de informatie kan worden verstrekt. Dat kan via het zogenaamde zwacri-informatierapport, een proces-verbaal of door middel van een analyserapport.

6. Registreren van de verstrekking.
Nadat de informatie is verstrekt wordt in het register zware criminaliteit aangetekend welke informatie is verstrekt en aan wie de informatie is verstrekt. Deze aantekening is van belang omdat daardoor achteraf kan worden gecontroleerd waarvoor de betreffende informatie is gebruikt. Bovendien kunnen deze metagegevens worden gebruikt om in geval van relevante mutaties, degene aan wie de informatie is verstrekt op de hoogte te brengen van de mutatie.

In sectie 6.3 werken wij de deeltaken 1, 2, en 4 nader uit. Een korte beschouwing leert ons dat juist deze taken (relatief) kennisintensief zijn en daarom op voorhand het meest geschikt lijken te zijn voor de toepassing van normatieve multi-agenttechnieken. Voor de uitvoering van deeltaken 3, 5, en 6 zijn vooral technische (zoek)functionaliteiten van belang die slechts indirect een normatieve component kennen. In het kader van de toepassing van normatieve multi-agenttechnieken laten wij deze deeltaken hier verder buiten beschouwing.

6.2.4 Organisatiemodel 4: Benodigde kennis

In Organisatiemodel 4 wordt de focus gelegd op gedeelten van de kennis die wij hebben onderscheiden in tabel 6.3 en die actief in gebruik zijn bij de verschillende uitvoerders van de deeltaken. De analyse van de benodigde kennis ziet op twee vragen (1) bij wie de kennis aanwezig is en (2) bij welke taakuitvoering deze kennis gebruikt wordt. Vervolgens vermelden wij of de kennis in de juiste vorm aanwezig is. Met de juiste vorm bedoelen wij in dit verband dat de (juridische) kennis effectief toegankelijk is voor de betrokkene in de organisatie. Hieronder beschrijven wij Organisatiemodel 4.

Organisatiemodel 4			
Kennis over:	**In bezit bij:**	**Gebruikt bij taak:**	**Juiste vorm?**
Verstrekkings-bepalingen	RCIE	Controle informatiegerechtigde & beoordeling verstrekkingrisico's	Nee
Protocolplicht bepalingen	RCIE	Controle informatiegerechtigde, & beoordeling versterkingsrisico's	Nee
Afhandelingscodes	RCIE	Beoordeling versterkingsrisico's	Ja
Betrouwbaarheids-codes	RCIE	Selecteren relevante informatie	Ja
Achtergrond informatieverzoek	Informatie-verzoeker	Vaststellen informatieprobleem, beoordelen verstrekkinsgrisico's, bepalen informatieproduct, registreren verstrekking	Nee
Risico-inschatting informanten	CIE-chef en runner	Beoordelen verstrekkingsrisico's	Nee

Tabel 6.6: Benodigde kennis.

In hoofdstuk 4 hebben wij enkele onderzoeken besproken waaruit naar voren is gekomen dat de Wpolr en de Bpolr voor politieambtenaren moeilijk toegankelijke wetgeving is. Wij constateren dat de aard van de privacynormen onder de Wpolg niet wezenlijk is veranderd of verduidelijkt. Ook in de Wpolg wordt veelvuldig gebruik gemaakt van open normen en vage begrippen die door de normadressanten nader dienen te worden geïnterpreteerd. Dit geldt ook voor de noodzakelijkheidscriteria die een nadere concretisering en interpretatie vereisen van de beginselen van proportionaliteit en subsidiariteit. Wij verwachten daarom dan ook dat ten aanzien van de onduidelijkheid van de regels uit de eerste verplichte evaluatie van de Wpolg in 2013 vergelijkbare knelpunten naar voren zullen komen als bij de Wpolr.

In dit verband is van belang dat tijdens de gesprekken die wij hebben gehouden met CIE-ers is gebleken dat het enkel aanwezig zijn van de wetteksten op de regionale afdelingen van de CIE niet de juiste vorm is voor de toepassing van die juridische kennis. Wij hebben dit geduid als het eerste hoofdknelpunt (moeilijk toegankelijke juridische kennis) en menen dat de implementatie van de juridische kennis in softwareagenten kan bijdragen aan het op een adequate wijze toegankelijk maken van deze kennis en geautomatiseerd toepassen van deze kennis. Voor de toegankelijkheid van kennis van het doel van het informatieverzoek, de zogenaamde achtergrondkennis, geldt hetzelfde, zij het in mindere mate. In de praktijk wordt deze kennis mondeling verstrekt aan het hoofd CIE en deze tracht zich door middel van het stellen van vragen een zo compleet mogelijk beeld te vormen van de informatiebehoefte van de verzoeker en het doel van het informatieverzoek. Vervolgens is niet voorzien in een protocol waarin de wijze waarop met de achtergrondkennis door het hoofd CIE moet worden vastgelegd en doorgegeven aan een analist die de informatie uit de systemen moet halen. In de praktijk gebeurt dat voor het merendeel mondeling. Dat maakt de afhandeling daarvan ondoorzichtig en verhoogt bovendien de kans op fouten in de zoekresultaten.

Verder constateren wij daarin geen bijzonderheden. Wel constateren wij bijzonderheden bij de beoordeling van de kwaliteit van de kennis. Met name is uit verschillende evaluatieonderzoeken naar voren gekomen dat de van toepassingzijnde wet- en regelgeving door politieambtenaren als moeilijk toepasbaar wordt ervaren (Schreuder e.a., 2005). In die zin beoordelen wij de kwaliteit van de juridische kennis als onvoldoende, waarbij het dan dus met name gaat over de moeilijke toegankelijkheid daarvan (hoofdknelpunt 1). Gelet op het doel van de wet- en regelgeving en gelet op de normadressanten (politieambtenaren) schiet de kwaliteit tekort. Deze onduidelijkheid levert voorts ook problemen op bij de ontwikkeling en implementatie van de juridische normen in informatie- en kennissystemen voor de politie. Voor toepassing van deze kennis in computersystemen zal immers een vertaalslag nodig zijn waarin een zeer concrete interpretatie van de open en soms vage normen wordt gegeven (Mommers, Voermans, Koelewijn en Kielman, 2009).

Met betrekking tot de benodigde kennis komt uit de analyse naar voren dat een deel daarvan variabel is. Dit heeft tot gevolg dat een kennissysteem dat adviseert of zelfs beslissingen neemt over informatietransacties ook moet kunnen redeneren over variabele kennis. Met name kennis met betrekking tot de betekenis en interpretatie van de verschillende verwerkingsdoelen is daarbij relevant. Bovendien moet naast het informatiedoel ook het informatieprobleem voldoende duidelijk worden gespecificeerd. Indien een informatieverzoeker onvoldoende concreet aangeeft welke informatie precies wordt gezocht kan de zoekopdracht niet adequaat kan worden uitgevoerd.

6.3 Taakmodellen

Een taak wordt in het normale spraakgebruik omschreven als een menselijke activiteit die gericht is op het bereiken van een bepaald doel. In de context van dit onderzoek is deze definitie een goed aanknopingspunt. Wij beperken de taakuitvoering evenwel niet tot een menselijke activiteit. In onze benadering kunnen taken ook worden uitgevoerd door softwareagenten. Verder beschouwen wij de uitvoering van een taak als een gespecificeerd onderdeel van een bedrijfsproces waardoor het vooral een technisch concept wordt. Het concept 'taak' kan die benadering het beste worden omschreven als een onderdeel van een bedrijfsproces dat:

(1) omschreven kan worden als een doelgerichte activiteit met een duidelijke toegevoegde waarde voor de organisatie;
(2) bepaalde input verwerkt en gewenste output levert op een gestructureerde en gecontroleerde wijze;
(3) bij de uitvoering gebruik maakt van bepaalde bronnen;
(4) voor de uitvoering kennis en vaardigheden nodig heeft en vervolgens ook zelf verstrekt;
(5) wordt uitgevoerd volgens vastgestelde criteria;
(6) wordt uitgevoerd door verantwoordelijke en betrouwbare agenten.

Deze definiëring van het taakconcept wordt in de CommonKads-methode als uitgangspunt gebruikt voor het Taakmodel. In het Taakmodel wordt de kennis uit het Organisatiemodel 3, waarin de deeltaken binnen het bedrijfsproces zijn gespecificeerd, nader uitgewerkt. Enkele elementen in het model die specifiek op organisatorische aspecten zien hebben wij buiten beschouwing gelaten omdat wij de methode uitsluitend als analyse-instrument gebruiken. Wij behandelen achtereenvolgens in subsectie 6.3.1 Taakmodel 1 (controle informatiegerechtigde), in subsectie 6.2.3 Taakmodel 2 (vaststellen doel), en in subsectie 6.3.3 Taakmodel 3 (beoordeling afbreukrisico's).

6.3.1 Taakmodel 1: Controle informatiegerechtigde

In Taakmodel 1 wordt de focus gelegd op de eerste deeltaak die ziet op de vraag of de informatieverzoeker ook gerechtigd is in de zin van de Wpolg. Dit betreft dus een controle op de persoon en functie van degene die het informatieverzoek indient. Er worden in dit taakmodel, evenals in Taakmodel 2 en 3, negen externe elementen met betrekking tot de taakuitvoering beschreven. Het gaat daarbij om de organisatorische context waarbinnen de taak wordt uitgevoerd en het doel van de taakuitvoering. Verder wordt de afhankelijkheid van andere deeltaken beschreven. Deze afhankelijkheid volgt uit de opsplitsing van het proces van gegevensuitwisseling in deeltaken die onderling na elkaar moeten worden uitgevoerd. Het resultaat van een eerdere deeltaakuitvoering moet zodoende worden meegenomen als een interpretabel informatiebericht (of interpretabele metadata) die gebruikt kan worden bij de uitvoering van de volgende deeltaak. Voorts wordt in het model inhoudelijke aangegeven welke kennis er nodig is voor de deeltaakuitvoering en wat de input- en output-objecten zijn. Volledigheidshalve tekenen wij hierbij aan dat uit ons veldwerk naar voren is gekomen dat in de huidige CIE-praktijk van gegevensuitwisseling geen van deze deeltaken is geautomatiseerd.

Taakmodel 1	**Taakanalyse**
Deeltaak:	Controle informatiegerechtigde.
Organisatie:	Regionale CIE.
Doel:	Het doel van de uitvoering van deze taak is het waarborgen van de rechtmatigheid van de gegevensuitwisseling.
Afhankelijkheid en informatiestroom:	Input: Identificerende gegevens van verzoeker. Output: Toestemming of weigering het informatieverzoek verder in behandeling te nemen.
Objecten:	Input: Identificatiegegevens (eventueel geverifieerd bij Trusted Third Party), doelomschrijving. Output: verificatieresultaat m.b.t. de ontvangstgerechtigde.
Timing en controle:	De taak dient bij ieder informatieverzoek te worden uitgevoerd en de frequentie is daarmee afhankelijk van het aantal informatieverzoeken. De aanvang van de overige taken hangt af van de uitkomst van deze taakuitvoering.
Agenten:	In de praktijk: Hoofd CIE of plaatsvervangend hoofd CIE.
Kennis en bekwaamheid:	Juridische kennis ten aanzien van de ontvangstgerechtigden: de verificatie vindt plaats aan de hand van de in de wet opgesomde informatiegerechtigden en een marginale toetsing aan de hand van het doel waarvoor de informatie wordt gevraagd.
Bronnen:	Wpolg en Bpolg, CIE-regeling.

Tabel 6.7: Controle informatiegerechtigde.

In tabel 6.7 wordt de eerste deeltaak van het proces van informatie-uitwisseling uitgewerkt. Deze deeltaak bestaat uit een controle van de vraag of de informatieverzoeker ook daadwerkelijk informatiegerechtigde is in de zin van de wet. In hoofdstuk 3 hebben wij het juridisch kader uiteengezet waarbij wij het gesloten verstrekkingenregime van de Wpolg hebben beschreven. De controle van de informatiegerechtigde is concreet samen te vatten in twee toetsen:

(1) Is de informatievrager ook informatiegerechtigde in de zin van de wet?
(2) Heeft de informatiegerechtigde in de zin van de wet de informatie nodig voor de goede uitvoering van zijn (politie)taak?

Bij de eerste toets wordt aan de hand van de wettelijke gedefinieerde informatiegerechtigden nagegaan of de informatieverzoeker als zodanig geclassificeerd kan worden. Indien de informatieverzoeker is gekwalificeerd dan is op basis van de wettelijke regel tevens bekend welke eventuele beperkingen er met betrekking tot de informatieverstrekking gelden. Ten aanzien van de tweede toets volgt uit het systeem van de wet dat het een marginale toets betreft aangezien anders de situatie zou kunnen ontstaan waarin politieambtenaren *de facto* een soort controlebevoegdheden jegens elkaar zouden kunnen uitoefenen. Dat zou in strijd komen met het beginsel dat de wetgever ten grondslag heeft gelegd aan de Wpolg, namelijk de *free flow* van informatie. Een te strikte opvatting van de onderlinge controlebevoegdheden ten aanzien van de noodzaak van het informatieverzoek voor de uitvoering van de politietaak zou deze *free flow* onwenselijk kunnen belemmeren. Bovendien is het in de praktijk moeilijk voor een hoofd CIE om na te gaan in hoeverre de informatieverzoeker nu zijn informatie nodig heeft voor de uitvoering van zijn taak. Bij deze marginale toetsing zal ons inziens noodzakelijkerwijs moeten worden volstaan met het zo concreet mogelijk communiceren van het doel van het informatieverzoek. Aan de hand van de doelomschrijving kan dan toetsing plaatsvinden of de gevraagde informatie nodig is (1) voor het doel en (2) de daarmee samenhangende uitvoering van de betreffende taak. Wij menen dat slechts in gevallen waarin het informatieverzoek onmiskenbaar in strijd is met de in de Wpolg vastgelegde doelen, er een grondslag is om een informatieverzoek te weigeren.

6.3.2 Taakmodel 2: Vaststellen doel

In Taakmodel 2 wordt de tweede deeltaak in het proces van informatie-uitwisseling beschreven betreffende het vaststellen van het doel van het informatieverzoek. De vaststelling van het doel is om ten minste twee redenen een cruciaal onderdeel van het proces van informatie-uitwisseling.

Ten eerste vormt deze deeltaak het aanknopingspunt om te controleren of het informatieverzoek en daarmee de verstrekking van informatie blijft bin-

nen de wettelijke vastgelegde doeleinden voor de verwerking van politiegegevens. Deze deeltaak vormt daarmee een essentieel onderdeel van de rechtmatigheidscontrole van de informatie-uitwisseling en is daarmee een belangrijk aanknopingspunt voor de normatieve beperkingen in het informatiesysteem.

Ten tweede is de vaststelling van de doelstelling van het informatieverzoek ook in het belang van de goede uitvoering van de politietaak omdat het kan bijdragen aan het voorkomen van een zogenaamde *information overload*. Hoe nauwkeuriger immers het doel van de informatiebehoefte in kaart kan worden gebracht des te gerichter kan de zoekopdracht worden uitgevoerd. Zodoende kan worden voorkomen dat de vragende politieambtenaar teveel niet-relevante informatie ontvangt. De deeltaak moet daarom tevens worden beschouwd als een uitwerking van het *need-to-know*-principe dat binnen de politieorganisatie algemeen geldt als een principe dat in het belang is van de goede taakuitvoering. Hieronder beschrijven wij kort de negen relevante elementen ten aanzien van deze taakuitvoering.

Taakmodel 2	**Taakanalyse**
Deeltaak:	Vaststellen doel.
Organisatie:	Regionale CIE.
Doel:	Het doel van de uitvoering van deze taak het vaststellen van de informatiebehoefte van de verzoeker mede op basis van het doel waarvoor de informatie gevraagd wordt. Voorkomen van information overload.
Afhankelijkheid en informatiestroom:	Input: Doel en achtergrond van informatieverzoek. Output: Een of meer specifieke zoekvragen.
Objecten:	Input: Informatie achtergrond en doel. Output: Een of meer specifieke zoekvragen.
Timing en controle:	De taak dient pas uitgevoerd te worden nadat is vastgesteld dat de informatieverzoeker ook een mogelijke ontvangstgerechtigde is.
Agenten:	In de praktijk: Hoofd CIE of plaatsvervangend hoofd CIE.
Kennis en bekwaamheid:	Het stellen van vragen aan de informatieverzoeker. Met behulp van de antwoorden moet dan een specifieke zoekvraag geformuleerd worden.
Bronnen:	Wpolg en uitwisselingsprotocollen zoals ontwikkeld door Abrio en het protocol elektronisch uitwisselen zwacri-gegevens.

Tabel 6.8: Vaststellen doel.

Wij zien bij de uitvoering van deze deeltaak zoals gezegd goede mogelijkheden om aan de hand van het doel van het informatieverzoek ook de informatiebehoefte nauwkeuriger in kaart te brengen. Dat kan bijvoorbeeld door het stellen van een aantal gerichte vragen door een 'zoekagent' aan de informatieverzoeker. Met behulp van de input (antwoorden) kan vervolgens een gerichte

zoekvraag worden geformuleerd. Wanneer de zoekagent tevens uitgerust zou kunnen worden met een bepaalde mate van zelflerend vermogen zou deze op basis van reeds uitgevoerde informatieproblemen 'intelligentere' zoekvragen moeten kunnen formuleren. Voor de kennis die nodig is voor het stellen van vragen aan de informatieverzoeker kan aansluiting worden gezocht bij het Abrio-protocol dat ziet op de uitwisseling van gegevens (zie ook: Meesters, Kortekaas en Tragter, 2000). Daarin wordt onder meer onderscheid gemaakt tussen gegevens die verstrekt worden ten behoeve van operationele doeleinden en gegevens die worden verstrekt voor analysedoeleinden.

6.3.3 Taakmodel 3: Beoordeling afbreukrisico's

In Taakmodel 3 beschrijven wij de uitvoering van deeltaak 4 in het proces van informatie-uitwisseling. De uitvoering van deze deeltaak geschiedt op basis van de informatie die de zoekagent heeft gevonden nadat deze aan de hand van het informatiedoel een zoekopdracht heeft uitgezet in het register zware criminaliteit. De beoordeling van de afbreukrisico's kan pas plaatsvinden op het moment dat bekend is welke informatie potentieel zal worden uitgewisseld. Opnieuw speelt bij de beoordeling van de afbreukrisico's het concrete doel van het informatieverzoek een belangrijke rol. De aard van het doel bepaalt in belangrijke mate de omvang van de risico's. Zo geldt in zijn algemeenheid dat de risico's bij gebruik van informatie in een lopend rechercheonderzoek groter zijn dan bij een analyse ten behoeve van het handhavingsbeleid. Zoals wij uiteen hebben gezet in hoofdstuk 4 gaat het bij afbreukrisico's in de eerste plaats om de afscherming van de informatiebron. Daarnaast wordt met afbreukrisico's gedoeld op het risico dat lopende CIE-onderzoeken naar bepaalde subjecten of een criminele organisatie die door het vrijgeven van stuk informatie kan worden gefrustreerd. Hieronder volgt een beschrijving van Taakmodel 3.

In de huidige CIE-praktijk worden de afbreukrisico's beoordeeld door het hoofd CIE of diens plaatsvervanger in samenspraak met de betreffende runners. Wij zien evenwel goede mogelijkheden om deze deeltaak gedeeltelijk te automatiseren en de risico's te laten beoordelen door de een softwareagent. Het belangrijkste aanknopingspunt voor de beoordeling wordt gevormd door de geregistreerde afhandelingscodes. Wel menen wij dat bij deze cruciale deeltaak de poortwachteragent rechtstreeks moet kunnen communiceren met het verantwoordelijke hoofd van de CIE. Daarbij kan het bijvoorbeeld gaan over de actualiteit van de geregistreerde afhandelingscode. Denkbaar is dat een poortwachteragent alvorens de informatieverstrekking wordt geweigerd vanwege afhandelingscode 00, eerst bij het hoofd CIE nagaat of de afhandelingscode nog altijd actueel is en of deze niet zou moeten worden aangepast. Daarnaast kan in een dergelijk communicatieprotocol ook worden geprogrammeerd of de informatie niet toch onder bepaalde beperkende voorwaarden kan worden verstrekt. Een beperkende voorwaarde zou bijvoorbeeld kunnen zijn dat de informatie niet mag worden gebruikt

voor operationele doeleinden of pas na het verstrijken van een bepaalde termijn daarvoor mag worden gebruikt.

Taakmodel 3	**Taakanalyse**
Deeltaak 4:	Beoordeling afbreukrisico's.
Organisatie:	Regionale CIE.
Doel:	Het doel van deze deeltaak is om op basis van de gevonden resultaten met bijbehorende afhandelingscodes te bepalen of de verstrekkingsrisico's zodanig zijn dat verstrekking geweigerd moet worden of aan beperkende voorwaarden moet worden onderworpen.
Afhankelijkheid en informatiestroom:	Input: Zoekresultaat met afhandelingscodes. Output: Weigering, toestemming of starten van onderhandeling over de voorwaarden.
Objecten:	Input: Bericht met afhandelingscode. Output: Bericht met weigering of toestemming of voorwaarden.
Timing en controle:	De taak dient pas uitgevoerd nadat het zoekresultaat bekend is.
Agenten:	Hoofd CIE of plaatsvervangend hoofd CIE in overleg met betreffende runner.
Kennis en bekwaamheid:	Beoordeling geschiedt op basis van de afhandelingscodes en ervaring van de CIE-ers.
Bronnen:	Aanwijzingen opsporing, afhandelingscodes CIE-regeling en Abrio-protocol. Ervaring CIE-ambtenaren.

Tabel 6.9: Beoordeling afbreukrisico's.

6.4 Beantwoording derde onderzoeksvraag

In de hoofdstukken 5 en 6 stond de derde onderzoeksvraag (OV 3) centraal te weten: Op welke wijze is de huidige uitwisseling van criminele inlichtingen ingericht en wat zijn daarin de (juridische) knelpunten? Ter beantwoording van deze vraag hebben wij allereerst in hoofdstuk 5 een vijftal (evaluatie)onderzoeken besproken die vanaf het midden van de jaren negentig zijn gedaan naar de uitwisseling van politiegegevens. Vervolgens hebben wij de bevindingen van ons eigen veldwerk besproken. Voor de tussenconclusies met betrekking tot de hoofdknelpunten in het proces van informatie-uitwisseling ten aanzien van criminele inlichtingen verwijzen wij naar sectie 5.3 waarin de derde onderzoeksvraag aangaande de inventarisatie van de knelpunten wordt beantwoord.

In het onderhavige hoofdstuk hebben wij met behulp van de CommonKads-methode de wijze geanalyseerd waarop de huidige informatie-uitwisseling binnen de CIE plaatsvindt. In de analyse hebben wij laten zien dat het huidige bedrijfsproces met betrekking tot de informatie-uitwisseling binnen de

CIE kan worden onderverdeeld in zes deeltaken. Geen van deze deeltaken is in het huidige systeem van informatie-uitwisseling geautomatiseerd. Zo bezien is er in beginsel voldoende ruimte voor automatiseringstoepassingen. Aangezien evenwel het doel van ons onderzoek is gelegen in de vraag waar in dit proces van informatie-uitwisseling normatieve beperkingen zouden kunnen worden ingebouwd hebben wij voorts de analyse toegespitst op het nader ontleden van de zes deeltaken en de kennis die nodig is voor de uitvoering van deze deeltaken.

Deze analyse heeft tot het inzicht geleid dat tenminste drie deeltaken (controle ontvangstgerechtigde, vaststellen informatiedoel, beoordelen afbreukrisico's) verhoudingsgewijs kennisintensief zijn omdat voor de uitvoering van deze deeltaken moeilijk toegankelijke juridische kennis is vereist. De drie deeltaken hebben wij vervolgens aan de hand van drie taakmodellen geanalyseerd waarbij wij tot de conclusie komen dat de deeltaken aanknopingspunten bieden voor (gedeeltelijke) normatieve automatisering. De normatieve automatisering is vanuit twee perspectieven van belang.

Rechtshandhaving
Vanuit het perspectief van de rechtshandhaving bieden normatieve softwareagenten ons inziens goede mogelijkheden om de informatie-uitwisseling te verbeteren. Met behulp van de toepassing van dergelijke softwareagenten kunnen verschillende standaardisatieproblemen in gedistribueerde informatiesystemen worden ondervangen waardoor onvoldoende standaardisatie niet langer een knelpunt behoeft te zijn. Bovendien kan door de inzet van softwareagenten het arbeidsintensieve handmatige proces van informatie-uitwisseling (gedeeltelijk) worden geautomatiseerd waardoor een betere *free flow* van informatie tot stand kan komen. Een ander voordeel voor de uitvoering van de politietaak is dat normatieve beperkingen in de geautomatiseerde informatie-uitwisseling er toe kan leiden dat meer gewerkt wordt volgens het *need-to-know*-principe waardoor een *information overload* kan worden voorkomen.

Rechtsbescherming
Vanuit het perspectief van de rechtsbescherming zien wij verschillende mogelijkheden om in het proces van informatie-uitwisseling beter de privacy te waarborgen door middel van normatieve beperkingen. Wij denken daarbij aan (1) het zorgvuldiger toepassen van de wettelijke bepalingen, (2) het verbeteren van (geautomatiseerd) toezicht op de registraties, en (3) het vergroten van de transparantie van de gegevensregistratie en -uitwisseling. In de taakmodellen hebben wij (a) aangegeven waar in het proces van informatie-uitwisseling zich deze mogelijkheden voordoen en (b) waar mogelijkheden zitten om softwareagenten in te zetten die juridische regels kunnen toepassen of daarover kunnen adviseren om zodoende de *compliance* van de uitwisseling te verbeteren. Daarnaast menen wij dat de inzet van software-

agenten kan bijdragen aan (1) het verbeteren van de kwaliteit van de registraties en (2) de transparantie van de uitwisseling.

In hoofdstuk 7 introduceren wij zes verschillende typen softwareagenten (indexeringsagent, autorisatieagent, zoekagent, transactieagent, poortwachteragent en de surveillanceagent) die uitvoering van de zes deeltaken automatiseren of ondersteunen. Vervolgens werken wij op conceptueel niveau de toepassing van deze softwareagenten uit.

7 Conceptuele analyse

In dit hoofdstuk beantwoorden we de vierde onderzoeksvraag (OV 4) waarin wordt nagegaan op welke wijze de in hoofdstuk 2 beschreven multi-agenttechnieken kunnen worden ingezet om de (geautomatiseerde) uitwisseling van informatie in het CIE-domein te verbeteren. Met verbeteren doelen wij op de mate waarin de multi-agenttechniek kan bijdragen aan (1) het oplossen van de in hoofdstuk 5 geconstateerde knelpunten en (2) een rol kan spelen als reguleringsinstrument.

Dit hoofdstuk is als volgt opgebouwd. In sectie 7.1 zetten wij allereerst de theoretische basis voor de normatieve geautomatiseerde informatie-uitwisseling uiteen. Vervolgens beschrijven wij in sectie 7.2 op basis van de organisatieanalyse op conceptueel niveau zes modellen van softwareagenten die naar onze mening in de toekomst een centrale rol kunnen vervullen in het geautomatiseerde proces van politiële informatie-uitwisseling. Om de toepassing van softwareagenten in het CIE-domein nader te illustreren werken wij in sectie 7.3 op conceptueel niveau vier mogelijke toepassingen uit ten aanzien van de normatieve geautomatiseerde uitwisseling in het CIE-domein. In sectie 7.4 verantwoorden wij de functionele uitwerkingen vanuit (1) het perspectief van de rechtshandhaving en (2) vanuit het perspectief van de rechtsbescherming. In sectie 7.5 beantwoorden wij de vierde onderzoeksvraag.

7.1 Theoretische basis

Binnen het rechtswetenschappelijk onderzoekdomein dat zich bezighoudt met informatica kan grofweg onderscheid worden gemaakt tussen twee typen onderzoek. Enerzijds gaat het om onderzoek dat zich richt op rechtsvragen naar aanleiding van het toepassen van ICT-middelen. Daarbij worden de traditionele (aangepaste) leerstukken uit de rechtswetenschap gebruikt om bepaalde nieuwe rechtsvragen te onderzoeken die de toepassing van (nieuwe) ICT-middelen met zich meebrengt (zie: Groothuis, 2004 en Siemerink, 2006). Anderzijds gaat het om onderzoek dat zich richt op de mogelijkheden die nieuwe informaticatechnieken bieden voor toepassing in de (rechts)praktijk, ook wel aangeduid als de rechtsinformatica (Van den Herik, 1991). Het gaat bij dit rechtsinformatica-onderzoek om de inzet van elektronische hulpmiddelen voor het ondersteunen, automatiseren en intelligentiseren van (juridische) besluitvormingsprocessen. Ons onderzoek richt zich in dat verband op de toepassing van softwareagenten in een deeldomein van de politiële gegevensverwerking en meer specifiek op de uitwisseling van gegevens. Daarbij onderzoeken wij de mogelijkheden om de juridische

besluitvormingsprocessen ten aanzien van de uitwisseling te automatiseren of te ondersteunen met behulp van softwareagenten.

Franken (2004) wijst er in dit verband terecht op dat het recht niet louter bestaat uit een systeem van regels waarmee door middel van een juiste toepassing gekomen kan worden tot een rechtsbeslissing. De kern van het probleem bij de toepassing van rechtsinformaticatechnieken is gelegen in de omstandigheid dat er vrijwel altijd keuzen moeten worden gemaakt ten aanzien van de interpretatie van een regel en van de classificatie van de feiten. Deze keuze wordt bemoeilijkt doordat de juridische taal zich kenmerkt door ambiguïteit. Effectieve informaticatoepassingen voor rechtsbeslissingen zouden daarom slechts toegepast kunnen worden in 'overzichtelijke' rechtsgebieden waarbij er niet of nauwelijks discussie is over de uitleg van regels of de interpretatie van rechtsconcepten. In dergelijke domeinen zijn de rechtsregels en begrippen immers relatief eenvoudig en eenduidig te formaliseren. Een en ander betekent volgens hem echter niet dat er in het geheel geen perspectief voor rechtsinformatica-onderzoek zou zijn of dat dergelijk onderzoek zich noodzakelijkerwijs zou moeten beperken tot overzichtelijke rechtsdomeinen. Franken stelt in dat verband voor om het recht op te vatten als een vorm van informatieverwerking:

> "We moeten kijken naar individuen, die met elkaar in interactie zijn en daarmee een sociaal systeem vormen. Bezien we de interacties van meerdere personen – sociale organisaties als een vereniging, onderneming, staat, *de* samenleving – dan gaat het niet zozeer om de individuen waaruit die organisaties zijn samengesteld, maar de wijze waarop het individu zich gedraagt, met andere woorden om de *rol*, die een individu binnen een organisatie vervult. Het meest eenvoudige sociale systeem is de interactie tussen twee met elkaar communicerende individuen. In de communicatie neemt ieder net zoals bij formele en informele organisaties het geval is, een rol op zich, die inhoudt hoe hij zich *moet* gedragen. In de interactie bestaat dan een norm als bindende verwachting met betrekking tot het gedrag van de ander, die tevens bepalend is voor het eigen gedrag." (Franken, 2004, p. 68)

Deze opvatting raakt de kern van het uitgangspunt van ons onderzoek dat zich richt op de toepassing van een normatief multi-agentsysteem in het domein van de uitwisseling van politiegegevens. Immers, uit hoofdstuk 5 en 6 is naar voren gekomen dat het bij de besluitvorming rondom de uitwisseling van politiële gegevens – en in het bijzonder bij de uitwisseling van criminele inlichtingen – in beginsel gaat om de interactie tussen de individuele politieambtenaren. Dat geldt met name voor de toepassing van de (open) normen in het domein van de gegevensuitwisseling.

In het onderhavige hoofdstuk stellen wij voor om (delen) van de huidige informatie-uitwisseling te automatiseren en te intelligentiseren door de toepassing van softwareagenten die, al dan niet in opdracht van hun gebruiker, met elkaar onderhandelen over de vraag of bepaalde informatie mag of moet worden verstrekt. Bij deze onderhandeling gaat het om de toepassing en interpretatie van relevante feiten en rechtsregels. Het is onvermijdelijk dat in

de kennisbank van de betreffende softwareagenten regels worden opgeslagen die feitelijk een interpretatie van de wettelijke normen vormen. Daarmee worden de softwareagenten de uitvoerders van een (regionaal) beleid ten aanzien van de interpretatie van de open normen. Uit de analyse van het juridisch kader in hoofdstuk 3 is naar voren gekomen dat de regionale verantwoordelijken, gelet op de relatieve grote regionale autonomie, binnen de grenzen van de wet de vrijheid hebben om lokaal beleid te ontwikkelen ten aanzien van de uitwisseling van politiegegevens. Deze autonomie komt tot uitdrukking in de regionaal georganiseerde verantwoordelijkheidsstructuur die in de Wpolg is vastgelegd met betrekking tot de verwerking van politiegegevens. Hierdoor kunnen in het domein van de uitwisseling van criminele inlichtingen regionale verschillen optreden in de wijze waarop dit beleid is ingevuld. In sectie 7.4 gaan wij in op de juridische vragen die dit met zich meebrengt bij de inzet van softwareagenten.

De toepassing van de wettelijke regels en de omzetting van deze regels in (regionaal) beleid brengt ons op het volgende punt, namelijk de theoretische basis die ten grondslag ligt aan ons voorstel tot het toepassen van informatie-uitwisseling met behulp van softwareagenten. Wij menen dat de inzet van softwareagenten, mits op de juiste wijze toegepast, op een adequate wijze kan bijdragen aan de regulering van de informatie-uitwisseling in het politiedomein. Waar het bij de informatie-uitwisseling in de kern van de zaak om gaat is immers het reguleren van gedrag van politieambtenaren.

Ons idee over het geautomatiseerd reguleren van het gedrag van politieambtenaren met behulp van softwareagenten is geïnspireerd door het werk van Lessig (1996, 1999) met betrekking tot het reguleren van gedrag van de mens in de zogenaamde *Cyberspace*. Hiermee doelt Lessig op de 'ruimte' tussen de geografisch gescheiden computers die via een computernetwerk (Internet) verbonden zijn. Lessig onderscheidt vier soorten dwangmiddelen om het gedrag van mensen te reguleren: (1) recht, (2) sociale normen, (3) markten, en (4) *nature*. Vervolgens betoogt hij dat het equivalent van '*nature*' in de cyberspace de softwarecode is. Hij introduceert daarmee de gedachte om het gedrag van Internetgebruikers te reguleren door middel van technische protocollen en netwerkarchitecturen en stelt dat de softwarecode een bijzonder sterke vorm van reguleren is omdat het direct werkt en het gedrag normeert op een krachtiger manier dan met wetten en sociale normen het geval is. Lessig stelt dan dat een softwarecode mogelijkheden biedt om als 'wet' te functioneren in de *cyberspace (*de '*Code as Law'* theorie).

Op deze gedachte is in de rechtswetenschappelijke literatuur van verschillende kanten kritiek geuit. Franken (2004) stelt dat aan de theorie van Lessig de gedachte ten grondslag ligt dat *cyberspace* wordt gezien als een andere wereld dan de omgeving waarin mensen van vlees en bloed leven. Hij wijst erop dat het ook in cyberspace uiteindelijk gaat om mensen die een communicatiemiddel gebruiken waarbij het recht en de wet dus ook geldt voor de

mensen die het middel gebruiken. Bovendien kleeft volgens Franken aan de stelling van Lessig het bezwaar dat de technische code niet alleen cyberspace zal reguleren maar ook de normen en waarden van de reële wereld zal gaan bepalen. De technologie vormt dan de wet voor de samenleving zelf. Franken kiest daarom voor een benadering waarin wordt uitgegaan van de waarden en normen die *offline* gelden. Dommering (2006) sluit zich aan bij deze benadering en wijst op de mogelijkheden om een softwarecode in de *cyberspace* van Internet te gebruiken als een instrument om de wet te handhaven.

Ons onderzoek richt zich niet primair op de cyberspace van Internet maar op de cyberspace van de politiële informatiesystemen waarbij wij de C*ode as Law* theorie van Lessig toepassen in het domein van de gegevensuitwisseling. Wij kiezen daarmee voor het uitgangspunt van Franken en Dommering. Dus: wat in de offline wereld geldt met betrekking tot de gegevensuitwisseling dient het uitgangspunt te vormen voor de normatieve beperkingen in de softwarecode van de verschillende softwareagenten. Dit biedt ons inziens een goed aanknopingspunt voor een adequaat handhavingsinstrument in de cyberspace van het politiële informatiesystemen.

7.2 Normatieve softwareagenten in het CIE-domein

De toepassing van normatieve multi-agenttechnieken in het CIE-domein en specifiek de inzet van softwareagenten in het proces van informatie-uitwisseling, roept allereerst een fundamentele vraag op *welk type* softwareagent zou moeten worden ingezet in het proces van informatie-uitwisseling. In hoofdstuk 2 hebben wij het onderscheid beschreven dat Brazier e.a. (2003) maken tussen de verschillende gradaties van autonomie bij softwareagenten: (1) de slaaf, (2) vertegenwoordiger, en (3) de vrije agent. In het proces van informatie-uitwisseling menen wij dat, afhankelijk van de deeltaakuitvoering, deze drie typen softwareagenten bruikbaar kunnen zijn.

Uit de organisatieanalyse is naar voren gekomen dat de uitwisseling in dit deeldomein van de politieorganisatie nog grotendeels een fysieke aangelegenheid is waardoor het risico bestaat dat de gegevensuitwisseling sterk afhankelijk is van personen en functies. Dit betekent dat naarmate de schaal waarop informatie wordt uitgewisseld toeneemt, het risico ontstaat dat de feitelijke informatie-uitwisseling stroperiger gaat verlopen. De menselijke capaciteit met betrekking tot het doorzoeken van informatiesystemen en het selecteren is immers beperkt.

In de organisatieanalyse hebben wij in kaart gebracht hoe het uitwisselingsproces in de praktijk verloopt en welke functies en organisatieonderdelen bij deze uitwisseling zijn betrokken. De volgende stap die wij in het ANITA-onderzoek hebben gezet om te komen tot een normatief multi-agentsysteem bestaat uit het definiëren van de verschillende rollen en taken die software-

agenten kunnen vervullen bij de uitvoering van de kennisintensieve deeltaken. Wij stellen een systeem voor waarin de huidige en grotendeels handmatige gegevensuitwisseling zal worden geautomatiseerd. Wij merken op dat wij daarbij zijn uitgaan van de drie onderscheiden kennisintensieve deeltaken (hoofdstuk 6) maar dat wij ons daartoe niet zullen beperken.

Zes voorbeeldagenten
In dit hoofdstuk doen wij enkele voorstellen om normatieve softwareagenten op een bredere schaal in te zetten teneinde de informatie-uitwisseling binnen het bestaande juridische kader te optimaliseren. In deze sectie definiëren wij deze rollen aan de hand van zes agentmodellen die binnen een normatief multi-agentsysteem voor het politiedomein een bepaalde (deel)taak moeten uitvoeren. De CommonKads-methode voorziet in de beschijving van 'menselijke' agenten waarbij het onder meer gaat om de beschrijving van veranderingen die geautomatiseerde toepassingen kunnen hebben op de mensen in de organisatie. Het gaat dan om veranderingen op het terrein van bevoegdheden, taken en benodigde kennis. Wanneer bepaalde kennisintensieve taken immers geheel of gedeeltelijk worden geautomatiseerd heeft dat consequenties voor de personen die voorheen belast waren met die taakuitvoering. In het ANITA-project hebben wij ons beperkt tot het onderzoeken van de mogelijkheden voor de inzet van softwareagenten in het proces van informatie-uitwisseling.

Onze normatieve agentmodellen zijn als volgt opgebouwd. Allereerst wordt er een beschrijving gegeven van de naam van de agent. Vervolgens wordt in het model aangegeven in welk deel van de organisatie wij menen dat de softwareagent zou moeten functioneren. In de CommonKads-methode wordt daarbij een onderscheid gemaakt tussen menselijke agenten en softwareagenten. Wij beschrijven in deze sectie slechts de softwareagenten omdat ons onderzoek zich richt op de mogelijkheden voor toepassing van softwareagenten in het uitwisselingsproces. In het model geven wij in afwijking van de standaard CommonKads-modellen tevens aan welk type softwareagent (slaaf, vertegenwoordiger, vrije agent) de betreffende deeltaak zou moeten uitvoeren. Het onderscheid naar typen softwareagenten is in het CIE-domein van belang omdat we zullen zien dat bij bepaalde taakuitvoeringen de mogelijkheden om de taak volledig te laten uitvoeren door een autonome softwareagent juridische beperkingen kent. Wij zullen de keuze voor de mate van autonomie per agentmodel toelichten.

Het agentmodel bestaat verder uit een beschrijving van de betrokken taken en een overzicht van de andere agenten waarmee moet worden gecommuniceerd. Voorts wordt gespecificeerd over welke kennisitems de agent dient te beschikken en welke competenties en bevoegdheden de agent nodig heeft voor de uitvoering van de deeltaak. Natuurlijk wordt ook in het agentmodel beschreven welke verantwoordelijkheden de agent heeft ten aanzien van de taakuitvoering en welke eventuele beperkingen hem worden opgelegd.

De agentmodellen van CommonKads zijn niet specifiek ontwikkeld voor normatieve softwareagenten. In de modellen wordt slechts aangegeven welke kennis nodig is voor de uitvoering van de betreffende taken. Wij richten ons in dit onderzoek specifiek op de juridische kennis die nodig is voor de uitvoering van de deeltaken door de onderscheiden softwareagenten. Voor het specificeren van deze normatieve kennis, die wij beperken tot de relevante normen uit de Wpolg en de Bpolg en zoeken wij aansluiting bij de *normframes* zoals deze zijn onderscheiden door Van Kralingen (1995). Hij heeft zich in zijn onderzoek gericht op het nader specificeren van juridische domeinkennis ten behoeve van de ontwikkeling van kennis- en expertsystemen waarbij hij met name een oplossing heeft gezocht voor de taakafhankelijkheid van de representatie van juridische kennis. Door deze afhankelijkheid dient de juridische kennis per taak te worden gerepresenteerd. Van Kralingen heeft in zijn onderzoek modellen ontwikkeld voor de representatie van wet- en regelgeving die het mogelijk maakt dat dezelfde kennisrepresentatie voor verschillende soorten taken kan worden gebruikt. Voor ons onderzoek is dat van belang, aangezien het betekent dat het technisch mogelijk is dat de representatie van de juridische kennis in het CIE-domein gebruikt kan worden door de verschillende typen deeltaken en bijbehorende softwareagenten.

In de agentmodellen beschrijven wij de verschillende softwareagenten en geven wij geïnspireerd door de normframes van Van Kralingen (1995, p. 56) aan wat de juridische modaliteit is van de betreffende gedragsregulerende norm. Van Kralingen onderscheidt vier juridische modaliteiten voor gedragsnormen, te weten: (1) de verplichting, (2) het verbod, (3) de toestemming, en (4) de beoordelingvrijheid. In de verschillende agentmodellen geven wij ten aanzien van de benodigde normatieve kennis tevens aan welke van de vier juridische modaliteiten de relevante normen hebben. Deze modaliteiten zijn in het kader van het onderzoek van belang omdat zij nauw samenhangen met het type agent en de keuze om een softwareagent een bepaalde deeltaak te laten verrichten. In zijn algemeenheid zou daarbij kunnen gelden dat de modaliteiten die zien op een verplichting of een verbod, ruimere mogelijkheden laten voor meer autonome softwareagenten.

Hieronder formuleren wij in de subsecties 7.2.1 tot en met 7.2.6 op conceptueel niveau zes agentmodellen waarin softwareagenten worden beschreven die volgens ons in de toekomst zouden kunnen worden toegepast in het proces van de informatie-uitwisseling.

7.2.1 Indexeringsagent

De eerste softwareagent duiden wij als de indexeringsagent. Deze softwareagent voert op centraal niveau een indexeringstaak uit welke inhoudt dat de agent alle regionaal opgeslagen informatie indexeert in een centrale beheers-

index (cf. Kielman en Koelewijn, 2006). De beheersindex wordt opgebouwd uit informatie die afkomstig is uit alle regionale databases waarin de inlichtingen met betrekking tot zware criminaliteit liggen opgeslagen. Dit betekent dat de indexeringsagent onbelemmerd toegang moeten krijgen tot alle regionaal opgeslagen informatie waardoor de centrale beheersindex in feite een centrale database vormt waarin alle criminele inlichtingen beschikbaar zijn. Naast het eenmalig indexeren en opbouwen van de centrale beheersindex heeft de indexeringsagent tot taak om onafgebroken en autonoom alle mutaties te registreren die worden gedaan in de verschillende regionale databases. Hierdoor bevat de centrale beheersindex altijd actuele informatie.

Ten aanzien van de centrale beheersindex doet zich de juridische vraag voor, wie moet worden aangemerkt als verantwoordelijke in de zin van de Wpolg. Voor het antwoord op deze vraag zoeken wij aansluiting bij art. 6 CIE-regeling. Daarin is bepaald dat CIE-en gevraagd en ongevraagd criminele inlichtingen uitwisselen indien die van belang kunnen zijn voor de uitvoering van de politietaak. De legitimatie van de opbouw van een centrale beheersindex vloeit daarmee rechtstreeks voort uit de CIE-regeling aangezien het ons inziens verdedigbaar is dat de centrale beheersindex van belang is voor de uitvoering van de politietaak. Voorts is in art. 7 lid 1 sub b CIE-regeling voorzien in de instelling van een verwijsindex. Ingevolge dit artikel moeten alle regionale CIE-en volgens een vastgesteld model persoons- en bedrijfsgegevens, die staan geregistreerd in de regionale registers zware criminaliteit, aanleveren ten behoeve van een centrale verwijsindex die wordt beheerd door de Nationale CIE.

Wij pleiten ervoor om ten aanzien van de door ons voorgestelde centrale beheersindex aansluiting te zoeken bij deze beheersstructuur en de nationale CIE het feitelijke beheer van de centrale beheersindex te laten uitvoeren. De nationale CIE is een onderdeel van de KLPD en dat betekent dat op grond van art. 1 sub f Wpolg de Minister van Binnenlandse Zaken en Koninkrijksrelaties moet worden aangemerkt als de verantwoordelijke voor de centrale beheersindex. Een ander argument voor de keuze voor deze verantwoordelijkheidsstructuur is dat de centrale beheersindex in feite een nationaal register zware criminaliteit vormt. Gelet op de omvang van privacygevoelige informatie die daarin ligt opgeslagen is het ons inziens nodig om via de Minister van Binnenlandse Zaken een rechtstreekse democratische controle mogelijk te maken.

Wij bevelen in dat licht aan om de verwijsindex waarin de CIE-regeling thans voorziet, uit te breiden naar een centrale beheersindex en daarmee het criterium voor de aanlevering van criminele inlichtingen aan de Nationale CIE los te laten. Dit criterium bepaalt namelijk dat naast de gegevens die ten behoeve van de verwijsindex (VROS-systeem) moeten worden aangeleverd, slechts gegevens aan de Nationale CIE worden verstrekt voor zover deze

gegevens van nationale of internationale betekenis zijn. Wij pleiten er voor om één op één alle regionale gegevens aan te leveren aan Nationale CIE.

Uit de taakbeschrijving van de regionale CIE-en is naar voren gekomen dat er veel belang wordt gehecht aan rechtstreekse controle op de uitwisseling van de gegevens waarvoor zij verantwoordelijk zijn. Toepassing van een centrale beheersindex zou op het eerste gezicht kunnen betekenen dat de controle op regionaal niveau niet meer kan worden uitgeoefend. Binnen het ANITA-project hebben wij dit probleem onderkend. Daarom hebben we als uitgangspunt genomen dat de centrale beheersindex moet worden opgebouwd uit clusters die overeenkomen met de regionale registers zware criminaliteit. De regionale controle op de uitwisseling is het meest van belang bij de 00-informatie aangezien deze gevoelige informatie de grootste afbreukrisico's met zich meebrengt. De geclusterde registratie maakt het mogelijk dat regionaal rechtstreeks controle kan worden uitgeoefend op de uitwisseling van gegevens uit het cluster. Ten aanzien van de 00-informatie stellen wij verder voor om de binnen het ANITA-project ontwikkelde *information designators* toe te passen zodat ten aanzien van deze informatie een extra waarborg wordt ingebouwd tegen onbevoegde kennisneming, en kennisneming door derden die naar het oordeel van de verantwoordelijke CIE een verhoogd afbreukrisico meebrengen. Het model van de indexeringsagent ziet er zodoende als volgt uit.

Agentmodel 1	**Beschrijving**
Naam:	Indexeringsagent
Type:	Vrije agent
Organisatieonderdeel:	NCIE & Regionale CIE
Betrokken bij (deel)taak:	Indexering van de regionale registers zware criminaliteit
Communicatie:	Poortwachteragent Transactieagent Indexeringsagent
Competenties:	Mutaties detecteren en registreren Information designators maken van de 00-informatie
Verantwoordelijkheid:	Actueel houden van informatie in de centrale beheersindex.
Normatieve kennis:	Verstrekkingsbepalingen Wpolg en Bpolg
Juridische modaliteit:	Toestemming, gesloten norm

Tabel 7.1: Indexeringsagent.

De indexeringsagent dient kennis te hebben van de verstrekkingsbepalingen uit de Wpolg en de Bpolg. Zoals wij uiteen hebben gezet in hoofdstuk 3 kent de Wpolg een gesloten verstrekkingen regime. De juridische modaliteit van het gesloten verstrekkingenregime interpreteren wij als gesloten toestemmingsnormen. De in de wet genoemde ontvangstgerechtigden hebben toestemming om de informatie te ontvangen. Ten aanzien van de indexerings-

agent menen wij echter dat geen sprake zou moeten zijn van een normatieve beperking aangezien deze agent vrij moet kunnen handelen ten behoeve van de volledige opbouw van de centrale beheersindex. De taakuitvoering van de indexeringsagent vloeit voort uit de wettelijke norm inhoudende dat ter ondersteuning van de uitvoering van de politietaak politiegegevens geautomatiseerd mogen worden verwerkt.

7.2.2 Autorisatieagent

De eerste deeltaak in het proces van informatie-uitwisseling is het vaststellen van de identiteit van de informatieverzoeker. Deze deeltaak wordt in ons model uitgevoerd door de autorisatieagent. De huidige politiële informatiesystemen kennen een relatief eenvoudig systeem van autorisaties. Kort gezegd houdt dit systeem in dat daartoe bevoegde politieambtenaren door de verantwoordelijke worden geautoriseerd voor deze systemen. Concreet betekent dit dat zij een persoonlijke inlogcode met bijbehorend wachtwoord krijgen. Ten aanzien van ons voorstel tot het invoeren van een autorisatieagent roept dit de terechte vraag op welke toegevoegde waarde deze softwareagent heeft ten opzichte van het huidige autorisatiesysteem. Het antwoord op deze vraag heeft te maken met de richting waarin de computersystemen zich ons inziens zullen gaan ontwikkelen. Wij menen dat in de nabije toekomst de schaal waarop politiële informatie elektronisch zal worden geregistreerd en beschikbaar gemaakt, groter wordt en wij zijn er dan ook van overtuigd dat op de lange termijn alle regionale informatiesystemen op Europees niveau gekoppeld zullen gaan worden en deel gaan uitmaken van wat wij aanduiden met een 'politieel intranet' bestaande uit een koppeling van alle Europese politiële informatiesystemen. In het licht van deze toekomstige ontwikkelingen kan niet meer worden volstaan met de huidige regionaal georganiseerde systematiek van autorisaties.

Op de korte termijn voorzien wij een ontwikkeling waarbij naast politieambtenaren ook de ketenpartners van de politie steeds meer gebruik gaan maken van de elektronische beschikbaarheid van politiegegevens. Hierbij moet worden gedacht aan veiligheidsdiensten, de immigratie- en naturalisatiedienst, bureau Bibob etc. Dat vraagt ons inziens om een ander systeem van autorisaties aangezien de beperking tot een uitsluitend regionaal georganiseerd autorisatiesysteem niet zal kunnen volstaan.

Binnen het ANITA-project is ten aanzien van de toepassing van softwareagenten op het politiële Intranet op termijn een rol weggelegd voor een Trusted Third Party (TTP) waarbij de autorisatieagent kan nagaan of een 'onbekende', dat wil zeggen een niet-geautoriseerde softwareagent, die voor de behandeling van een informatieverzoek tijdelijk toelating vraagt, toegelaten kan worden tot de betreffende database. De autorisatieagent zal bij deze TTP moeten kunnen verifiëren of de informatieverzoeker ook informatiegerech-

tigde is in de zin van de Wpolg. Bij de TTP moeten zodoende alle informatiegerechtigden op grond van de Wpolg geregistreerd worden zodat de autorisatieagent via raadpleging van de TTP kan nagaan of er rechtmatig gegevens kunnen worden verstrekt aan de informatieverzoeker. Deze systematiek komt er op neer dat alle niet-politie-ambtenaren, die op grond van de Wpolg en de Bpolg gerechtigd zijn om politiegegevens te raadplegen en te verwerken, geregistreerd moeten worden bij de TTP.

De toepassing van een TTP vraagt ook om uitbreiding van de Wpolg waarin de TTP ons inziens zal moeten worden voorzien van een wettelijke basis. In dat verband menen wij om redenen van eenduidigheid dat, evenals bij de verantwoordelijkheidstructuur voor het beheer van de centrale beheersindex, de Minister van Binnenlandse Zaken zou moeten worden aangewezen als de verantwoordelijke voor de TTP.

In tegenstelling tot de indexeringsagent achten wij voor de uitvoering van deze deeltaak in het proces van informatie-uitwisseling de 'vertegenwoordiger' het meest aangewezen als type softwareagent. De autorisatieagent wordt binnen de beheersindex ingezet in de clusters waarbij dus ieder cluster een eigen autorisatieagent heeft. Dat sluit aan bij de autorisatiestructuur die is vastgelegd in de Wpolg waarbij in art. 6 Wpolg de verantwoordelijke het systeem van autorisaties onderhoudt. De autorisatieagent vertegenwoordigt daarmee rechtstreeks de verantwoordelijke. In art. 6 Wpolg zal dan een wettelijke grondslag gecreëerd moeten worden waarbij de bevoegdheden van de verantwoordelijke worden uitgebreid en tevens wordt voorzien in tijdelijke autorisaties van softwareagenten die niet-politieambtenaren (ketenpartners) vertegenwoordigen of buitenlandse politieambtenaren vertegenwoordigen.

Naast de verificatie van 'onbekende' informatieverzoekers dient de autorisatieagent in de tweede plaats een controle uit te voeren naar het doel van de informatieverzoek. Aan de hand van het opgegeven doel kan de autorisatieagent vervolgens de rechtmatigheid van het informatieverzoek beoordelen en nagaan welke verstrekkingsbepalingen er moeten worden toegepast.

De normatieve kennis waarmee de autorisatieagent moet worden uitgerust betreft de wettelijke bepalingen met betrekking tot het gesloten verstrekkingenregime. Aangezien er in de Wpolg en de Bpolg limitatief staat opgesomd wie gerechtigd is en de geregistreerde politiegegevens te gebruiken voor de uitvoering van de politietaak, kwalificeren wij de juridische modaliteit van deze normen als 'toestemming'. Het betreffen gesloten normen, hetgeen in concreto betekent dat wanneer de wet voorziet in verstrekking aan de informatieverzoeker, de eigenaar in beginsel de behandeling van het informatieverzoek niet kan weigeren.

Agentmodel 2	**Beschrijving**
Naam:	Autorisatieagent
Type:	vertegenwoordiger
Organisatieonderdeel:	Regionale CIE Beheersindex
Betrokken deeltaak:	Controle informatiegerechtigde
Communicatie:	Zoekagent Transactieagent
Competenties:	Verificatie autorisatie Communicatie
Verantwoordelijkheid:	Identiteit van de informatieverzoeker vaststellen en rechtmatigheid van de zoekvraag beoordelen
Normatieve kennis:	Doel informatieverzoek (Wpolg) Verstrekkingsbepalingen Wpolg en Bpolg
Juridische modaliteit:	Verplichting, gesloten norm Toestemming, gesloten norm

Tabel 7.2: Autorisatieagent.

7.2.3 Zoekagent

Als derde agent stellen wij voor om in het multi-agentsysteem rondom de centrale beheersindex binnen ieder cluster een 'slimme' vrije zoekagent in te zetten. Door middel van communicatie met een informatieverzoeker heeft de zoekagent tot taak om in kaart te brengen wat precies het informatieprobleem is. Grofweg dient de zoekagent voor het vaststellen van het informatieprobleem twee stappen te doorlopen. De eerste stap sluit aan bij de strategische uitgangspunten die zijn vastgesteld door de RHC (zie subsectie 5.4.1). De politie dient informatie zoveel mogelijk te personaliseren, dat wil zeggen dat de geregistreerde informatie moet kunnen worden toegeschreven aan een subject. De zoekagent moet daarom door middel van een aantal vragen allereerst vaststellen over welk subject er informatie wordt gezocht. Vervolgens moet de informatieverzoeker in de tweede stap aangeven wat hij precies wil weten. Deze stap is met name relevant voor de politieambtenaren die betrokken zijn bij een bepaald type rechercheonderzoek. Zij zijn veelal op zoek naar specifieke informatie over een bepaalde persoon. Kenmerkend voor de registraties in de registers zware criminaliteit is dat daarin allerlei uiteenlopende informatie over een CIE-subject ligt opgeslagen waartussen zich ook informatie bevindt die niet relevant is voor het betreffende rechercheonderzoek. Het vaststellen van het informatieprobleem ziet erop dat niet meer informatie wordt uitgewisseld dan voor het betreffende rechercheonderzoek van belang is.

Met beide stappen wordt in de zoekagent een functionele uitwerking van het proportionaliteitsbeginsel ingebouwd. Het personaliseren van de zoekvraag is daarmee zowel in het belang van de rechtshandhaving als in het belang van de rechtsbescherming. Het doel van de personalisatie van de zoekvraag is namelijk enerzijds om zo gericht en zo specifiek mogelijk zoekresultaten aan de informatieverzoeker te verstrekken. Dat is in het belang van de goede uitvoering van de politietaak omdat op die manier uitsluitend de relevante informatie verstrekt wordt en daarmee geen onnodig beslag op de tijd van de ontvanger wordt gelegd. Bovendien bestaat er minder risico dat niet relevante informatie uitlekt. Anderzijds is deze toepassing in het belang van de rechtsbescherming omdat in de personalisatie van de zoekvraag een privacywaarborg is ingebouwd. Een selectie tot het verstrekken van uitsluitend relevante informatie met betrekking tot een persoon zal immers betekenen dat zoveel mogelijk wordt voorkomen dat overbodige, niet-relevante informatie van derden eveneens wordt verstrekt. Personalisatie en informatieselectie is daarmee een functionele uitwerking van het proportionaliteitsbeginsel en een toepassing van een beperking tot het *need-to-know*-principe. De zoekagent zal daarom onderscheid moeten kunnen maken tussen de verschillende typen informatieverzoekers. Na vaststelling van de zoekvragen zal de zoekagent deze doorgeven aan de zoekmachine op de beheersindex.

Agentmodel 3	**Beschrijving**
Naam:	Zoekagent
Type:	Vrije agent
Organisatieonderdeel:	Regionale CIE Centrale beheersindex
Betrokken deeltaak:	Vaststellen informatieprobleem
Communicatie:	Identificatieagent Transactieagent
Competenties:	Kwalificeren informatieverzoekers Vaststellen van de zoekvragen
Verantwoordelijkheid:	Proportionaliteit van de zoekvraag
Normatieve kennis:	Doel informatieverzoek
Juridische modaliteit:	Verplichting, gesloten norm

Tabel 7.3: Zoekagent.

De normatieve kennis waarmee de zoekagent wordt uitgerust betreft het interpreteren van de doelstellingen voor de politiële informatieverwerkingen. Aangezien op grond van de wet slechts gegevens verwerkt mogen worden voor de wettelijk bepaalde doeleinden kwalificeren wij de juridische modaliteit als een verplichting om binnen de wettelijke doelen gegevens te zoeken.

7.2.4 Transactieagent

In het multi-agentsysteem rond de centrale beheersindex onderscheiden wij verder als vierde type agent de zogenaamde transactieagenten. Een transactieagent vertegenwoordigt informatieverzoekers. In het huidige systeem van informatie-uitwisseling zullen de transactieagenten uitsluitend CIE-ambtenaren vertegenwoordigen. Wij menen dat op er op korte termijn meer behoefte zal ontstaan ten aanzien van de mogelijkheden om ook rechercheurs door middel van transactieagenten rechtstreeks toegang te geven tot de criminele inlichtingen. Dit betekent dat ook rechercheurs vertegenwoordigd zullen worden door transactieagenten. Op de middellange en lange termijn zal in onze visie de politiële informatiehuishouding zich, als gezegd, ontwikkelen naar een politieel intranet waarop ook de nationale en Europese ketenpartners van de politiediensten via transactieagenten rechtstreeks toegang krijgen.

De transactieagenten moeten in dit systeem worden gezien als digitale 'informatiemakelaars' die namens een verzoeker onderhandelen over de vraag of zij de informatie ook verstrekt mogen krijgen. De onderhandeling wordt feitelijk geopend op het moment dat een informatieverzoek daadwerkelijk wordt geweigerd. In het geval van een weigering van een informatieverstrekking zal de transactieagent door middel van een onderhandeling met de poortwachteragent nagaan of er mogelijkheden zijn om de informatie, of delen daarvan, toch onder bepaalde beperkende voorwaarden verstrekt te krijgen. Bij deze onderhandeling zal met name het doel waarvoor de informatie gebruikt gaat worden bepalend zijn voor het antwoord op de vraag of de informatie ook daadwerkelijk verstrekt kan worden. Binnen het ANITA-project heeft Dijkstra (2007) daarvoor communicatieprotocollen ontwikkeld. Aan de hand van een aantal relatief eenvoudige voorbeelden laat hij zien hoe een informatietransactie tot stand kan komen op basis van een wisseling van argumenten tussen softwareagenten onderling.

Het doel van een dergelijke onderhandeling is een gecontroleerde informatieuitwisseling die met name binnen het CIE-domein van belang is. Gelet op het privacygevoelige karakter van criminele inlichtingen zal steeds moeten worden nagegaan of het noodzakelijk is om de informatie te verstrekken, of dat er, gelet op het doel waarvoor de informatie wordt gevraagd, afbreukrisico's zijn en of er dientengevolge aanleiding bestaat om beperkende voorwaarden te stellen aan het gebruik van de informatie. De inzet van de communicatieprotocollen en de onderhandeling ten aanzien van een informatietransactie

tussen de transactieagent en de poortwachteragent beogen de rechtmatigheid en de doelmatigheid van de informatie-uitwisseling te bevorderen.

Agentmodel 4	**Beschrijving**
Naam:	Transactieagent
Type:	Vertegenwoordiger
Organisatieonderdeel:	Alle
Betrokken deeltaak:	Beoordeling weigeringsgronden Vaststellen informatieproduct
Communicatie:	Autorisatieagent Poortwachteragent
Competenties:	Onderhandelen
Verantwoordelijkheid:	Rechtmatigheid en doelmatigheid
Normatieve kennis:	Verstrekkingsbepalingen Wpolg en Bpolg Doel informatieverzoek Voorwaarden
Juridische modaliteit:	Toestemming, gesloten norm Verplichting, gesloten norm Beoordelingsvrijheid, open norm

Tabel 7.4: Transactieagent.

De normatieve kennis waarmee de transactieagent moet worden uitgerust is buitengewoon complex omdat het een combinatie is van gesloten en open normen. De verstrekkingsnormen en de doeleinden zijn, zoals hiervoor reeds uiteengezet, limitatief opgesomd en derhalve kwalificeren wij de juridische modaliteit als toestemming en verplichting. Beide betreffen gesloten normen. Ten aanzien van de vraag of de informatieverzoeker, of de transactieagent namens de informatieverzoeker, bepaalde beperkende voorwaarden accepteert staat te zijner beoordeling. De transactieagent dient daarin een beperkte beoordelingsruimte te krijgen. Daarin moet hij bepalen of hij akkoord gaat met bepaalde beperkende voorwaarden.

7.2.5 Poortwachteragent

Binnen de centrale beheersindex zal in ons model ieder cluster worden uitgerust met een zogenaamde poortwachteragent. De poortwachter is ons vijfde agenttype. Het is de rechtstreekse vertegenwoordiger van de regionale verantwoordelijke in de zin van de Wpolg. De taak van de poortwachteragent is om aan de hand van de zoekresultaten en het doel waarvoor de informatie werd opgevraagd, te bepalen of de gevonden informatie ook kan worden verstrekt. De poortwachteragent heeft daarmee de taak om na te gaan of er reden is om het informatieverzoek te weigeren. Bij de beoordeling

van de vraag of het verstrekken van de zoekresultaten moet worden geweigerd vormen in het huidige systeem van informatie-uitwisseling in het CIE-domein de afhandelingscodes het belangrijkste aanknopingspunt.

Daarnaast moeten ook de betrouwbaarheidscoderingen meegenomen worden bij de beoordeling van de verstrekking. De betrouwbaarheidscoderingen van de geregistreerde informatie spelen ons inziens een belangrijke rol ten aanzien van het doel waarvoor de informatie wordt verzocht. Voor een rechercheonderzoek is het eerst en vooral van belang om zoveel mogelijk betrouwbare en geverifieerde informatie uit te wisselen. Voor een informatieverzoek dat afkomstig is van een CIE-ambtenaar met als doel het veredelen van zijn eigen informatie kan het evenwel ook zinvol zijn om kennis te nemen van 'onbetrouwbare' zachte informatie omdat juist deze informatie meegenomen kan worden in de beoordeling van de eigen (zachte) informatie. Wanneer het informatieverzoek gedaan wordt in het kader van een integriteitsbeoordeling van een persoon ten behoeve van het openbaar bestuur, oftewel, een informatieverzoek van het bureau Bibob, dan zal de poortwachteragent uitsluitend geverifieerde en betrouwbare informatie moeten verstrekken. Op basis van het zoekresultaat, de afhandelingscodes en de betrouwbaarheidscoderingen zal de poortwachteragent voorts moeten nagaan of aan de verstrekking van de informatie beperkende voorwaarden moeten worden gesteld. Hierbij kan gedacht worden aan de voorwaarde dat bepaalde gevoelige informatie niet gebruikt mag worden voor operationele doeleinden. De onderhandeling over de voorwaarden wordt gevoerd met de transactieagent.

Agentmodel 5	**Beschrijving**
Naam:	Poortwachteragent
Type:	Vertegenwoordiger
Organisatieonderdeel:	Regionale CIE
Betrokken deeltaak:	Beoordeling toepassing van de weigeringsgronden Stellen van beperkende voorwaarden
Communicatie:	Hoofd CIE Transactieagent
Competenties:	Beoordelen en onderhandelen
Verantwoordelijkheid:	Rechtmatigheid van de informatieverstrekking Controleren van de regionale belangen
Normatieve kennis:	Verstrekkingsbepalingen Weigeringsgronden Afhandelingscodes & betrouwbaarheidscodes
Juridische modaliteit:	Toestemming, gesloten norm Beoordelingsvrijheid, open norm Toestemming, gesloten norm

Tabel 7.5: Poortwachteragent.

Met betrekking tot de normatieve kennis geldt voor de poortwachteragent in beginsel hetzelfde als voor de transactieagent, met dien verstande dat de complexiteit van de uitvoering van de taak door de poortwachteragent, complexer is. Dat wordt veroorzaakt doordat de wettelijke weigeringsgronden en de beoordeling van de afbreukrisico's in feite een ruime beoordelingsvrijheid laten aan de informatie-eigenaar. Datzelfde geldt voor de eventueel te stellen beperkende voorwaarden met betrekking tot de verdere verwerking van gegevens.

7.2.6 Surveillanceagent

Om de integriteit en de betrouwbaarheid van een multi-agentsysteem binnen het politiedomein te vergroten heeft Aldewereld (2007) voorgesteld om een elektronische institutie te introduceren. In de elektronische institutie wordt de verzameling protocollen en normen gedefinieerd waaraan de softwareagenten zich in dit domein dienen te houden. Met behulp van de elektronische institutie kan worden bewerkstelligd dat enerzijds de vrije (autonome) softwareagenten in het multi-agentsysteem vrij kunnen handelen, terwijl anderzijds in de elektronische institutie is vastgelegd binnen welke normen en protocollen dit handelen dient plaats te vinden. In het domein van de politiële gegevensverwerking menen wij dat de toepassing van een elektronische institutie nodig is om toezicht te kunnen houden op de vrije softwareagenten binnen het systeem. Daarmee moet ongewenst emergent gedrag worden gecorrigeerd. Dit toezicht wordt, zo stellen wij voor, dan feitelijk uitgevoerd door de zogenaamde surveillanceagenten die ons zesde type agenten vertegenwoordigen. Het doel van de surveillanceagenten is het registeren en controleren van alle informatietransacties binnen de centrale beheersindex en daarbij dienen zij zonder enige vorm van vrijheid de in de elektronische institutie gedefinieerde normen en protocollen bij de controle toe te passen. De surveillanceagenten houden specifiek toezicht op de vrije indexeringsagenten en de vrije zoekagenten. Wanneer bijvoorbeeld blijkt dat een zoekagent binnen de centrale beheersindex ook zoekopdrachten gaat uitvoeren binnen andere clusters dan hem is toegestaan dan heeft de surveillanceagent de bevoegdheid negatieve feedback te geven aan de zoekagent teneinde deze weer binnen de normen te laten functioneren. Aldewereld (2007) heeft in zijn onderzoek laten zien dat dergelijk normafwijkend gedrag van vrije softwareagenten langs deze weg gecorrigeerd kan worden. In de functionele uitwerking die wij voorstellen verricht de surveillanceagent (1) het toezicht en (2) in normafwijkende situaties deelt hij de negatieve feedback uit.

Gelet op de toezicht- en controletaak zal de surveillanceagent alle informatietransacties moeten controleren op rechtmatigheid. Dit betekent dat de surveillanceagent voor deze taak moet worden uitgerust met alle relevante juridische kennis die de andere softwareagenten gebruiken voor de uitvoering van hun deeltaken. Het betreft zowel de open normen als de gesloten normen.

Agentmodel 6	**Beschrijving**
Naam:	Surveillanceagent
Type:	Slaaf
Organisatieonderdeel:	Centrale beheersindex
Betrokken deeltaak:	Toezicht op de rechtmatige uitvoering van de deeltaken en geven van negatieve feedback bij onrechtmatige handelingen
Communicatie:	Elektronische institutie
Competenties:	Registratie en controle op de informatietransacties Negatieve feedback
Verantwoordelijkheid:	Handhaven van de normen in het uitwisselingsproces
Normatieve kennis:	Wpolg, Bpolg, CIE-regeling
Juridische modaliteit:	Verplichting, gesloten normen Verbod, gesloten normen Toestemming, gesloten en open normen

Tabel 7.6: Surveillanceagent.

7.3 Conceptuele uitwerking

In deze sectie werken wij de toepassing van de in sectie 7.2 beschreven softwareagenten op conceptueel niveau verder uit. Het betreft relatief eenvoudige voorbeelden waarmee wij beogen te laten zien waar softwareagenten en de binnen het ANITA-project ontwikkelde AI-technieken, toegepast kunnen worden bij deeltaken in het proces van informatie-uitwisseling. Het gaat daarbij in het bijzonder om de vraag of met de inzet van deze softwareagenten ook de in hoofdstuk 5 geconstateerde knelpunten kunnen worden opgelost en welke invloed de inzet van softwareagenten in dit domein voorts heeft op een verbetering van de informatie-uitwisseling. Zoals wij in hoofdstuk 1 uiteen hebben gezet benaderen wij verbetering vanuit het perspectief van de rechtshandhaving en de rechtsbescherming.

Deze sectie is als volgt opgebouwd. In subsectie 7.3.1 werken wij ons idee voor de opbouw van een centrale beheersindex verder uit. Vervolgens beschrijven wij in subsectie 7.3.2 de toepassing van de autorisatieagenten en de TTP. Subsectie 7.3.3 beschrijft de wijze waarop informatietransacties tot stand kunnen komen via een poortwachteragent en een transactieagent. Tenslotte geven wij in subsectie 7.3.4 een nadere uitwerking van de toepassing van controle op de informatie-uitwisseling met behulp van de surveillanceagenten.

7.3.1 Centrale beheersindex

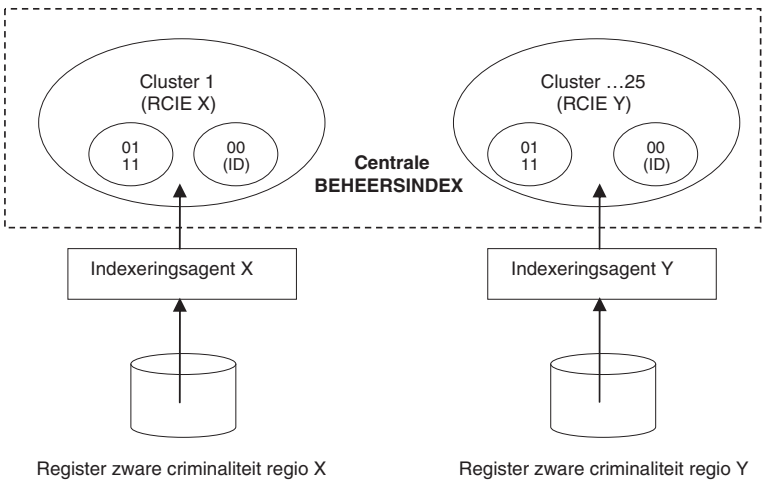
Voor de toepassing van softwareagenten in de elektronische uitwisseling van criminele inlichtingen zoeken wij aansluiting bij het PZU-systeem zoals wij dat hebben beschreven in hoofdstuk 4. In het PZU-systeem worden de regionale registers zware criminaliteit ontsloten via een centrale server. Op de regionale informatiesystemen van de CIE kan worden ingelogd op de centrale server van het PZU-systeem. Na de autorisatieprocedure kan er een zoekopdracht worden uitgezet. De centrale server 'vertaalt' als het ware de zoekopdracht naar de 25 regionale registers zware criminaliteit waarna de resultaten van de zoekopdracht vervolgens via de centrale server weer worden teruggekoppeld naar het regionale informatiesysteem. PZU functioneert daarmee als een schakel tussen de regionale registers zware criminaliteit.

In hoofdstuk 4 hebben wij beschreven dat aan het PZU-systeem een aantal (vooral praktische) bezwaren lijken te kleven. De gebruikers van het PZU-systeem die wij hebben gesproken klaagden met name over de traagheid van de afhandeling van informatieverzoeken en het gebrek aan zoekmogelijkheden. Het verbeteren van de prestaties van het systeem is ons inziens vooral een technische kwestie omdat verbetering kan worden gerealiseerd door snellere systemen en verbindingen. Technische verbeteringen op dit niveau vallen echter buiten het bereik van ons onderzoek. Fundamenteler zijn de functionele keuzen die ten grondslag liggen aan het PZU-systeem. Binnen het systeem wordt namelijk uitsluitend 11-informatie en 01-informatie ontsloten. Hoewel deze mogelijkheid reeds een aanzienlijke verbetering betreft in de uitwisseling van criminele inlichtingen, kwam uit ons veldwerk naar voren dat bij veel regionale CIE-en de behoefte leeft om elektronisch ook de zogenaamde 00-informatie van andere regio's te kunnen raadplegen. Gevraagd naar de reden waarom dat nog niet gebeurt werd door verschillende CIE-ers aangevoerd dat er nog onvoldoende technische en organisatorische waarborgen zijn die het mogelijk maken om ook deze 'zeer gevoelige' politiële informatie gecontroleerd elektronisch uit te wisselen. Met name voor de 00-informatie geldt dat de elektronische uitwisseling juist vanwege de grote afbreukrisico's die eraan kunnen kleven, zeer zorgvuldig zal moeten geschieden.

Om de elektronische uitwisseling van alle criminele inlichtingen, met name de 00-informatie, te automatiseren hebben wij in de voorgaande sectie het idee van de centrale beheersindex geïntroduceerd. Deze index wordt opgebouwd uit alle informatie die ligt opgeslagen in de regionale registers zware criminaliteit. De centrale beheersindex wordt vervolgens opgedeeld in clusters die overeenkomen met de regionale registers zware criminaliteit. In de clusters moet dan onderscheid worden gemaakt tussen de 00-informatie enerzijds en de 11- en 01-informatie anderzijds. Van de regionaal geregistreerde 00-informatie zal in de centrale beheersindex uitsluitend conform het idee van Teepe (2006) een *information designator* worden opgeslagen. Het doel van het uitsluitend opslaan van een *information designator* is gelegen in

de omstandigheid dat het bij 00-informatie gaat om politiegegevens met een hoog afbreukrisico. Ten aanzien van deze informatie bestaat daarom binnen de CIE de behoefte vergaande controle te houden op het verstrekken van deze informatie. De *information designator* maakt deze controle mogelijk doordat niet de informatie zelf wordt opgeslagen in de centrale beheersindex maar slechts een 'digitale vingerafdruk' van deze informatie. Uit de opgeslagen *information designators* zelf kan geen inhoudelijke informatie worden afgeleid.

Om de informatie in de centrale beheersindex actueel te houden wordt ieder regionaal register zware criminaliteit voorzien van een indexeringsagent. Deze softwareagent heeft tot taak om alle regionale mutaties op te slaan in het overeenkomende cluster binnen de centrale beheersindex. Daardoor is er op de centrale server een actueel nationaal register zware criminaliteit met daarin alle in Nederland beschikbare 11-informatie en 01-informatie. Het doel van de clustering is om aan te sluiten bij de bestaande regionale verantwoordelijkheidsstructuur zoals die is vastgelegd in de Politiewet 1993 en in de Wpolg. De regionale CIE blijft dus primair verantwoordelijk voor het beheer en de uitwisseling van de eigen informatie binnen deze database. Schematisch is de werking van de indexeringsagenten gegeven in Figuur 7.1.



Figuur 7.1: Opbouw centrale beheersindex.

Ten aanzien van de taakuitvoering van de indexeringsagent rijst de vraag aan welke regels deze softwareagent gebonden is. Daarvoor is bepalend of de verstrekking van de regionaal opgeslagen politiegegevens gekwalificeerd zou moeten worden als een verstrekking in de zin van de Wpolg en daarmee valt onder de beperkingen van de verstrekkingsbepalingen. Wij menen echter dat dit niet het geval is. De elektronische gegevensverstrekkingen van de regionale registers zware criminaliteit naar een centrale beheersindex zijn geen verstrekkingen in de zin van art. 1 sub d Wpolg. In dit artikel is het ver-

strekken van politiegegevens gedefinieerd als het "ter beschikking stellen van politiegegevens". Onder het ter beschikkingstellen van politiegegevens moet blijkens art. 1 sub e Wpolg worden verstaan het verstrekken van politiegegevens aan personen die overeenkomstig de wet zijn geautoriseerd. Bepalend is met andere woorden dat de politiegegevens aan personen worden verstrekt die krachtens art. 6 Wpolg door de verantwoordelijke zijn geautoriseerd. Bij het uitsluitend opbouwen van de beheersindex worden geen politiegegevens verstrekt aan personen en daarom zal voor deze vorm van gegevensverstrekking niet het juridisch kader voor de verstrekkingen van toepassing zijn. Hoewel er geen sprake is van een verstrekking in de zin van de Wpolg blijft wel de vraag overeind of de opbouw van een centrale beheersindex zoals wij die voorstaan op grond van de Wpolg een wettelijke grondslag kent.

Voor het antwoord op deze vraag is art. 13 Wpolg bepalend. Daarin is de juridische grondslag vastgelegd voor de verdere verwerking van politiegegevens. Wij kwalificeren de taakuitvoering van de indexeringsagent als een 'verdere verwerking' van de regionaal opgeslagen criminele inlichtingen. Art. 13 lid 1 en 3 Wpolg legitimeren deze verdere verwerking voor zover relevant voor:

1. het vaststellen van eerdere verwerkingen ten aanzien van eenzelfde persoon of zaak, onder meer ter bepaling van eerdere betrokkenheid bij strafbare feiten;
2. het ophelderen van strafbare feiten die nog niet herleid konden worden tot een verdachte;
3. identificatie van personen of zaken;
4. het onder de aandacht brengen van personen of zaken met het oog op het uitvoeren van een gevraagde handeling dan wel met het oog op een juiste bejegening van personen;
5. het uitvoeren van taken ten dienste van de justitie;
6. de geautomatiseerde vergelijking met het oog op de melding van verschillende verwerkingen jegens eenzelfde persoon.

De Memorie van Toelichting zegt over de toepassing van dit artikel het volgende.

> "Bij de gegevens die op grond van het eerste lid ter beschikking worden gesteld voor zover nodig ter ondersteuning van de politietaak, geldt dit niet en moet per geval worden beoordeeld in hoeverre het andere korps de gegevens daadwerkelijk nodig heeft voor de uitvoering van de politietaak. Voor deze gegevens geldt conform het principe van art. 15, eerste lid, dat de aldus ter beschikking gestelde gegevens in beginsel alleen gebruikt mogen worden voor het doel waarvoor zij in het betreffende geval ter beschikking worden gesteld. Via de schriftelijke vastlegging geeft de verantwoordelijke vooraf aan welke van de gegevens rechtstreeks raadpleegbaar worden gesteld en welke ter beschikking worden gesteld aan andere korpsen voor zover nodig ter ondersteuning van de politietaak alsmede voor welk doel."[127]

127 Kamerstukken II 2005/06, 30 327, nr. 3, p. 59.

Wij menen dat de centrale beheersindex ten aanzien van de CIE-informatie binnen dit wettelijk kader opgebouwd en gebruikt zou kunnen worden. Vooraf dient de verdere verwerking echter door de regionaal verantwoordelijken te worden vastgelegd conform art. 13 Wpolg juncto art. 6:2 Bpolg. Wel brengen de bovenstaande zes doelen, beperkingen mee voor de mogelijkheden van derden om gebruik te maken van de gegevens die liggen opgeslagen in de centrale beheersindex. De Wpolg beperkt het raadplegen van deze gegevens in art. 13 lid 1 Wpolg namelijk tot de politieambtenaren die ingevolge art. 6 geautoriseerd zijn.

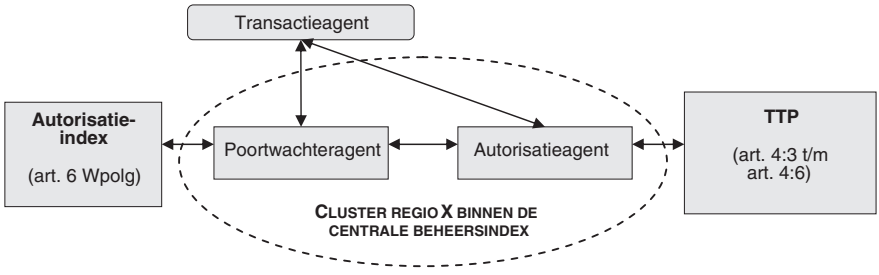
Met het idee van de centrale beheersindex beogen wij zoveel mogelijk aan te sluiten bij de bestaande informatiesystemen en de daarbij behorende protocollen voor de informatie-uitwisseling. Het voordeel van indexering is ten eerste dat de zoeksnelheid significant toeneemt. Een zoekvraag hoeft immers niet meer via het netwerk uitgezet te worden bij de verschillende regionale informatiesystemen maar kan zich beperken tot de index. Een tweede voordeel dat de beheersindex biedt is dat een centrale database de technische mogelijkheden voor het geautomatiseerd vergelijken en het gecombineerd zoeken vergroot. Ten derde faciliteert de centrale beheersindex de verplichting van de verantwoordelijke ingevolge art. 15 Wpolg welke inhoudt dat hij politiegegevens ter beschikking stelt die door hemzelf dan wel door een andere verantwoordelijke overeenkomstig art. 6 lid 2 Wpolg zijn geautoriseerd voor de verwerking van politiegegevens.

7.3.2 Autorisatie en doelstellingscontrole

De elektronische informatie-uitwisseling van criminele inlichtingen wordt in het door ons voorgestelde model uitsluitend afgehandeld via de centrale beheersindex. Dit zou betekenen dat de drie vormen van elektronische informatie-uitwisseling (hoofdstuk 4), welke wij in de onderzoeksperiode met betrekking tot de uitwisseling van criminele inlichtingen hebben geconstateerd, worden vervangen. Met betrekking tot de autorisatie hebben wij aangegeven dat wij met de introductie van een autorisatieagent beogen te anticiperen op een toekomstige ontwikkeling. Wij gaan zoals gezegd uit van een trend waarin informatiesystemen steeds meer gekoppeld worden aan andere (niet politiële) netwerken. Wij hebben daarbij aangegeven dat wij voorzien dat ook de politiële informatiesystemen in toenemende mate gekoppeld gaan worden en een onderdeel gaan vormen van grotere gedistribueerde politiële informatiesystemen waarop Europese politiediensten, inlichtingen- en veiligheidsdiensten en politiële ketenpartners worden aangesloten. Wij hebben in dat verband aangegeven dat op termijn sprake zal zijn van een politieel intranet waarop alle verschillende diensten kunnen communiceren en informatie uitwisselen. Dat vraagt ons inziens om een nieuwe wijze van autoriseren aangezien de huidige regionaal georganiseerde autorisatie gelet op deze ontwikkeling te veel beperkingen met zich meebrengt. In ons model

(specifiek met de introductie van de autorisatieagent) beogen wij reeds op deze ontwikkeling te anticiperen en werken wij hieronder op conceptueel niveau een idee uit om de autorisatieprocedure verder te automatiseren door de inzet van een autorisatieagent en een TTP.

In het huidige systeem van elektronische informatie-uitwisseling kunnen uitsluitend politieambtenaren die daartoe door de verantwoordelijke zijn geautoriseerd inloggen in het systeem. Met betrekking tot de uitwisseling van criminele inlichtingen worden in de praktijk slechts politieambtenaren met een CIE-status geautoriseerd. Naast de autorisatie van politieambtenaren met een CIE-status voorzien wij evenwel dat op termijn hoe langer hoe meer behoefte zal bestaan aan elektronische uitwisseling van gegevens bij onder meer politieambtenaren met een recherchefunctie, buitenlandse politieambtenaren en ambtenaren die werkzaam zijn bij ketenpartners. Om de autorisatie tot de systemen en de elektronische uitwisseling van deze categorieën van gebruikers mogelijk te maken hebben wij de autorisatie en de TTP geïntroduceerd. In ons model ten aanzien van de toepassing van een autorisatieagent gaan wij ervan uit dat iedere gebruiker op het politiële netwerk zich toegang verschaft tot de centrale beheersindex via een transactieagent. De transactieagenten onderhandelen namens hun gebruikers met de poortwachteragenten van de clusters binnen de centrale beheersindex waarin de criminele inlichtingen liggen opgeslagen. Indien de poortwachter via de nationale autorisatie-index, waarin alle conform art. 6 lid 2 Wpolg geautoriseerde politieambtenaren geregistreerd staan, constateert dat er sprake is van een informatieverzoeker die niet conform art. 6 lid 2 Wpolg is geautoriseerd, dan wendt de poortwachteragent zich tot de autorisatieagent met het verzoek om na te gaan of de informatieverzoeker alsnog tijdelijk toegang zou moeten kunnen krijgen tot het cluster in de beheersindex. De autorisatieagent raadpleegt daartoe een TTP. In figuur 7.2 is een overzicht gegeven van de conceptuele uitwerking.



Figuur 7.2: Autorisatie informatieverzoeken.

De TTP moet door de autorisatieagent kunnen worden geraadpleegd om de regionaal 'onbekende' informatieverzoeker, dat wil zeggen de informatieverzoekers die niet voorkomen in de autorisatie-index, te verifiëren. Dit betekent nagaan of de informatieverzoeker voor het specifieke geval op

grond van de Wpolg en de Bpolg gerechtigd is om informatie verstrekt te krijgen. Binnen de TTP moeten alle mogelijke informatiegerechtigden, niet zijnde politieambtenaren, worden geregistreerd. De autorisatieagent kan door raadpleging van de TTP nagaan of de informatieverzoeker gerechtigd is tot het verkrijgen van informatie. Wanneer de autorisatieagent heeft vastgesteld dat er sprake is van een rechtmatige informatieverzoeker, dan vormt een tweede onderdeel van de autorisatieprocedure het vaststellen van het doel van het informatieverzoek. Daartoe communiceert de autorisatieagent rechtstreeks met de transactieagent. De autorisatieagent verifieert op basis van zijn kennis of de rechtmatige verzoeker ook de informatie wil raadplegen voor een legitiem doel. De legitieme doelen vormen een nadere specificering van de politietaak en de doelen die voortvloeien uit de taakuitvoering van derden. Bij deze laatste doelen moet worden gedacht aan de informatieverstrekking aan de IND in verband met het nemen van beslissingen omtrent de toelating, het verblijf of ongewenstverklaring van asielzoekers (art. 4:3 lid 1 sub g Bpolg). Wanneer de informatieverzoeker het doel van zijn informatieverzoek bekend heeft gemaakt aan de autorisatieagent, dan is het de taak van de autorisatieagent om te controleren of dit doel in overeenstemming is met de doeleinden uit de Wpolg. Wanneer dat het geval is zal het informatieverzoek in behandeling worden genomen en zal de poortwachteragent de informatieopdracht doorgeven aan de zoekagent.

In de conceptuele uitwerking in figuur 7.2 hebben wij de TTP beperkt tot de ketenpartners die zijn vastgelegd in art. 4:3 tot en met art. 4:6 Bpolr. Zoals bij de bespreking van het juridisch kader in hoofdstuk 3 reeds uiteen is gezet, is het niet de bedoeling van de wetgever geweest om het rechtstreeks geautomatiseerd verstrekken mogelijk te maken voor deze ketenpartners. In de Memorie van Toelichting staat bij de algemene verstrekkingsbepaling, art. 15 Wpolg, dat de oude Wpolr die met betrekking tot het verstrekken van informatie uit politieregisters steeds wettelijk voorschreef dat daarvoor menselijk handelen van de verantwoordelijke politieambtenaar nodig was. Ten opzichte van dit vereiste is er reeds in de Wpolg gekozen voor een nieuwe benadering die past in de lijn van de ontwikkelingen zoals wij die uiteen hebben gezet. In de Memorie van Toelichting overweegt de wetgever in dit verband het volgende.

> "De ontwikkelingen binnen de informatietechnologie maken het echter mogelijk politiegegevens op geautomatiseerde wijze te verstrekken, de overdracht van politiegegevens zonder menselijke tussenkomst zal dan eerder regel zijn dan uitzondering. Rekening houdend met de technische ontwikkelingen, en ook gelet op de ontwikkeling van de bovenregionale informatiehuishouding binnen de politie, kan de verantwoordelijke ervoor kiezen de politiegegevens rechtstreeks en geautomatiseerd beschikbaar te stellen aan ambtenaren van politie die vallen onder het beheer van een andere verantwoordelijke." [128]

128 Kamerstukken II 2005/06, 30 327, nr. 3, p. 68.

Uit deze toelichting op de art. 15 Wpolg blijkt duidelijk dat de wetgever met de invoering van de Wpolg beoogt te anticiperen op de toekomstige ICT-ontwikkelingen. Het systeem van autorisaties gaat er echter vanuit dat, nadat de autorisatieprocedure doorlopen is, de gebruiker vrije toegang heeft tot alle opgeslagen informatie. In het model dat wij voorstaan is dat echter niet de bedoeling maar worden de databases uitsluitend geraadpleegd naar aanleiding van concrete informatieverzoeken waarmee voorkomen wordt dat geautoriseerde gebruikers gaan rondneuzen in de systemen. Met het oog op het voorkomen van het doelloos rondneuzen van derden in de informatiesystemen heeft de wetgever in art. 23 Wpolg juncto art. 4:6 Wpolg de mogelijkheden tot het rechtstreeks geautomatiseerd verstrekken daarom beperkt tot:

(1) ambtenaren van de IND, en voor zover zij deze informatie nodig hebben voor de identificatie van personen;
(2) ambtenaren van het Ministerie van Buitenlandse Zaken voor zover zij deze informatie nodig hebben voor de uitvoering van opdrachten tot signalering van personen in het buitenland en het nemen van een beslissing omtrent de afgifte van een paspoort of omtrent de verlenging van een visum;
(3) personen die werkzaam zijn bij het MOT voor zover zij informatie nodig hebben voor de taakuitvoering (art. 3 Wet MOT);
(4) ambtenaren die werkzaam zijn bij de nationale politiële contactpunten voor de geautomatiseerde vergelijking van politiegegevens binnen de EU.

Buiten deze categorieën van personen kan dus op grond van de huidige wetgeving geen rechtstreekse geautomatiseerde verstrekking plaatsvinden. Ook toepassing van de door ons voorgestelde autorisatieagent en de TTP is daarom op grond van de Wpolg niet mogelijk. Wij menen echter dat de wetgever op termijn tevens rekening moet houden met autorisatiemethoden waarbij het na de autorisatie niet vanzelfsprekend is dat de geautoriseerde gebruiker vrijelijk toegang heeft tot de database. Wij voorzien dat deze technieken binnen de komende tien jaar voldoende zijn 'doorontwikkeld' om ingezet te kunnen worden in het domein van de gecontroleerde normatieve informatie-uitwisseling. Naast de uitwisseling met de nationale ketenpartners voorzien wij tevens dat een toenemende politiële samenwerking op Europees niveau uiteindelijk zal leiden dat ook Europese politieambtenaren op termijn langs deze weg toegang zullen krijgen tot de politiële informatiesystemen.

7.3.3 Informatietransacties

Zoals wij in de sectie 7.2 hebben voorgesteld wordt de informatie-uitwisseling in het door ons voorgestelde multi-agentsysteem vormgegeven door onderhandelingen tussen transactieagenten en poortwachteragenten. De

onderhandelingen ten aanzien van de informatietransacties vinden plaats in de centrale beheersindex en op het niveau van de daarin onderscheiden clusters. De onderhandelingen tussen de poortwachteragent en de transactieagent vormen een wezenlijk andere benadering van geautomatiseerde informatie-uitwisseling dat thans binnen de huidige systemen het geval is. Wij beogen met deze agenttoepassing een fundamenteel gedeelte uit het proces van informatie-uitwisseling met de inzet van beide softwareagenten verder te automatiseren met als doel de elektronische informatie-uitwisseling te verbeteren. Het model met de toepassing van beide agenten werkt als volgt.

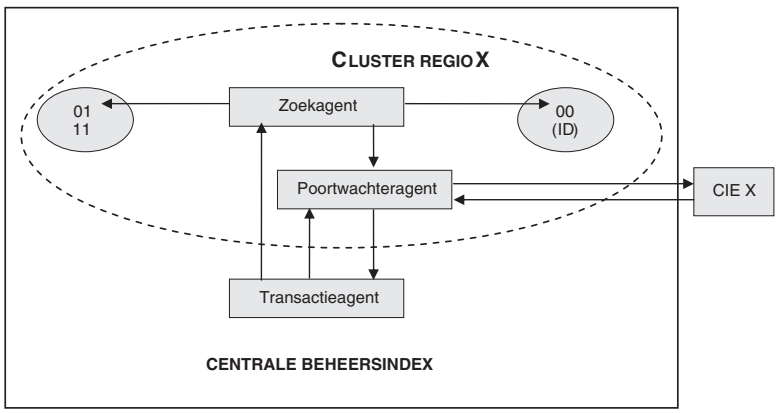
Nadat de transactieagent de autorisatieprocedure, zoals beschreven in de subsectie 7.3.2 heeft doorlopen, wordt de transactieagent toegelaten tot de centrale beheersindex. Daar communiceert de zoekagent met de transactieagent ten einde het informatieprobleem duidelijk in kaart te krijgen. De communicatie tussen deze beide agenten is erop gericht de zoekagent van zodanige informatie te voorzien dat deze gericht het betreffende cluster op relevante informatie kan doorzoeken. Daarbij wordt allereerst als uitgangspunt genomen dat de zoekvraag zoveel mogelijk dient te worden gepersonaliseerd zodat uitsluitend informatie ten aanzien van de voor de zoekvraag relevante persoon of personen wordt verstrekt. Voorts wordt nagegaan ten behoeve waarvan de informatie wordt gevraagd zodat ook op deze gronden een selectie kan worden gemaakt van de relevante informatie.

Wij geven een voorbeeld. Wanneer in een rechercheonderzoek op enig moment door verschillende getuigenverklaringen een mogelijke verdachte in beeld is gekomen, zal een arrestatieteam deze persoon willen arresteren. Het is dan in de voorbereiding voor deze arrestatie van belang om te weten of de betreffende persoon aangemerkt zou moeten worden als vuurwapengevaarlijk zodat het arrestatieteam daarop voorbereid is. In dat geval kan de zoekopdracht beperkt blijven tot de vraag of (1) verdachte X bekend is in de registers en zo ja, (2) of er informatie beschikbaar is met betrekking tot de vraag of X in het bezit is van een vuurwapen. Allerlei andere informatie over de drugshandel waarbij X betrokken is, en de criminele organisatie waaraan hij leiding geeft is ten aanzien van de specifieke zoekvraag niet relevant. Alle overige eventueel beschikbare informatie over X is in het licht van de specifieke zoekvraag niet relevant en zal daarom niet aan de transactieagent worden verstrekt. Daarmee wordt beoogd met de zoekagent te voorzien in een systeem van proportionele informatieverstrekking.

Het zoekresultaat wordt voorts eerst voorgelegd aan de poortwachteragent. Zoals bij de beschrijving van het agentmodel van de poortwachteragent aangegeven is hier ruimte voor regionale beleidskeuzes. Zo kan bijvoorbeeld een regio ervoor kiezen om ten aanzien van de 00-informatie een beleid te voeren dat 00-informatie wel verstrekt mag worden ter verificatie van 00-informatie van andere regio's. In dat geval worden slechts bij een positieve match van de betrokken *information designators* 00-informatie vrijgege-

ven om zodoende de informatie zoveel mogelijk af te schermen. Anderzijds kan de codering van de informatie met 00 inmiddels achterhaald zijn zodat er eerst een heroverweging van de betreffende codering dient plaats te vinden. In ons model stellen wij daarom voor dat, binnen de beleidsvrijheid die de regionale CIE ten aanzien van deze informatie-uitwisseling heeft, de poortwachteragent kan besluiten dat bijvoorbeeld eerst het verantwoordelijk hoofd van de CIE wordt geraadpleegd alvorens de informatie wordt verstrekt aan de transactieagent. Indien het hoofd CIE op basis van het zoekresultaat en het doel waarvoor de informatie wordt gevraagd concludeert dat er geen afbreukrisico's zijn, dan wel dat er een ander groter belang prevaleert, dan kan de poortwachteragent alsnog besluiten de informatie te weigeren.

Dijkstra (2007) heeft een transactieagent ontwikkeld waarbij het communicatieprotocol wordt geactiveerd zodra de poortwachteragent aangeeft dat de informatie wordt geweigerd. Het protocol van de transactieagent is erop gericht om door middel van een onderhandeling alsnog te trachten de informatie te bemachtigen. De onderhandeling ziet daarbij primair op het bereiken van overeenstemming over eventuele beperkende voorwaarden met betrekking tot het gebruik van de betreffende informatie. Indien informatie wordt gevraagd in het kader van een rechercheonderzoek, dan kan de beperkende voorwaarde eruit bestaan dat de informatie binnen een bepaalde termijn niet gebruikt mag worden voor operationele doeleinden. Tussentijds kan de informatie geverifieerd worden bij andere bronnen zodat de herleidbaarheid tot één informant kleiner wordt. Naarmate de herleidbaarheid groter is zal immers het afbreukrisico ook groter zijn en kan de informatie niet voor operationele doeleinden worden gebruikt.



Figuur 7.3: Informatietransactie.

Het idee van onderhandelingen ten aanzien van geautomatiseerde informatietransacties is geïnspireerd op de wijze waarop de niet geautomatiseerde informatie-uitwisseling thans plaatsvindt binnen de CIE-praktijk. Bij de

beschrijving van het juridisch kader hebben wij laten zien dat er een ruime beoordelingsmarge zit ten aanzien van de vraag of de verstrekking van informatie al dan niet zou moeten worden geweigerd. Wij menen dat het enkele hanteren van de afhandelingscodes daarvoor onvoldoende is. In het kader van ons veldwerk is door verschillende CIE-ers naar voren gebracht dat de verstrekking van 00-informatie veelal afhangt van de vraag waarvoor de informatieverzoeker de informatie nodig heeft en of zij het eens kunnen worden over de voorwaarden waaronder de informatie verstrekt wordt. Een voorwaarde kan bijvoorbeeld zijn dat deze informatie niet mag worden geregistreerd in het eigen register zware criminaliteit, of uitsluitend daarin geregistreerd mag worden indien de afspraak wordt gemaakt dat deze niet zal worden verstrekt aan enige derde dan nadat overleg is gevoerd met de eerste verstrekker. Door het stellen van dergelijke beperkende voorwaarden kan daardoor ook de controle op verstrekte 00-informatie behouden blijven, ook nadat deze is verstrekt.

Art. 15 Wpolg laat binnen deze grenzen de afweging over aan de regionaal verantwoordelijke. Door de toepassing Dijkstra's onderhandeling- en communicatieprotocollen kan er binnen het informatiesysteem nadere invulling worden gegeven aan de vereiste toetsing aan het beginsel van proportionaliteit zoals voortvloeit uit art 15 lid 2 Wpolg. De toepassing van de communicerende transactieagenten is daarmee ten eerste in het belang van de rechtshandhaving. Wij verwachten dat er op grotere schaal informatie kan worden uitgewisseld omdat het systeem de gebruiker als het ware dwingt per informatietransactie na te gaan of niet toch onder voorwaarden een verstrekking mogelijk is. In zijn algemeen geldt dat het in het belang van de uitvoering van de politietaak zal zijn om op grotere schaal toegang tot de waardevolle maar gevoelige criminele inlichtingen te krijgen. Met een systeem waarbinnen onderhandeling mogelijk is kan actief worden gezocht naar een balans. Dit betekent een vooruitgang ten opzichte van de uitsluitende ja/nee beslissing die thans binnen de elektronische uitwisseling gebruikelijk is. Met betrekking tot de rechtsbescherming menen wij dat de informationele privacy beter wordt gewaarborgd nu binnen het systeem beperkende voorwaarden kunnen worden overeengekomen met betrekking tot het gebruik en de registratie. Dat laatste punt is met name van belang omdat het binnen een multi-agentsysteem tevens mogelijk zal zijn om de naleving van de beperkende voorwaarden ten aanzien van de registratie of het doorverstrekken aan derden van de geleverde informatie beter te handhaven.

7.3.4 Surveillancetoepassing

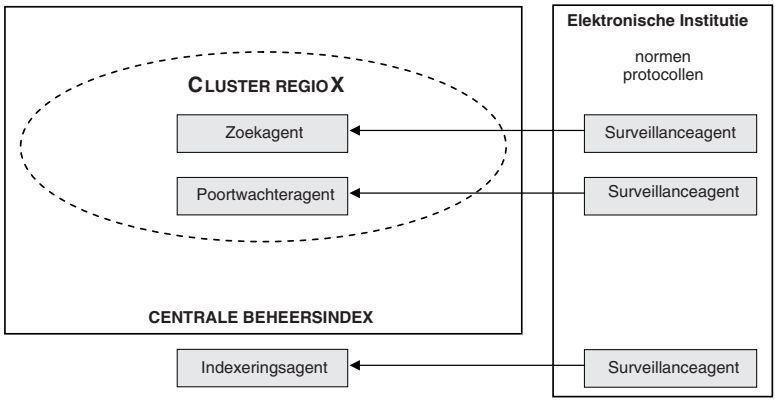
Aldewereld (2007) heeft binnen het ANITA-project een toepassing voorgesteld waarmee een balans wordt gezocht tussen de waarborging van de autonomie van de vrije agent enerzijds en de bevordering van diens conformiteit anderzijds. Deze balans zou bereikt kunnen worden door de toepas-

sing van een elektronische institutie waarin alle normen en protocollen van het deeldomein zijn vastgelegd. In ons model maken wij slechts op beperkte schaal van deze normatieve multi-agenttechniek van Aldewereld gebruik. Zoals wij in de sectie 7.2 uiteen hebben gezet introduceren wij een beperkt aantal 'vrije' agenten waarop het toezicht via surveillanceagenten en een elektronische institutie vormgegeven wordt, te weten de indexeringsagent en de zoekagent. Voor de overige softwareagenten kiezen wij voor vertegenwoordigers die vooraf zo geprogrammeerd dienen te worden dat zij in hun keuzemogelijkheden beperkt zijn en dat de keuzes die zij maken afhangen van de regels die op lokaal niveau worden toegepast. De softwareagenten die hun taak vervullen als vertegenwoordigers zijn dus langs deze weg beperkt in hun keuzevrijheid. Door de autonomie van de vertegenwoordigende softwareagenten te beperken beogen wij de integriteit en betrouwbaarheid van het multi-agentsysteem te vergroten en de kans op ongewenst emergent gedrag te verkleinen. Wij achten dit van belang omdat juist in het domein van de politiële informatie-uitwisseling, en met name bij de uitwisseling van criminele inlichtingen, de behoefte aan een integer en betrouwbaar systeem groot is.

Naast de *surveillance* op de vrije softwareagenten (indexeringsagent en zoekagent) zal de surveillanceagent in ons model ook toezicht houden op de poortwachteragenten. Zoals hiervoor aangegeven in subsectie 7.3.3 wordt aan de poortwachteragent een zekere mate van regionale autonomie gegeven. De regionale autonomie betekent dat er op regionaal niveau door de gebruiker regels kunnen worden gesteld voor de poortwachteragent met betrekking tot de uitwisseling. Deze regels zien bijvoorbeeld op de mate waarin op regionaal niveau wordt toegestaan om in bepaalde gevallen 00-informatie te verstrekken of de beperkende voorwaarden die worden gesteld aan de informatieverstrekkingen. Het toezicht van de surveillanceagenten is erop gericht om deze regionale autonomie en beleidskeuzen te toetsen aan het wettelijk kader (Aldewereld, 2007).

In figuur 7.4 is een conceptuele uitwerking weergegeven van de wijze waarop de surveillanceagenten een taak vervullen in het toezicht houden op de werking van de overige softwareagenten in het systeem. De surveillanceagenten vormen daarin een onderdeel van de elektronische institutie en controleren alle handelingen van de vrije agenten en de lokale regels van de poortwachteragent. Zodra blijkt dat een van de gecontroleerde softwareagenten de regels overtreedt, die zijn vastgelegd in de elektronische institutie, zal een negatieve feedback worden gegeven om het gedrag van de betreffende softwareagent te corrigeren.

Met betrekking tot de controle op de invulling van het regionale beleid van de poortwachteragent is art. 15 lid 2 Wpolg van belang. In deze bepaling is de wettelijke grondslag neergelegd voor de weigering om informatie te ver-



Figuur 7.4: Toepassing surveillanceagenten.

strekken. Zoals in hoofdstuk 3 uiteen is gezet heeft de wetgever een *free flow* van informatie als uitgangspunt genomen, zeker waar het gaat om de informatie-uitwisseling binnen de politieorganisatie. In bijzondere gevallen kan de regionale verantwoordelijke er evenwel voor kiezen om een informatieverstrekking desondanks te weigeren. Daarbij gaat het meestal om 00-informatie maar het is ook mogelijk dat juist door de combinatie van verschillende 11 en 01-informatie een afbreukrisico ontstaat doordat deze naar de bron leidt. Waar het bij het regionale beleid ten aanzien van de mogelijkheden om informatieverstrekkingen te weigeren om gaat, is de vraag of de weigering, of het beleid ten aanzien van de weigering ook rechtmatig is. In concreto zal daarom het regionale beleid van de poortwachteragent worden getoetst aan art. 2:13 Bpolg waarin limitatief de weigeringsgronden zijn bepaald. Deze weigeringsgronden zullen in ons model worden geïmplementeerd in de elektronische institutie. De surveillanceagent controleert of het regionale beleid binnen deze wettelijke grenzen blijft.

7.4 Verantwoording en discussie

De conceptuele voorbeelden van multi-agenttoepassingen in het domein van de informatie-uitwisseling doen allereerst de vraag rijzen welke toegevoegde waarde de inzet van deze technieken zou kunnen hebben in het politiedomein.

Rechtshandhaving
Binnen de huidige systemen worden nauwelijks privacywaarborgende technieken toegepast. De belangrijkste waarborg bestaat uit het toepassen van verschillende autorisatieniveaus. Naarmate een politieambtenaar een 'hoger' niveau van autorisatie krijgt toegekend heeft hij toegang tot meer gegevens die hij vrijelijk kan doorzoeken.

Ons inziens kleeft er vanuit het perspectief van de rechtshandhaving een bezwaar aan dit systeem aangezien aan de keuze voor autorisatieniveaus de veronderstelling ten grondslag ligt dat vooraf zou kunnen worden bepaald welke informatie de politieambtenaar nodig heeft voor de uitoefening van zijn taken. De aard van de uitoefening van de politietaak brengt echter met zich mee dat informatie die in concrete gevallen nodig is, zich op voorhand niet laat bepalen door autorisatieniveaus. Bovendien staat een systeem van autorisaties op gespannen voet met het beginsel dat de wetgever ten grondslag heeft gelegd aan de Wpolg, namelijk dat er binnen de politieorganisatie ter uitvoering van de politietaak in beginsel sprake dient te zijn van een *free flow* van informatie. Met onze conceptuele voorstellen voor de toepassing van een normatief multi-agentsysteem wordt een fundamenteel andere keuze gemaakt. Bepalend is immers niet het autorisatieniveau maar de (individuele) informatiebehoefte van de betrokken politieambtenaar.

Rechtsbescherming
Vanuit het perspectief van de rechtsbescherming geldt dat met de huidige systematiek van autorisaties na de inlogsessie, afhankelijk van zijn autorisatieniveau, toegang heeft tot alle informatie. De toepassing van softwareagenten draagt ten opzichte van deze mogelijkheden een belangrijke privacybeschermende werking in zich omdat een zoekagent aan de hand van concrete zoekopdrachten voor de gebruiker, de opgeslagen informatie doorzoekt. De privacywaarborg die daarin schuilt is dat niet-relevante politiegegevens niet worden ingezien. De zoekagent koppelt uitsluitend de relevante zoekresultaten terug naar de gebruiker. Bovendien wordt in de communicatie tussen de autorisatieagent, de poortwachteragent, en de transactieagent gecontroleerd of de verzoeker ook gerechtigd is kennis te nemen van de gevonden informatie en of de kennisneming rechtmatig is gelet op het doel waarvoor de informatie is opgevraagd.

Voorts beogen de zorgvuldig geprogrammeerde softwareagenten de uitwisselingsmogelijkheden binnen het informatiesysteem te reguleren. Doordat de keuzemogelijkheden die de softwareagenten binnen het politiële informatiesysteem hebben normatieve beperkingen kent, ontstaat een informatiesysteem waarbij de rechtmatigheid van de informatietransacties wordt afgedwongen. De normatieve beperkingen zijn in het belang van de privacy van de geregistreerde (onverdachte) burgers. Wij menen dat deze vorm van *regulating by architecture* een effectievere privacywaarborg is dan het huidige systeem van autorisatie, controle en toezicht (Lessig, 1996). Bovendien is de beperkte juridische kennis van gebruikers ten aanzien van de informatieverwerking in beginsel geen probleem meer omdat deze regels in het systeem zijn geïmplementeerd. Daarmee kan een multi-agentsysteem ons inziens bijdragen aan het oplossen van het knelpunt dat is geconstateerd ten aanzien van de onduidelijkheid van de regelgeving in het domein. Van belang is in dit verband dat regels slechts gedrag van mensen beïnvloeden indien de mensen ook gemotiveerd zijn om de regels na te leven (Greif, 2006 p. 36).

De verschillende evaluatieonderzoeken die besproken zijn in hoofdstuk 5 hebben laten zien dat politieambtenaren niet gemotiveerd zijn om de privacyregels in het domein na te leven. Deze regels worden als onduidelijk en daarom als lastig toe te passen ervaren. Bovendien ligt in de aard van de politietaak besloten dat bij de uitvoering daarvan het privacybelang een ondergeschikt belang is. De informationele privacy is meer een algemeen maatschappelijk belang dan een politieel belang. Politieambtenaren zijn daarom niet of nauwelijks gemotiveerd om met privacyregels rekening te houden bij de verwerking en uitwisseling van politiegegevens. Een adequaat waarborgingsmechanisme in de vorm van normatieve beperkingen in de architectuur van een multi-agentsysteem kan dat compenseren.

De legitimiteit van normatieve beperkingen
Ten aanzien van de keuze voor *regulating by architecture* rijst voorts de vraag wie uiteindelijk de normen in het systeem bepaalt. Weizenbaum (1976, p. 221) stelde dat de computerprogrammeur als enige verantwoordelijk is voor het digitale universum dat hijzelf creëert. Toepassing van dit uitgangspunt zou betekenen dat de programmeur van de softwareagenten en de bouwer van het informatiesysteem degenen zijn die bepalen welke normatieve beperkingen in het systeem zouden moeten gelden.

Zoals in sectie 7.2 uiteen is gezet hebben wij aansluiting gezocht bij de opvattingen van Franken (2004) en Dommering (2006) die normatieve softwarecodes primair beschouwen als een instrument om het recht te handhaven.

Dit uitgangpunt raakt de kern van het wetenschappelijk debat rondom de ontwikkeling en legitimiteit van nieuwe technologieën. Uitgaande van het technologisch determinisme zouden de multi-agenttechnieken zich min of meer autonoom ontwikkelen volgens bepaalde (economische) wetmatigheden. Dat leidt onvermijdelijk tot de situatie waarin niet de wetgever maar de ontwikkelaars bepalen welke normatieve beperkingen uiteindelijk in een systeem worden aangebracht. De stand van de techniek is daarbij bepalend voor de mogelijkheden. Tot op heden zien wij deze ontwikkeling in de politiële informatiehuishouding duidelijk terug waarbij de wetgever de technologische ontwikkelingen volgt. Kenmerkend daarvoor is het citaat uit de Memorie van Toelichting (subsectie 7.3.3) waarin de wetgever met zoveel woorden aangeeft dat ontwikkelingen op het gebied van de ICT vragen om aanpassing van de wet. Een ander kenmerkend voorbeeld in het politiedomein is het Blue View systeem. Door middel van indexering van alle regionaal opgeslagen informatie is het voor medewerkers van de infodesks mogelijk om tot op detailniveau de gegevens te bekijken. Blue View ontsluit zodoende (1) de basisregistraties en (2) de regionale tijdelijke registers op voorwaarde dat deze in RBS of Octopus worden beheerd. Het systeem Blue View was tot 1 januari 2008 in strijd met art. 13 van de Wpolr omdat voor tijdelijke registers het bijzonder verstrekkingenregime (zie hoofdstuk 3) van toepassing was. Dit verstrekkingenregime hield in dat uit een tijdelijk regis-

ter slechts gegevens mochten worden verstrekt voor het doel waarvoor het register is aangelegd, *tenzij* verstrekking plaatsvindt ten behoeve van de opneming in het register zware criminaliteit of een voorlopig register. Ondanks deze beperking is de politie vooruitlopend op de wetswijziging overgegaan tot de ontwikkeling van een softwareapplicatie die het technisch mogelijk maakt alle regionale tijdelijke registers te ontsluiten. Blue View is in 2007 in gebruik genomen en pas vanaf 1 januari 2008 is de nieuwe Wet Politiegegevens van kracht. De invoering van de Wpolg legaliseerde op die manier het Blue View systeem.

Wij menen echter dat niet de technische mogelijkheden bepalend zouden moeten zijn bij de ontwikkeling van politiële informatiesystemen. Wij pleiten in dat kader voor de inzet van softwarecodes als instrument om in casu de toepasselijke privacywetgeving te handhaven. Vanwege de omstandigheid dat de softwarecode dan gebruikt wordt als 'wet' in de *cyberspace* van de politiële informatiesystemen dienen de te implementeren normen zoveel mogelijk decmocratisch te worden gelegitimeerd. Een voldoende democratische legitimatie ontbreekt wat ons betreft in ieder geval wanneer de implementatie van normatieve beperkingen uitsluitend zou worden overgelaten aan de software-ontwikkelaars. Het initiatief tot het aanbrengen van normatieve beperkingen dient daarom niet overgelaten te worden aan de vrije markt die vooral eenzijdig is gericht op het zo goed mogelijk ondersteunen van de politietaak (rechtshandhaving). De rechtsbescherming dreigt daarbij uit het oog te worden verloren. Wij menen voorts dat het goed is om de toepassing van privacywaarborgende technieken in de politiële informatiesystemen te voorzien van een wettelijke basis. Gebeurt dat niet dan bestaat het risico dat door technologische ontwikkelingen het recht op privacy (te zeer) wordt uitgehold.

7.5 Beantwoording vierde onderzoeksvraag

In dit hoofdstuk stond de beantwoording van de vierde onderzoeksvraag centraal (OV 4). Deze vraag luidt als volgt:

Op welke wijze kunnen de multi-agenttechnieken bijdragen aan een verbetering van het proces van informatie-uitwisseling vanuit het perspectief van de rechtshandhaving en de rechtsbescherming?

Ter beantwoording van deze vraag hebben wij laten zien dat de toepassing van multi-agenttechnieken in het politiedomein de uitwisseling van politiegegevens op verschillende wijze toekomstbestendig zou kunnen maken.

Wij hebben gesteld dat informatie de komende decennia hoe langer hoe meer digitaal beschikbaar zal zijn. Daarmee groeit onvermijdelijk de behoefte aan elektronische uitwisseling van gegevens. Slimme inzet van zoekmechanismen maakt het mogelijk dat gerichter en succesvoller relevante informatieselecties kunnen worden gemaakt alvorens gegevens worden uitgewisseld. Multi-agentsystemen bieden ook op het gebied van de (elektronische) autorisaties goede mogelijkheden om te anticiperen op toekomstige ontwikkelingen waarbij op grotere schaal dan nu het geval is, gebruik zal worden gemaakt van een politieel intranet waarop zowel Europese politieambtenaren als (Europese) ketenpartners actief zijn. Een uitsluitend regionaal georganiseerd systeem van autorisaties zal niet langer kunnen volstaan en de toepassing van softwareagenten in het autorisatieproces biedt mogelijkheden tot flexibele oplossingen in het belang van de uitvoering van de politietaak.

Voorts hebben wij gesteld dat door de toepassing van de *information designator* de verticale uitwisseling met ketenpartners verder kan worden geautomatiseerd vanwege de omstandigheid dat het beheer en de controle over de informatie geheel bij de verantwoordelijke regio blijft, ook tijdens het zoekproces. Daarmee wordt voorkomen dat de verantwoordelijke van de informatie controle over 'zijn' informatie verliest. Juist in het domein van de criminele inlichtingen lijkt dat een goede oplossing omdat actualiteit en controle over de informatie van groot belang zijn.

De inzet van softwareagenten biedt verder een adequaat (rechts)waarborgingsmechanisme door de mogelijkheid van implementatie van juridische regels in de softwarecode. Gebruikers van de politiële informatiesystemen worden daardoor als het ware gedwongen om de relevante rechtsregels na te leven omdat het systeem hen geen andere mogelijkheden geeft. Op die manier wordt een technische oplossing gevonden voor het knelpunt dat de rechtsregels door de politieambtenaren als moeilijk toepasbaar en onduidelijk worden ervaren. Automatische toepassing van deze regels betekent immers dat de gebruikers deze regels niet noodzakelijkerwijs behoeven te begrijpen, terwijl zij wel worden toegepast.

Wij hebben verder betoogd dat privacy en technologische ontwikkelingen geen tegengestelde krachtenvelden behoeven te zijn. Technologie kan immers ook ingezet worden om de privacy beter te waarborgen terwijl het tegelijkertijd de belangen van de rechtshandhaving ten goede komt. Het gaat bij de toepassing van nieuwe technieken uiteindelijk om een balans tussen rechtshandhaving en rechtsbescherming. De laatste jaren hebben wij gezien dat onder druk van terroristische dreigingen meer het accent is komen te liggen op het verzamelen van gegevens waarbij het oude adagium 'meer is beter' weer lijkt te gelden. Daarom is het noodzakelijk om in een

informatiesysteem technieken in te zetten die politiële autoriteiten als het ware dwingen zorgvuldig daarmee om te gaan.

Tenslotte hebben wij gesteld dat de ontwikkeling van politiële informatiesystemen niet slechts kan worden overgelaten aan de politiële autoriteiten zelf. Dat leidt er onherroepelijk toe dat er een eenzijdige nadruk op het belang van de rechtshandhaving komt te liggen waardoor de rechtsbescherming van geregistreerde (onverdachte) burgers te zeer onder druk komt te staan. Juist daarom zou bij de ontwikkeling van informatiesystemen een partij betrokken moeten zien die onafhankelijk toezicht houdt op de ontwikkeling. Te denken valt aan het Cbp.

8 Conclusies en aanbevelingen

Dit hoofdstuk beoogt aan de hand van de vier onderzoeksvragen een antwoord te formuleren op de probleemstelling die centraal staat in dit onderzoek. De probleemstelling luidde als volgt.

In hoeverre kan de inzet van softwareagenten en normatieve multi-agenttechnieken bijdragen aan de verbetering en de regulering van elektronische uitwisseling van politiegegevens?

Wij beginnen de beantwoording van deze probleemstelling door allereerst in sectie 8.1 de eerste onderzoeksvraag (OV 1) te beantwoorden. Daarmee werd beoogd inzicht te verkrijgen in de (theoretische) mogelijkheden van softwareagenten en multi-agenttechnieken. Voorts beantwoorden wij in sectie 8.2 de tweede onderzoeksvraag (OV 2) naar de wijze waarop de uitwisseling van criminele inlichtingen door de wetgever is genormeerd. In sectie 8.3 wordt antwoord gegeven op de derde onderzoeksvraag (OV 3) waarmee is beoogd na te gaan hoe de uitwisseling van criminele inlichtingen is ingericht en wat daarin de knelpunten zijn. Sectie 8.4 geeft antwoord op de vierde onderzoekvraag (OV 4) naar de wijze waarop softwareagenten en multi-agenttechnieken kunnen worden ingezet in het proces van elektronische gegevensuitwisseling in het CIE-domein. Na aldus in sectie 8.1 tot en met 8.4 de vruchten van ons onderzoek te hebben beschreven gaan wij in sectie 8.5 na of dit alles ertoe heeft bijgedragen dat de centrale probleemstelling is beantwoord, of dat er althans een vruchtbare aanzet daartoe is gegeven. In sectie 8.6 doen wij enkele aanbevelingen aan de wetgever, politie en justitie, en het Cbp. Wij ronden in sectie 8.7 af met een slotbeschouwing.

8.1 Softwareagenten en multi-agenttechnieken

Onze eerste onderzoeksvraag luidde als volgt.

Wat zijn de (theoretische) mogelijkheden van softwareagenten en multi-agenttechnieken?

In hoofdstuk 2 hebben we de mogelijkheden van multi-agenttechnieken in kaart gebracht door enkele algemene trends binnen de artificiële intelligentie te beschrijven. In aansluiting daarop hebben we de toekomstverwachtingen van een vooraanstaand informaticus (Kurzweil, 2005) onderzocht over de richting waarin de artificiële intelligentie zich volgens hem zal ontwikkelen.

Voorts zijn wij aan de hand van de drie voornaamste eigenschappen van softwareagenten de theoretische mogelijkheden nagegaan, en hebben wij de mogelijkheden van normatieve multi-agent systemen onderzocht.

De algemene trends binnen de AI laten zien hoe deze wetenschap zich heeft ontwikkeld en waar intelligente (software) systemen reeds toe in staat zijn. Op basis van de voorspellingen van Kurzweil komen wij tot de conclusie dat het bereiken van het door hem onderscheiden *singularity point* naar verwachting vergaande consequenties zal hebben voor de wijze waarop in de toekomst zal worden omgegaan met informatiesystemen in het algemeen, en met informatiesystemen voor de politie in het bijzonder. Kurzweil stelt dat op enig moment in de nabije toekomst computers 'intelligenter' worden dan mensen en uiteindelijk in staat zullen zijn om 'betere' beslissingen te nemen. Voor het politiedomein zal dit betekenen dat geautomatiseerde gegevensverwerking en informatietransacties volledig kunnen worden uitgevoerd door softwareagenten.

Wij menen dat serieus rekening zal moeten worden gehouden met de voorspelling van Kurzweil (2005) dat het *singularity point* in deze eeuw zal worden bereikt. Deze voorspelling roept nieuwe (juridische) vraagstukken op ten aanzien van de verantwoordelijkheid, de controle van emergent gedrag, de rol van de individuele politieambtenaar, en de positie van geregistreerde burgers. Schmidt (2009) wijst in dat verband op de mogelijke gevolgen die het *singularity point* kan hebben voor de houdbaarheid van ons rechtssysteem. Hij wijst erop dat Kurzweil er in zijn optimistische voorspellingen volledig aan voorbij gaat dat het huidige rechtssysteem volstrekt onvoldoende is geëquipeerd om rechtsvragen te beantwoorden die deze nieuwe technologische omgeving met zich zal meebrengen. Dat is met name aan de orde als het gaat om de toepassing van artificiële technieken die niet langer door de mens kunnen worden begrepen. Hoewel Schmidt sceptisch tegenover de voorspellingen van Kurzweil staat en deze voorspellingen zelfs kwalificeert als romantische fantasieën in plaats van wetenschappelijk verantwoorde inzichten, erkent hij wel dat de artificiële technologieën zich in toenemende mate sneller ontwikkelen. Interessant is zijn suggestie dat deze technologische vooruitgang volgens hem zal leiden tot een ander *singularity point*, namelijk dat ieder individu binnen een samenleving in staat zal blijken te zijn tot massadestructie. Die individuele capaciteit vraagt volgens hem wereldwijd om een rechtssysteem waarin een allesomvattende surveillancesysteem en proactieve rechtshandhaving noodzakelijk zullen zijn. De technologische ontwikkelingen dragen volgens Schmidt dan ook het gevaar in zich dat zij ons huidige rechtssysteem destabiliseren en dat de voor het rechtssysteem noodzakelijke legitimiteit onder druk komt te staan.

Voor het politiedomein zullen deze ontwikkelingen onherroepelijk leiden tot een nog verdere proactivering van de opsporing en de rechtshandhaving. Politie en justitie zullen de komende decennia hoe langer hoe meer

in staat worden gesteld om op steeds grotere schaal persoonsgegevens over onverdachte burgers te verzamelen en bruikbaar en zinvol te verwerken. De technologische ontwikkelingen zullen het bovendien mogelijk maken dat computers op termijn eerder verbanden en verdenkingen signaleren en construeren dan de mens.

Voorts is uit het literatuuronderzoek naar de eigenschappen van softwareagenten gebleken dat er, vanuit een juridisch perspectief, binnen de AI geen eenduidigheid bestaat over de precieze definiëring van de mogelijkheden. Voor informatici ligt dat per specialisme verschillend. Niettemin bemoeilijkte deze uitkomst ons bij de beantwoording van de eerste onderzoeksvraag. Het is immers niet altijd duidelijk waarover we het precies hebben als gesproken wordt over softwareagenten en MAS-technieken. Wij zijn echter wel tot de conclusie gekomen dat de onderzochte eigenschappen van softwareagenten te weten: autonomie, reactief en adaptief gedrag, en communicatie, veelbelovende mogelijkheden lijken te bieden voor toepassing in het domein van de informatietransacties in zijn algemeenheid en de uitwisseling van politiegegevens in het bijzonder. Daarbij zien wij niet alleen mogelijkheden om de elektronische uitwisseling van gegevens te verbeteren vanuit het perspectief van de rechtshandhaving (opsporing en vervolging van strafbare feiten) maar juist ook vanuit het perspectief van de rechtsbescherming. Wij denken met name aan het zodanig programmeren van softwareagenten dat in de informatiesystemen normatieve beperkingen worden ingebouwd, zodat privacyregels automatisch worden gehandhaafd, of een zodanige *incentive* geven aan de gebruiker dat deze zijn gedrag daarop afstemt.

Ten slotte zijn wij voor de beantwoording van de eerste onderzoeksvraag nagegaan wat de mogelijkheden van normatieve multi-agentsystemen zijn. In dat verband hebben wij gesteld dat bij de toepassing van de MAS-techniek in het politiedomein het emergent gedrag vrijwel zeker als onwenselijk zal worden beschouwd. Met name in het CIE-domein wordt het controleren van informatiestromen zeer belangrijk gevonden en emergent gedrag binnen informatiesystemen leidt er onvermijdelijk toe dat de verantwoordelijke CIE-ambtenaren gedeeltelijk controle verliezen over hetgeen er gebeurt met 'hun' informatie.

Wij hebben daarnaast ook de onderzoeksresultaten beschreven van het AI-onderzoek dat in het kader van het ANITA-project is verricht. Binnen het project zijn met het oog op het politiedomein drie AI-toepassingen ontwikkeld die in de toekomst ingezet zouden kunnen worden om de elektronische informatie-uitwisseling, zowel vanuit het perspectief van de rechtshandhaving als vanuit het perspectief van de rechtsbescherming te verbeteren.

8.2 Juridisch kader

Onze tweede onderzoeksvraag luidde als volgt.

Op welke wijze is de huidige uitwisseling van criminele inlichtingen ingericht en wat zijn daarin de (juridische) knelpunten?

De Nederlandse wetgever was en is bij de wijze van normering van de verwerking en uitwisseling van politiegegevens niet volledig vrij maar is gebonden aan internationale rechtsbeginselen die zijn vastgelegd in onder meer het EVRM en het Europees Dataverdrag. In deze verdragen kunnen vijf leidende rechtsbeginselen worden onderscheiden die het uitgangspunt vormen voor de normering van de verwerking en uitwisseling van politiegegevens op nationaal niveau.

Het eerste rechtsbeginsel is de *rechtmatigheid*. In de Wpolg wordt dit tot uitdrukking gebracht door de regel dat uitsluitend politiegegevens mogen worden verwerkt die rechtmatig zijn verkregen. Wij hebben in ons onderzoek vastgesteld dat in het huidige systeem van rechtsbescherming ten aanzien van deze rechtmatigheid niet effectief kan worden genoemd omdat toetsing ten aanzien van de rechtmatigheid van de verwerkte of verstrekte gegevens per definitie achteraf plaatsvindt. Wij hebben betoogd dat in het licht van de technologische ontwikkelingen deze reactieve vorm van rechtsbescherming op termijn ons inziens onvoldoende de privacy van de geregistreerde onverdachte burgers zal waarborgen, te meer daar dan de waarborgings- en controle mechanismen tekortschieten.

Het tweede beginsel is de *doelbinding*. In de Wpolg dient de (rechtmatige) verwerking van politiegegevens altijd plaats te vinden met het oog op een vooraf vastgesteld doel. De gegevens mogen slechts worden verzameld, opgeslagen, en verwerkt voor zover deze handelingen noodzakelijk zijn voor dat doel. In de Wpolg zijn met het oog daarop vijf doelstellingen vastgelegd waaraan weer bepaalde bevoegdheden met betrekking tot de gegevensverwerking gekoppeld zijn. Het doel waarvoor de CIE gegevens mag verzamelen en uitwisselen is het verkrijgen van inzicht in personen en organisaties die zich bezighouden met bepaalde categorieën van ernstige misdrijven. Dit betekent in beginsel dat de CIE geen gegevens kan verzamelen, verwerken en uitwisselen buiten dit doel. Wordt dit binnen de CIE toch gedaan dan is er sprake van een onrechtmatige gegevensverwerking. De inbreuk die de verwerking en uitwisseling van gegevens maakt op het grondrecht van de informationele privacy wordt gelegitimeerd door de ernst van de strafbare feiten waarop de gegevensverwerking betrekking heeft. Het betekent omgekeerd dat deze legitimatie er niet is wanneer desondanks over andere onderwerpen gegevens worden verzameld en verwerkt. Die informatieverwerking dient dan ook als onrechtmatig te worden aangemerkt.

Het derde beginsel is de *proportionaliteit*. Dit beginsel stelt normatieve eisen aan de informatie-uitwisseling in het CIE-domein. De toepassing van het beginsel brengt mee dat bij iedere gegevensverstrekking zou moeten worden nagegaan of de verstrekking van de politiegegevens in een redelijke verhouding staat tot het doel dat daarmee beoogd wordt. Meer concreet betekent dit dat er niet meer gegevens mogen worden verstrekt dan strikt noodzakelijk is voor het doel waarvoor de gegevens gevraagd worden. Het verstrekken van overbodige gegevens is in dat licht derhalve onrechtmatig en mag vanwege de onderliggende privacybescherming niet worden verstrekt.

Het vierde beginsel is de *subsidiariteit* en houdt in dat gegevens pas mogen worden verwerkt en uitgewisseld indien er geen minder ingrijpend middel voor handen is waarmee hetzelfde resultaat zou kunnen worden bereikt. In de politiepraktijk wordt de gegevensverwerking en uitwisseling algemeen aangemerkt als een weinig ingrijpend opsporingsmiddel. De betrokken burgers ervaren, zo is de gedachte, geen rechtstreekse inbreuk op hun privéleven. Waar het echter bij de toepassing bij dit beginsel eveneens om gaat is dat het een rol speelt bij de schaal waarop gegevens worden verwerkt. Daarbij geldt als algemeen uitgangspunt dat naarmate op een grotere schaal gegevens worden verwerkt, terwijl net zoveel inzicht verkregen kan worden in de criminele organisatie door op kleinere schaal gegevens te verwerken, de grootschalige gegevensverwerking mogelijk in strijd is met het subsidiariteitsbeginsel.

Het vijfde beginsel is de *transparantie.* Het houdt in dat degene die de persoonsgegevens verwerkt hierover op verzoek van de betrokkene de nodige informatie zal moeten verstrekken. In het CIE-domein speelt dit beginsel een geringe rol omdat in de praktijk vrijwel altijd inzage in de gegevens geweigerd of beperkt zal worden in het belang van de uitvoering van de politietaak (zie daarover: Kielman, 2009). Een tweede aspect van het transparantiebeginsel is het uitgangspunt dat achteraf de gegevensverwerking en uitwisseling controleerbaar dient te zijn. Om die reden dient aantekening te worden gehouden van de gegevensverstrekkingen.

De vijf rechtsbeginselen vormen het juridische kader waarbinnen de normatieve beperkingen voor politie-informatiesystemen moeten worden ontwikkeld. De wetgever heeft deze beginselen voor een deel nader uitgewerkt in de wetgeving maar daarbij rechtsconcepten als 'rechtmatigheid' en 'noodzakelijk' niet nader ingevuld. Het stelsel van rechtsbescherming is thans zo ingericht dat de controle op deze beginselen een voornamelijk reactief karakter heeft. Wij hebben in sectie 8.1 gewezen op de toenemende snelheid waarmee de AI en ICT-technieken zich ontwikkelen. Kort samengevat worden computers intelligenter en kunnen deze steeds beter beslissingen overnemen van de mens. Internationale ontwikkelingen op het gebied van de grens-

overschrijdende politiële samenwerking laten zien dat ook in de nabije toekomst hoe langer hoe meer rechtstreeks en geautomatiseerd op internationaal niveau politiegegevens zullen worden verwerkt en uitgewisseld. Deze ontwikkelingen vormen in toenemende mate een bedreiging voor de privacy van burgers en daarom kan ons inziens niet meer worden volstaan met een voornamelijk reactief systeem van rechtsbescherming. Op grond daarvan pleiten wij ervoor dat, gelet op het doel van de privacybescherming, er meer aandacht zal worden besteed aan de proactivering van de rechtsbescherming. Het gaat daarbij wat ons betreft om een geautomatiseerde proactieve controle binnen de informatiesystemen. Een geautomatiseerde controle is noodzakelijk omdat door de groeiende omvang en schaal van politiële gegevensverwerking de bestaande toezicht- en controlemechanismen tekortschieten en bovendien de mens in de nabije toekomst eenvoudigweg niet meer in staat zal zijn om grote dataverzamelingen te controleren. Een mens kan nu eenmaal niet de verwerking van grote hoeveelheden persoonsgegevens controleren. Een geautomatiseerde controle betekent dan een vele malen effectievere waarborging van de privacy.

8.3 Organisatie en knelpunten

Onze derde onderzoeksvraag luidde als volgt.

Op welke wijze is de huidige uitwisseling van criminele inlichtingen ingericht en wat zijn daarin de (juridische) knelpunten?

Voor de inventarisatie van de knelpunten hebben wij vijf (evaluatie)onderzoeken besproken die vanaf het midden van de jaren negentig zijn gedaan naar de uitwisseling van politiegegevens. Daarnaast hebben wij veldwerk verricht waaruit een aantal nieuwe knelpunten naar voren zijn gekomen. Kennelijk is men er vanaf het midden van de jaren negentig niet of nauwelijks in geslaagd om een adequate oplossing voor deze problematiek te vinden. Dit leidde tot de conclusie dat de elektronische uitwisseling van politiegegevens vijf terugkerende en daarmee hardnekkige knelpunten kent. Om die reden hebben wij deze de *hoofd*knelpunten in de elektronische informatie-uitwisseling aangeduid.

1. *Moeilijk toegankelijke juridische kennis:* Complexe wet- en regelgeving voor de verwerking van politiegegevens bemoeilijkt de naleving daarvan door politieambtenaren bij onder meer de uitwisseling.
2. *Ontoereikende gegevenscontrole*: Het gaat dan om onvoldoende controle op de juistheid, tijdigheid, en volledigheid van de gegevens waardoor de kwaliteit van de opgeslagen gegevens te wensen over laat.
3. *Onvoldoende standaardisatie:* Diversiteit van de informatiesystemen en onvoldoende standaardisatie belemmeren de interne uitwisseling van gegevens en de externe uitwisseling met ketenpartners.

4. *Gesloten bedrijfscultuur:* Onvoldoende vertrouwen van politieambtenaren in elkaar heeft geleid tot een gesloten politiecultuur waarin het delen van informatie alles behalve vanzelfsprekend is.
5. *Ontoereikende privacywaarborgen:* De onafhankelijke controle- en toezichtmechanismen via de privacyfunctionaris en het Cbp schieten in de dagelijkse praktijk tekort waardoor er binnen de CIE nauwelijks prikkels zijn om privacyregels na te leven.

Wij hebben voorts gesignaleerd dat in samenhang met de in hoofdstuk 4 beschreven ontwikkeling van de informatie- en registratiesystemen binnen de CIE, ook steeds hogere eisen gesteld worden aan de informatie-uitwisseling. Dit hangt sterk samen met de in hoofdstuk 2 beschreven technologische ontwikkelingen. Wij constateerden dat naarmate de technische mogelijkheden toenemen, ook de maatschappelijke eisen die worden gesteld aan de politieorganisatie in evenredigheid toenemen. Van de politiesystemen wordt verwacht dat zij mee ontwikkelen met de technische mogelijkheden en aan de systemen worden daarom steeds hogere eisen gesteld. Dit laat zien dat ook binnen de politieorganisatie sprake is van een technologie-gedreven ontwikkeling. De mogelijkheden tot geautomatiseerde verwerking en uitwisseling gaan steeds sneller. Het gevolg daarvan is dat ook de politie op steeds grotere schaal van deze technologieën gebruik zal gaan maken waardoor in de nabije toekomst, en daar gaat het ons om, het recht op privacy te zeer in het gedrang komt. In het technologiedebat (sectie 1.5) hebben wij ons aan de zijde van de technologisch deterministen geschaard hetgeen betekent dat wij er vanuit gaan dat de techniek zich (onder meer) ontwikkelt volgens het autonome principe dat efficiëntie altijd gaat voor moraliteit. Wij hebben in dat verband betoogd dat het daarom van groot belang is dat er nieuwe methoden worden onderzocht die het recht op privacy effectiever waarborgen. Bij de technologische ontwikkelingen in het politiedomein mag daarom niet eenzijdig de aandacht worden gericht op het belang van de rechtshandhaving (efficiëntie). Wij menen dat meer aandacht zou moeten worden besteed aan de inzet van techniek in het belang van de rechtsbescherming (moraliteit).

Om na te gaan waar in het proces van informatie-uitwisseling aanknopingspunten gezocht zouden kunnen worden voor het aanbrengen van normatieve beperkingen in het proces van gegevensuitwisseling hebben wij met behulp van de CommonKads-methode de wijze geanalyseerd waarop de huidige informatie-uitwisseling binnen de CIE is ingericht. In deze organisatieanalyse hebben wij laten zien dat het huidige bedrijfsproces met betrekking tot de informatie-uitwisseling binnen de CIE kan worden opgesplitst in zes deeltaken. Geen van deze deeltaken is thans geautomatiseerd. Zo bezien is er in beginsel voldoende ruimte voor automatiseringstoepassingen. Aangezien evenwel het doel van ons onderzoek is gelegen in de vraag waar in dit proces van informatie-uitwisseling normatieve beperkingen zouden kunnen worden ingebouwd hebben wij voorts de analyse toegespitst op het

nader ontleden van de zes deeltaken en de kennis die nodig is voor de uitvoering van deze deeltaken.

Deze analyse heeft tot het inzicht geleid dat tenminste drie deeltaken (controle ontvangstgerechtigde, vaststellen informatiedoel, beoordelen afbreukrisico's) in het genoemde domein verhoudingsgewijs kennisintensief zijn. De drie deeltaken hebben wij vervolgens aan de hand van drie taakmodellen nader geanalyseerd waarbij wij tot de conclusie komen dat deze aanknopingspunten bieden voor (gedeeltelijke) normatieve automatisering en daarmee het verbeteren van de elektronische informatie-uitwisseling. Dat is ons inziens om twee redenen nodig.

Ten eerste is dat van belang voor de *rechtshandhaving*. Normatieve softwareagenten kunnen een meerwaarde vormen voor de informatie-uitwisseling waarbij onder meer de standaardisatieproblemen in gedistribueerde informatiesystemen kunnen worden overbrugd. De inzet van softwareagenten kan het mogelijk maken dat volledige standaardisatie niet langer een vereiste is voor de elektronische uitwisseling van gegevens met de ketenpartners. Bovendien kan door de inzet van softwareagenten het arbeidsintensieve handmatige proces van informatie-uitwisseling (gedeeltelijk) worden geautomatiseerd waardoor de door de wetgever gewenste *free flow* van informatie beter tot stand komt. Een ander voordeel voor de uitvoering van de politietaak is dat normatieve beperkingen in de geautomatiseerde informatie-uitwisseling er toe kan leiden dat meer gewerkt wordt volgens het *need-to-know*-principe waardoor een *information overload* kan worden voorkomen.

Ten tweede is verbetering van belang voor de *rechtsbescherming*. De privacy van geregistreerden binnen de informatiesystemen kan beter en effectiever worden gewaarborgd door middel van technische voorzieningen. Daarbij moet worden gedacht aan geautomatiseerde toepassing van wettelijke bepalingen (technologische regulering) en het instellen van (geautomatiseerd) toezicht op de registraties. Daarnaast kan de inzet van slimme ICT de transparantie van de gegevensregistratie verbeteren. In de taakmodellen hebben wij voorstellen gedaan waar ons inziens in het proces van informatie-uitwisseling zich deze mogelijkheden voordoen en waar ons inziens de mogelijkheden aanwezig zijn om softwareagenten in te zetten die juridische regels kunnen toepassen om de rechtmatigheid van de uitwisseling beter te waarborgen dan nu het geval is.

8.4 Conceptuele toepassing softwareagenten

Onze vierde onderzoeksvraag luidde als volgt.

Op welke wijze kunnen de multi-agenttechnieken bijdragen aan een verbetering van het proces van informatie-uitwisseling vanuit het perspectief van de rechtshandhaving en de rechtsbescherming?

In de conceptuele analyse hebben wij laten zien dat een MAS bij de uitvoering van de verschillende deeltaken goede mogelijkheden biedt om de uitwisseling van gegevens te ondersteunen. Wij hebben laten zien dat met behulp van autorisatieagenten kan worden geanticipeerd op toekomstige technologische ontwikkelingen die met name gericht zijn op schaalvergroting van de opslag, verwerking, en uitwisseling van politiegegevens. Wij voorzien een ontwikkeling waarin in de nabije toekomst in toenemende mate een koppeling zal plaatsvinden van politiële informatiesystemen waardoor een 'Europees politieel intranet' ontstaat. In het licht van deze ontwikkeling zal een regionaal georganiseerd systeem van autorisaties niet langer kunnen volstaan en ontstaat behoefte aan een flexibel autorisatiesysteem.

Daarnaast hebben wij meerwaarde van de toepassing van de door Teepe (2006) ontwikkelde *information designator* onderzocht. Toepassing van deze technologie biedt ons inziens goede mogelijkheden om de verticale elektronische uitwisseling mogelijk te maken. De grote meerwaarde van de toepassing van deze techniek is namelijk dat ondanks de schaalvergroting waarop de uitwisseling plaatsvindt, het beheer van de opgeslagen informatie regionaal georganiseerd blijft. Daarmee kan worden voorkomen dat de eigenaar van de informatie de controle over zijn informatie verliest. Juist in het domein van de criminele inlichtingen is dat een veelbelovende oplossing.

De inzet van softwareagenten biedt voorts een adequaat reguleringsmechanisme dat voorziet in de waarborging van de privacywetgeving. De juridische regels worden geïmplementeerd in de softwarecode waardoor het systeem normatieve beperkingen kent. Gebruikers van de politiële informatiesystemen worden door het systeem gedwongen tot rechtmatige gegevensuitwisseling. Op die manier draagt de techniek tevens bij aan een oplossing voor het knelpunt van de moeilijk toegankelijke rechtsregels. Automatische toepassing van deze regels betekent immers dat de gebruikers deze regels niet noodzakelijkerwijs hoeven te begrijpen, terwijl zij wel worden toegepast.

Kortom, wij zien in de toepassing van MAS-technieken mogelijkheden om privacybescherming en technologische ontwikkelingen hand in hand te laten gaan. Technologie kan juist ingezet worden om de privacy beter te waarborgen, terwijl het tegelijkertijd de belangen van de rechtshandhaving ten goede komt. Het gaat bij de toepassing van deze nieuwe technieken om een balans tussen rechtshandhaving en rechtsbescherming.

8.5 Beantwoording probleemstelling

Nu vast staat dat er goede mogelijkheden zijn om de informatie-uitwisseling door de inzet en toepassing van MAS-technieken te verbeteren en adequaat te reguleren dringt de vraag zich op of normatieve beperkingen in de politiele informatiesystemen op termijn wel noodzakelijk zijn. Wij menen in het licht van de steeds sneller gaande technologische ontwikkelingen dat dit het geval is en lichten dat als volgt toe. In subsectie 8.5.1 zetten wij allereerst uiteen op welke wijze het recht op privacy samenhangt met de politiële gegevensverwerking en waarom effectieve (technische) privacywaarborgen ons inziens noodzakelijk zijn. Vervolgens zetten wij in subsectie 8.5.2 de juridische achtergrond van technische regulering uiteen en ronden wij in subsectie 8.5.3 af met enkele discussiepunten ten aanzien van het antwoord op de probleemstelling.

8.5.1 Rechtsbescherming

Wij zijn in hoofdstuk 1 van ons proefschrift begonnen met het schetsen van enkele maatschappelijke ontwikkelingen rondom veiligheid, informatieverwerking, en privacy. Vanuit deze ontwikkelingen constateerden we dat vooral technologische vernieuwingen, in samenhang met nieuwe veiligheidsrisico's, zorgen voor veranderingen en verschuivingen in de grenzen tussen de privésfeer en het publieke domein (zie o.a.: Muller, 2005). Deze veranderingen blijken onder meer uit de grote stroom aan wetsvoorstellen en wetswijzigingen sinds de aanslagen op 11 september 2001 die in het belang van de veiligheid zijn gedaan. Vrijwel alle wetsvoorstellen noemen het vergroten van de veiligheid van de Nederlandse samenleving als belangrijkste noodzaak voor de betreffende wijziging. Het gevolg van deze wetgeving is echter dat de rechtsbescherming en de grondrechten van de burgers het vaak moeten ontgelden (Vedder e.a., 2007). Met name privacybelangen worden opgeofferd aan de veiligheid van veelal potentiële slachtoffers van criminaliteit of terrorisme (Prakken, 2003, De Hert en Gutwirth, 2005).

Naar aanleiding van maatschappelijke beeldvorming die daardoor is ontstaan, namelijk dat privacy en veiligheid elkaar uitsluitende waarden zouden zijn, hebben het Cbp, het Ministerie van BZK en het Ministerie van Justitie onderzoek laten doen naar de balans tussen veiligheid en privacy (Muller, Kummeling en Bron, 2007). De onderzoekers komen tot genuanceerde inzichten en stellen dat privacy en veiligheid niet beschouwd moeten worden als elkaar uitsluitende waarden. Beide waarden zijn noodzakelijk voor de waarborging van de democratische rechtsstaat. Dat de waarden zorgen voor een spanningsveld betekent volgens hen dat voordurend afwegingen gemaakt moeten worden waarbij als uitgangspunt geldt dat het in een democratische rechtsstaat uiteindelijk gaat om het zo optimaal mogelijk garanderen van de individuele vrijheid.

In het maatschappelijk debat rondom de balans tussen veiligheid en privacy hebben De Hert en Gurtwirth (2005) eerder de vraag opgeworpen wat nu de toekomst van de burgerrechten en vrijheden van de open samenleving zou mogen zijn in het licht van de grote zorg voor publieke veiligheid. Wat is met andere woorden nog het belang van privacybescherming? Het belang privacybescherming wordt breed onder ogen gezien wanneer het gaat om evidente inbreuken op de persoonlijke levenssfeer. Aanzienlijk lastiger wordt deze discussie echter op het moment dat het 'slechts' gaat over de privacybescherming in verband met de verwerking van persoonsgegevens. Helemaal moeilijk blijkt de discussie wanneer het gaat om de verwerking van deze gegevens door de politie. De verwerking dient immers het belang van de rechtshandhaving en de democratische rechtsorde. Een veel gehoorde stelling in dat verband is dat wie niets te verbergen heeft ook niets hoeft te vrezen van de politie. Uitgaande van deze redenering zou voor politiële autoriteiten uiteindelijk kunnen gelden dat zij onbeperkt persoonsgegevens mogen verzamelen aangezien de onschuldige burger daarvan toch niets hoeft te vrezen.

Het is ons inziens een groot misverstand te veronderstellen dat onschuldige en onverdachte burgers niets te verbergen of te vrezen zouden hebben. Onze stelling is dat, juist nu de overheid zich in toenemende mate bedient van nieuwe elektronische instrumenten voor de rechtshandhaving, het recht op privacy een grotere maatschappelijke betekenis toekomt (zie ook: De Hert en Koops, 2001). Het recht op privacy vormt een van de belangrijste waarden om de balans te behouden in het streven naar (maakbare) veiligheid en om een noodzakelijk tegenwicht te bieden aan een (te) machtige staat in verhouding tot de vrije individuele burger.

De vraag blijft echter wat nu precies het belang van privacybescherming is wanneer het gaat om de verwerking en uitwisseling van politiegegevens, zeker wanneer je als onverdachte burger op geen enkele wijze betrokken bent bij criminaliteit. Om deze principiële vraag te kunnen beantwoorden moet het recht op informationele privacy ons inziens bezien worden in samenhang met de vrijheid en de autonomie van burgers. Daarvoor grijpen wij terug op de koppeling tussen de individuele vrijheid en het recht op privacy dat reeds aan het einde van de negentiende eeuw werd gemaakt door de Amerikaanse rechters Warren en Bandeis (1890). Zij verklaarden het recht op privacy in de zin van het '*right to be let alone*' tot een authentiek liberaal vrijheidsrecht.

Met betrekking tot de relatie vrijheid en informationele privacy is op het eerste gezicht niet duidelijk wat het onderlinge verband is. Gesteld kan immers worden dat wanneer de politie persoonsgegevens (digitaal) verzamelt en verwerkt, zij daarmee de geregistreerde burgers in beginsel op geen enkele wijze belemmert of beperkt in hun vrijheid. Waarom zou het uitwisselen en verwerken van politiële informatie de vrijheid van individuele burgers in

gevaar kunnen brengen zolang dat niet gepaard gaat met enigerlei feitelijke beperkingen van die vrijheid, en de betrokkene bovendien van dat observeren niet eens op de hoogte is en er misschien ook nooit zal komen?

De Leidse filosofe Rössler (2008) geeft ten aanzien van deze vraag ons inziens een zeer verhelderend voorbeeld uit een roman van Barth (1958) waarin de hoofdpersoon Joe Morgan zich tegenover zijn omgeving graag doet voorkomen als een zeer beheerst en intellectueel mens. In zijn huis waant deze Morgan zich geheel alleen en onbespied maar in plaats van stil en rustig studeren, zoals je van een intellectueel zou verwachten, speelt hij thuis dat hij een legercommandant is en marcheert hij bevelen gevend door zijn huiskamer. De vriendin van Morgan staat hem op dat moment heimelijk te bespieden en is onhutst door het onverwachte gedrag van haar vriend. Vanaf dat moment is de relatie en interactie met zijn vriendin verstoord. Duidelijk is dat Morgan zich zeker anders had gedragen indien hij geweten had dat hij werd bespied. Rössler (2008) gebruikt dit voorbeeld om daarmee duidelijk te maken dat de individuele vrijheid, in de zin van controle over de presentatie van onszelf en over onze authenticiteit, kan worden verstoord door heimelijke observatie. Privacybescherming is in dat licht voor burgers van groot belang. Het vormt een belangrijke voorwaarde bij het vrij en ongecontroleerd kunnen bepalen hoe je jezelf presenteert (vgl. Buruma, 2008).

Wanneer een individuele burger weet dat hij geobserveerd wordt gaat hij zich anders gedragen of zich in ieder geval bewegen vanuit het besef dat hij geobserveerd wordt. Van Gusteren (2004) duidt dit als zelfdisciplinerend gedrag en stelt dat juist dergelijk zelfdisciplinerend gedrag een zeer fundamentele schending oplevert van de individuele vrijheid van burgers. De veelgehoorde stelling dat onschuldige burgers niets te vrezen hebben van de verzameling en verwerking van politiegegevens is daarom eenvoudigweg onjuist. De informationele privacy beschermt de vrijheid en het authentieke en autonome handelen van (onverdachte) burgers. Rössler waarschuwt ervoor dat wanneer burgers niet meer kunnen vertrouwen op de vanzelfsprekende bescherming van informatie, dit niet alleen de individuele vrijheid van burgers schaadt maar tegelijkertijd ook het functioneren van het maatschappelijk leven en van de democratische instellingen. Vrijheid en zelfbeschikking zijn immers elementaire voorwaarden voor het functioneren van een vrije democratische samenleving die is gebaseerd op het vermogen van burgers om autonoom te handelen.

Wanneer dus van staatswege burgers als subjecten worden beschouwd die verdacht zijn of verdacht kunnen worden dan leidt dit volgens Rössler uiteindelijk tot de legitimatie van een fundamentele asymetrie tussen staat als observeerder en de burgers als geobserveerden. Deze asymmetrie kan leiden tot de uitholling en het verval van het rechtsstatelijke vermoeden van onschuld. Het ideaal van een veilige samenleving gaat er immers vanuit dat alle burgers in principe gevaarlijk zijn of gevaarlijk kunnen zijn. Doordat dit

uitgangspunt het wezenlijke rechtstatelijke element van het vermoeden van onschuld op losse schroeven zet, zal ook het vertrouwen in de democratische instituties afnemen. Met de toename van technologische mogelijkheden zal daarnaast ook het gevaar van misbruik toenemen.

Schmidt (2009) wijst er in dat verband op dat de consequenties van technologische ontwikkelingen (zoals voorspeld door Kurzweil) voor de samenleving nauwelijks nog zijn te overzien en rechtsvragen meebrengt waarop ons rechtssysteem geen antwoord heeft (Klink, Prins en Witteveen, 2000). Ten aanzien van de verzameling en verwerking van politiegegevens is dan de vraag in hoeverre het idee van de individuele controle over informatie eigenlijk nog wel zin heeft. Burgers hebben immers geen idee meer welke informatie over hen ligt opgeslagen, wordt verwerkt, en met wie de informatie wordt uitgewisseld alsmede waar en wanneer *data mining* en *profiling* worden toegepast.

Wij menen om die reden dat privacy veel effectiever en adequater dient te worden beschermd dat nu het geval is. Dat is niet alleen noodzakelijk met het oog op de waarborging van de individuele vrijheid en autonomie van de burger maar ook voor de waarborging van de democratische rechtsstaat als geheel. Het gaat dan over de houdbaarheid van ons rechtssysteem dat immers valt en staat met de coöperatie van burgers en het vertrouwen in de integriteit van de rechtstatelijke instituties. Om deze integriteit te waarborgen is het ons inziens van groot belang dat de technologische innovaties in de systemen van de politie niet uitsluitend gericht zijn op de rechtshandhaving maar dat juist ook het belang van de rechtsbescherming onder ogen wordt gezien. Om die reden achten wij het noodzakelijk dat in de toekomst meer aandacht wordt besteed aan het implementeren van normatieve beperkingen in informatie- en registratiesystemen van de politie.

8.5.2 Technologische regulering

Wij hebben in hoofdstuk 7 laten zien dat er in het proces van informatie-uitwisseling binnen de CIE goede mogelijkheden en aanknopingspunten zijn om door middel van softwareagenten privacywaarborgende normen te implementeren. Daarnaast kunnen concrete gedragsregels worden geprogrammeerd die als resultaat hebben dat het gedrag van personen met behulp van deze technische instrumenten geheel dan wel gedeeltelijk wordt beïnvloed of beheerst. Het grote voordeel van deze wijze van regulering is dat de technologie de gebruiker van de informatiesystemen tot een bepaald soort handelen verplicht waarmee de onderscheiden juridische modaliteiten in de agentmodellen (rechten, plichten en bevoegdheden) rechtstreeks worden geëffectueerd. Dit betekent dat sprake is van een proactieve rechtsbescherming en niet, zoals met veel traditionele juridische instrumenten het geval is, van een reactieve rechtsbescherming. Wat wel en wat niet mag wordt in

het normatieve MAS voorgeprogrammeerd. Het normconforme gedrag wordt daarmee door het systeem afgedwongen.

Het idee van regulering door middel van ICT-technieken is niet nieuw. Lessig (1996 en 1999) introduceerde de gedachte dat hardware en software op een effectieve manier gedrag kunnen reguleren. De softwarecode bepaalt wat het apparaat wel en niet kan, en reguleert daarmee (in)direct ook het gedrag van de gebruiker. Dit verband tussen de software en de menselijke handelingen heeft Lessig gebracht tot zijn stelling '*code is law*'. In de rechtswetenschappelijke literatuur is veel discussie over de vraag of de softwarecode wel zou moeten worden aangemerkt als 'recht' (zie daarover o.a.: Asscher, Dommering, 2006). Wat daar ook van zij, wij stellen dat de programmeerbare softwareagenten en MAS-technieken een veelbelovende reguleringsmodaliteit kan zijn in het politiedomein, aangezien het kan zorgen voor een automatische en onmiddellijke handhaving van privacyregels. De impliciete en expliciete regels die zijn vastgelegd in de softwareagenten verrichten hun reguleren de werking zonder menselijke tussenkomst doordat zij de handelingen van de gebruiker toelaten of juist blokkeren.

In ons onderzoek hebben wij op hoofdlijnen laten zien dat de deeltaken in het proces van gegevensuitwisseling kunnen worden ondersteund door softwareagenten. De vraag is dan of de gebruikte softwarecode daarmee gekwalificeerd moet worden als 'recht'? Wij menen dat op deze vraag vooralsnog geen eenduidig antwoord mogelijk is voor het politiedomein, maar dat de vraag in beginsel wel ontkennend zou moeten worden beantwoord. Het ontkennende antwoord heeft te maken met de omstandigheid dat softwareagenten en MAS-technieken slechts het gedrag van politieambtenaren met betrekking tot de verwerking van politiegegevens reguleren waarbij uitgegaan wordt van de wettelijke normen. Daarmee is de softwarecode in beginsel niet zelf de norm maar wordt een bestaande wettelijke norm geïmplementeerd in het systeem. De softwarecode heeft daarmee een fundamenteel andere status dan de juridische norm. De werkelijkheid is echter weerbarstiger aangezien de Wpolg en de Bpolg niet geschreven zijn om te worden geïmplementeerd in softwarecodes. Er is met andere woorden een vertaalslag nodig. Binnen het ANITA-project heeft Aldewereld (2007) een methode geïntroduceerd om deze kloof tussen de abstracte algemene normen uit de wet te overbruggen door de wet te vertalen naar heel concrete protocollen en patronen die geïmplementeerd kunnen worden een MAS. Wij constateren echter dat in deze vertaalslag keuzen worden gemaakt ten aanzien van de interpretatie van de wet, welke keuzen vervolgens worden vastgelegd in de software. Hoewel wordt beoogd om de wettelijke normen te implementeren kan dat niet anders dan nadat deze abstracte normen zijn vertaald naar implementeerbare normen (zie ook: Hildebrandt en Koops, 2007). Bij deze vertaling worden opnieuw normatieve keuzen (interpretaties van de wettelijke normen) gemaakt.

Onze conclusie dat regulering vanwege het grote belang van de bescherming van de informationele privacy in het politiedomein, meer dan nu het geval is, zou moeten worden geïntroduceerd, stelt ons vervolgens voor de vraag naar de legitimiteit van softwaretechnologie als reguleringsinstrument. Dat geldt te meer nu voor de implementatie van de normen een vertaalslag nodig is die op zijn beurt 'nieuwe' normen creëert waarop de technologische regulering feitelijk ziet. Hoewel binnen de rechtswetenschap geen eenduidige opvatting bestaat over wat precies bedoeld wordt met legitimiteit kan in zijn algemeenheid wel worden gesteld dat legitimiteit bestaat uit formele voorwaarden die aan de uitoefening van staatsmacht worden gesteld en tevens uit een bepaalde mate van coherentie tussen de waarden van deze staatsmacht en de waarden van de gemeenschap waarover de macht wordt uitgeoefend (zie onder meer: Clark, 2003, Steffek, 2003). Wanneer wij dit legitimiteitsconcept meer concreet toespitsten op het recht op bescherming van de privacy als gemeenschappelijke waarde, dan signaleren wij dat door de uitholling van dit grondrecht een onevenwichtigheid kan ontstaan tussen opvattingen van de overheid en de burgers ten aanzien van het recht op privacy. Wij menen dat de inzet van technologische reguleringsinstrumenten een rol kan spelen bij het bewaren van een juist evenwicht. Van groot belang is echter wie bij de vertaling van de wettelijke normen daadwerkelijk de keuzen maakt met betrekking tot de te implementeren norm. In het privaatrechtelijke domein zien wij dat dergelijke keuzen niet noodzakelijkerwijs door publiekrechtelijke autoriteiten worden gemaakt maar in feitelijk door de software-ontwikkelaar. Wij menen dat dit in het politiedomein niet aan de ICT-ontwikkelaars zou moeten worden overgelaten maar dat ten aanzien van deze keuzen moet worden voorzien in een democratisch systeem van *checks and balances* om aan deze vorm van regulering ook de gewenste legitimiteit te verschaffen. Meer concreet stellen wij voor dat dergelijke keuzen gemaakt worden door het domein zelf, te weten politie en justitie in nauw overleg met het Cbp. Om de informationele privacy daarbij een effectieve mede normbepalende waarde van belang te laten zijn dienen ons inziens vertaalde normen, voordat deze worden geïmplementeerd, te worden goedgekeurd door het Cbp.

De inzet van technologische regulering met het oog op de bescherming van de privacy in het politiedomein sluit ons inziens goed aan bij de uitgangspunten zoals die zijn opgenomen in de Nota bruikbare rechtsorde uit 2004[129] en het in 2005 verschenen advies van de Sociaal Economische Raad (SER) ten aanzien van dit onderwerp. Daarin wordt gesteld dat de wetgever bij het maken van wetten en regels niet uitsluitend het belang van de overheid zelf als uitgangspunt moet nemen voor haar besluitvorming maar meer zou moeten werken vanuit de idee dat de belanghebbende burgers hun belangen ook daadwerkelijk tot recht moeten kunnen laten komen.

129 *Kamerstukken II* 2003/04, 29 279, nr. 9 en nr. 14.

Dat geldt te meer als het gaat om kwetsbare belangen (SER, 2005). Juist dat laatste is van belang wanneer het gaat om de bescherming van de informationele privacy. Burgers weten door de toegenomen technologische mogelijkheden niet wat er met hun gegevens gebeurt en bovendien wordt in de samenleving op grote schaal de potentiële schade voor de democratische rechtsorde onderschat. De inzet van het technologisch reguleringssystemen kan daarmee de dreigende onbalans met betrekking tot de waarborging van privacyrechten herstellen.

8.5.3 Discussie

De regulering door middel van softwareagenten en MAS-technieken roept een veelheid aan (rechts)vragen op die variëren van de gewenste kenbaarheid van de implicaties van het reguleringsinstrument tot meer fundamentele vragen rondom de mate waarin politieambtenaren zelf een zekere handelingsvrijheid behouden ten aanzien van de geregistreerde informatie.

Allereerst rijst de vraag in hoeverre de normatieve MAS-systemen nu werkelijk in staat zijn om de noodzakelijke flexibiliteit te bieden om de finesses van het normensysteem van de Wpolg te incorporeren. Implementatie van open normen in softwaresystemen zal, zoals hiervoor aangegeven, onvermijdelijk betekenen dat er keuzen gemaakt moeten worden met betrekking tot de invulling van deze normen. De wetgever heeft bovendien gekozen om een zekere beoordelingsvrijheid te laten aan de politieambtenaren. Dit betekent ook dat op regionaal niveau concrete beleidskeuzen gemaakt moeten kunnen worden met betrekking tot de toepassing van de wettelijke normen. Vanuit dat licht bezien zou kunnen worden betoogd dat de vertaling van de wettelijke normen uitsluitend zou moeten worden overgelaten aan het politiedomein zelf.

Wij achten het echter van belang dat een onafhankelijke toezichthouder, het Cbp, rechtstreeks de regionale beleidskeuzen en de te programmeren normen moet kunnen toetsen aan het wettelijk kader alvorens deze normen worden geïmplementeerd. Pas dan ontstaat immers een systeem waarin het tekortschietende toezicht door het Cbp op de naleving van privacyregels op een effectieve wijze wordt hersteld. Wij menen dan ook dat zowel de betrokken politieregio's, het openbaar ministerie als het Cbp een rol moeten hebben bij het vertalen en implementeren van de wettelijke normen. Wanneer de implementatie uitsluitend aan het politiedomein zou worden overgelaten zou de nadruk te veel komen te liggen op het belang van de rechtshandhaving.

In het verlengde daarvan rijzen vragen naar de mate waarin het normatief kader uit de Wpolg houdbaar is met het oog op de door ons geschetste toekomstige ICT-ontwikkelingen. Bieden de open normen en de ruime beoor-

delingsvrijheid voor politieambtenaren wel voldoende tegenwicht tegen de zich steeds verder en sneller ontwikkelende ICT-mogelijkheden en kan de wet een adequate bescherming van de privacy blijven waarborgen? Volstaat daarnaast het wettelijk kader nog wel wanneer steeds meer functies en taken in het proces van gegevensverwerking en uitwisseling worden overgelaten aan softwareagenten?

Wij hebben in hoofdstuk 7 aan de hand van een conceptuele analyse laten zien dat het huidige autorisatiesysteem in de Wpolg nieuwe vragen oproept met het oog op de ontwikkeling in de richting van een Europees politieel intranet waarop alle Europese politiegegevens in beginsel beschikbaar zijn en uitgewisseld moeten kunnen worden. De huidige nationale autorisatieregels volstaan op zo'n netwerk niet meer. De wetgever zal moeten nadenken over nieuwe mechanismen. Kortom, wij menen dat technologische ontwikkelingen op termijn opnieuw zullen vragen om verandering van het positieve recht teneinde de innovatie binnen het politiedomein op een kwalitatief en vanuit het privacyperspectief, verantwoord niveau te kunnen accommoderen en bij te sturen.

Meer in zijn algemeenheid rijst naar aanleiding van ons betoog de principiele vraag aan welke criteria de technologische regulering zelf zou moeten voldoen. In de rechtswetenschappelijke literatuur lopen de inzichten daarover uiteen. Lessig (1999) stelt dat wanneer de softwarecode kan worden aangemerkt als recht, de totstandkoming daarvan zal moeten voldoen aan vergelijkbare (democratische) waarborgen als waarmee 'normale' wetten tot stand komen. Het gaat dan o.a. om de waarborging van constitutionele rechten door te voorzien in een zorgvuldige procedure ten aanzien van de totstandkoming van normen in de softwarecode. Daarover moet evenwel worden opgemerkt dat Lessig primair doelt op 'nieuwe' normen die toegepast worden in de cyberspace van Internet, zonder dat deze normatieve beperkingen rechtstreeks zijn terug te voeren op wetten die reeds *offline* gelden.

Reidenberg (1998, en 2004) stelt dat voor de toepassing van technologische normering als handhavingsinstrument, dit zal moeten voldoen aan de voorwaarde dat een wettelijk gelegitimeerde autoriteit slechts tot technologische regulering mag overgaan en de toepassing daarvan moet voldoen aan de eis van proportionaliteit. Daarnaast noemt Reidenberg (2007) democratische legitimering, en de *rule of law* als de belangrijkste voorwaarden waaraan moet worden voldaan. Asscher (2006) heeft in dat verband een lijst met criteria ontwikkeld om de (juridische) kwaliteit en daarmee de legitimiteit van technologische regulering te beoordelen. Hij stelt dat (1) de normatieve regels in de softwarecode begrijpelijk moeten zijn voor de normadressant (transparantie), (2) dat de softwarecode moeten kunnen worden vertrouwd, (3) dat een legitieme autoriteit de regels moet vaststellen en (4) dat de softwarecode de keuzevrijheid niet onnodig beperkt. Brownword (2004) had eerder al gesteld dat technologische regulering rechtmatig en effectief dient

te zijn. Koops (2007) heeft naar aanleiding van deze verschillende inzichten een aanzet gegeven aan een model waarin systematisch de criteria zijn omschreven waaraan technologische regulering zou moeten voldoen om voldoende maatschappelijke legitimatie en acceptatie te krijgen. Het door Koops voorgestelde model vormt in feite een verdere verfijning van de reeds door Franken (1992) onderscheiden zes beginselen van behoorlijk IT-gebruik.[130]

Kortom, de technologische ontwikkelingen stellen de wetgever, politie, justitie en het Cbp de komende jaren voor een groot aantal fundamentele (rechts) vragen. Daarnaast rijst een scala aan technische vragen met betrekking tot de toepassing en beveiliging van de politiële informatiesystemen. In ons onderzoek beschrijven wij slechts de richting waarin de AI-technieken zich in de komende decennia zullen gaan ontwikkelen. Dat geeft ook (enig) inzicht in de wijze waarop in de toekomst politiële informatiesystemen ingezet zullen gaan worden. Naarmate de technische mogelijkheden toenemen en naarmate de schaal waarop ICT wordt toegepast groter wordt zal het ons inziens steeds noodzakelijker worden om effectievere waarborgingsmechanismen voor de (informationele) privacy in te zetten. Nader juridisch en AI-onderzoek naar de nieuwe vragen die dit meebrengt achten wij dan ook zeer nodig omdat voorkomen moet worden dat de democratische rechtsstaat geruisloos transformeert naar een 'gevaarlijk' veilige politiestaat waarin de autonome individuele vrijheid en zelfbeschikking van burgers heeft plaats gemaakt voor een vergaande vorm van zelfdisciplinerend gedrag.

8.6 Aanbevelingen

In deze sectie doen wij op basis van ons onderzoek en onze conclusies enkele concrete aanbevelingen aan de wetgever (subsectie 8.6.1), aan politie en justitie (subsectie 8.6.2) en aan de onafhankelijke toezichthouder, het Cbp (subsectie 8.6.3).

8.6.1 Aan de wetgever

Wij hebben betoogd dat de techniek zich in belangrijke mate ontwikkelt volgens twee regels: (1) efficiëntie gaat voor moraliteit en (2) technologie zoekt uiteindelijk een zo breed mogelijk werkingsgebied. Voor de politieorganisatie zijn nog twee wetmatigheden van toepassing, namelijk: (1) hoe meer

130 De zes beginselen zijn toegankelijkheid, vertouwelijkheid, integriteit, authenticiteit, flexibiliteit en transparantie. Deze beginselen zullen volgens Franken uiteindelijk de criteria bepalen waaraan de producten van informatietechnologie en de wijze waarop deze producten worden gehanteerd, in een democratische en sociale rechtsstaat zullen moeten voldoen.

meer gegevens worden verzameld, des te beter dat is voor de uitvoering van de politietaak en (2) *profiling* en *datamining* zijn erop gericht om uit zeer grote gegevensverzamelingen voor de opsporing nuttige informatie te construeren. Dergelijke technieken zullen in de komende jaren aan effectiviteit toenemen (zie o.a.: VanderLooy, 2009).

Daarnaast is er een duidelijke trend waarneembaar naar een verdere proactivering van de opsporing waarbij de informatiepositie van de politie van cruciaal belang is (zie ook: Cleiren, 2004). Privacybescherming speelt in die ontwikkeling nauwelijks een rol van betekenis, want ook de wetgeving blijkt in belangrijke mate technologie-gedreven. Een duidelijk voorbeeld daarvan is de Wpolg die de nog maar een paar jaar oude gewijzigde Wpolr verving vanwege onder meer nieuwe technische mogelijkheden. Het lijkt erop dat daarmee niet meer de grondwettelijke norm de maat is voor het juridisch kader maar de nieuwe technische mogelijkheden. Dit blijkt duidelijk uit de Memorie van Toelichting waarin de wetgever verwijzend naar de nieuwe technische mogelijkheden aangeeft dat zij met de Wpolg een nieuw evenwicht beoogt tot stand te brengen tussen de uitvoering van de politietaak aan de ene kant en de privacybescherming aan de andere kant. Het gebruik van de term evenwicht is hier echter misleidend. Het is volstrekt *onduidelijk* wat daarmee wordt bedoeld. Betekent dit bijvoorbeeld dat wanneer zich weer nieuwe technologische technieken aandienen er wederom een nieuw evenwicht gevonden zal moeten worden waarbij de wet opnieuw de inzet van nieuwe technieken verder legitimeert? Omdat privacybescherming bij de technologische ontwikkeling geen zelfstandige innovatieve prikkel heeft zal die prikkel naar ons oordeel kunstmatig gegeven moeten worden. Op dat punt zien wij een rol voor de wetgever weggelegd.

Wij bevelen aan om een zelfstandige wettelijke grondslag op te nemen in de Wpolg waarin een verplichting wordt vastgelegd dat bij het vernieuwen van de politiële informatiesystemen tevens, naar de alsdan geldende stand van de techniek, nieuwe technologische reguleringsinstrumenten moeten worden geïmplementeerd. Het Cbp als onafhankelijk toezichthouders zou vooraf een adviserende rol moeten krijgen bij de ontwikkeling van nieuwe systemen. Om het toezicht verder te effectueren achten wij het van belang dat het Cbp een goedkeuringsbesluit dient te nemen ten aanzien van het technisch ontwerp. Tegen dit goedkeuringsbesluit moet vervolgens beroep bij de bestuursrechter openstaan zodat een minimaal systeem van *checks and balances* ontstaat ten aanzien van technologische ontwikkelingen in het politiedomein.

Het evenwicht tussen nieuwe technische mogelijkheden, veiligheid, en privacy waar de wetgever in de Memorie van Toelichting bij de Wpolg op doelt moet worden gevonden binnen het grondwettelijk en verdragsrechtelijke kader. Ter waarborging van het recht op privacy is in art. 10 lid 2 Grondwet bepaald dat de wet regels stelt ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens.

Wij werpen in het licht van het voorgaande de vraag op of dit grondrecht in zijn huidige vorm nog wel voldoende waarborgende werking heeft en niet wordt ingehaald door de tijd en de techniek. Is in dat licht de houdbaarheidsdatum van art. 10 Grondwet niet verstreken? Wij menen dat dit binnen afzienbare tijd het geval zal kunnen zijn en dat het grondwettelijk kader nieuwe randvoorwaarden dient te scheppen voor technologische ontwikkelingen, met name waar het gaat om de politiële informatiesystemen.

Wij bevelen dan ook aan om een uitbreiding van het fundamentele recht op privacy op te nemen in de grondwet inhoudende dat naast het recht op kennisneming en verbetering van persoonsgegevens, ook het recht van de burgers op betrouwbare en integere overheidsinformatiesystemen wordt vastgelegd. Juist voor politiële informatiesystemen is dit van belang aangezien het recht op inzage en verbetering in de praktijk veelal niet mogelijk is vanwege de afscherming van de gevens in het belang van de uitvoering van de politietaak.

8.6.2 Aan Politie en Justitie

Het openbaar ministerie en de politie zijn belast met de strafrechtelijke handhaving van de openbare orde en de rechtsorde. Er is bij deze taakuitvoering een spanningsveld tussen de handhaving van de rechtsorde en het beschermen van de privacy. Illustratief voor dit spanningsveld is de opmerking van de Amsterdamse hoofdcommissaris Welten die het recht op privacy de schuilplaats van het kwaad noemde.[131] Privacyregels kunnen de uitvoering van de politietaak hinderen en het bevreemdt daarom niet dat de politie bij de ontwikkeling van haar eigen registratie- en informatiesystemen en bij de ontwikkeling van uiteenlopende analysesoftware niet of nauwelijks aandacht besteedt aan de implementatie en vertaling van privacyregels in de systemen. De ontwikkeling en inrichting van de systemen is vooral gericht op efficiëntie en doelmatigheid. Desondanks menen wij dat een te eenzijdige nadruk op de uitvoering van de politietaak op de lange termijn afbreuk zal doen aan het noodzakelijke vertrouwen van burgers in de integriteit van de politie- en justitieorganisatie.

Wij bevelen daarom aan dat in de scholing van politieambtenaren meer aandacht wordt besteed aan de privacywetgeving en met name wordt ingegaan op de rechtsstatelijke noodzaak van het effectief waarborgen van het recht op privacy. Meer kennis en een groter privacybewustzijn kan in belangrijke mate bijdragen aan het behouden van het noodzakelijke vertrouwen in de politiële autoriteiten dat op een integere wijze wordt omgegaan met de geregistreerde gegevens.

131 Bernard Welten deed deze uitspraak in de Volkskrant van 21 november 2003.

Wij bevelen voorts aan dat de politie bij de ontwikkeling van informatiesystemen niet langer eenzijdig en uitsluitend de nadruk leggen op de ontwikkeling van specificaties die eerst en vooral de politietaak ondersteunen. Bij het ontwerpen van nieuwe systemen moeten hogere eisen worden gesteld aan het ontwerp en de implementatie van normatieve (privacy)beperkingen. Naar ons oordeel blijft dan beter de balans bewaard tussen de voor de democratische rechtsorde noodzakelijke waarden met betrekking tot het recht op privacy enerzijds, en de noodzakelijke uitoefening van politiële bevoegdheden in het belang van de veiligheid anderzijds.

8.6.3 Aan het Cbp

Wij hebben geconstateerd dat het onafhankelijk toezicht op de verwerking van politiegegevens door het Cbp tekortschiet. Dat is voornamelijk een capaciteitsprobleem dat voortvloeit uit een te beperkt budget. Het Cbp zou echter ook in het politiedomein, meer kunnen aandringen op de toepassing van Privacy Enhancing Technologies en daarover het maatschappelijk debat aanzwengelen.

Wij bevelen aan dat het Cbp als onafhankelijke nationale privacywaakhond, meer dan nu het geval is, daarin het voortouw neemt. Daarnaast achten wij het van belang dat het Cbp ook een nadrukkelijkere rol opeist bij de ontwikkeling van politiële informatiesystemen. In de technische ontwerpen van de systemen zitten immers de 'grootste' privacybedreigingen en tegelijkertijd de meeste kansen voor effectieve controle. Het Cbp moet daarom beginnen met het ontwikkelen van een duidelijke visie op technologische reguleringsinstrumenten in het politiedomein en vervolgens haar beleid daarop afstemmen. Ons inziens liggen daar de mogelijkheden tot het effectief verbeteren van de controle en het toezicht op de politiële gegevensverwerking.

8.7 Slotbeschouwing

Dit proefschrift vormt de neerslag van een deelonderzoek binnen het ANITA-project naar mogelijkheden om de uitwisseling van gegevens in het politiedomein te ondersteunen en te verbeteren met behulp van multi-agenttechnieken. De verwachting die aan dit project ten grondslag lag was dat de inzet van deze softwaretechnieken een enorme verbetering zou kunnen betekenen in de elektronische informatie-uitwisseling. Wij hebben in ons onderzoek laten zien dat er vanwege verschillende hardnekkige knelpunten voldoende aanleiding bestaat tot het zoeken naar verbeteringen in de elektronische informatie-uitwisseling in het politiedomein.

Hoewel wij enkele oplossingsrichtingen aangeduid hebben roepen de resultaten van ons onderzoek en de resultaten van het ANITA-project uiteindelijk meer vragen op dan er beantwoord zijn. Vragen op het gebied van de AI, en fundamentele rechtsvragen over de toepassing van softwareagenten en de houdbaarheid van het juridisch kader. Voordat de door ons voorgestelde agenttechnologieën daadwerkelijk ingezet kunnen worden in het politiedomein zal veel aanvullend onderzoek nodig zijn. Onderzoek dat ons inziens noodzakelijk is aangezien de technologieën die inbreuken maken op de privacy zich in een hoog tempo ontwikkelen. De enige effectieve tegenkracht die ervoor kan zorgen dat het wankele evenwicht tussen veiligheid, ICT, en de privacy bewaard blijft, is ons inziens de technologie zelf: de reguleringstechnologie.

Samenvatting

Het proefschrift vormt een onderdeel van interdisciplinair onderzoek (het ANITA-project) naar de mogelijkheden van intelligente ICT-ondersteuning bij de elektronische uitwisseling van politiegegevens. Het doel van dit onderzoek is het ontwerpen van softwareagenten die in staat zijn om beslissingen te nemen over de vraag of politiegegevens al dan niet kunnen (of mogen) worden uitgewisseld. De nadruk van de verhandeling ligt op het conceptuele niveau: begrijpen wat er gebeurd en te gebeuren staat.

Het onderzoek kent een juridisch gedeelte waarbinnen het gaat om het in kaart brengen van de bestaande (juridische) knelpunten in het proces van informatie-uitwisseling. Het onderzoek kent daarnaast een technisch gedeelte waarbinnen onderzoekers met een achtergrond in de Artificiële Intelligentie (AI) zich bezighouden met de daadwerkelijke ontwikkeling van softwareagenten. Een belangrijke vraag is dan ook op welke wijze de binnen het ANITA-project ontwikkelde softwareagenten kunnen bijdragen aan het oplossen van de geconstateerde knelpunten. Dit proefschrift concentreert zich op het laatste deelonderzoek. De centrale probleemstelling luidt als volgt.

In hoeverre kan de inzet van softwareagenten en normatieve multi-agenttechnieken bijdragen aan de verbetering en de regulering van de elektronische uitwisseling van politiegegevens?

Binnen het raamwerk van deze probleemstelling en met het oog op de algemene doelstelling van het ANITA-project behandelt dit proefschrift vier onderzoeksvragen. Deze vragen luiden als volgt.

1. *Wat zijn de theoretische mogelijkheden van softwareagenten en multi-agenttechnieken?*

2. *Op welke wijze heeft de wetgever de uitwisseling van criminele inlichtingen genormeerd?*

3. *Op welke wijze is de huidige uitwisseling van criminele inlichtingen ingericht en wat zijn daarin de juridische knelpunten?*

4. *Op welke wijze kunnen softwareagenten en multi-agenttechnieken worden ingezet ten behoeve van de verbetering van het proces van informatie-uitwisseling vanuit het perspectief van de rechtshandhaving en de rechtsbescherming?*

Hoofdstuk 2 behandelt de eerste onderzoeksvraag. Om inzicht te krijgen in de mogelijkheden van agenttechnieken beschrijven wij enkele wetenschappelijke ideeën en achtergronden van de ontwikkeling van softwareagenten en multi-agenttechnieken. Het hoofdstuk geeft een kort historisch overzicht van de AI in het algemeen en softwareagenten in het bijzonder. Wij signaleren daarin een trend waaruit met enige voorzichtigheid een richting kan worden afgeleid waarin computersystemen en informatiesystemen zich de komende decennia zullen ontwikkelen. Voorts bespreken wij aan de hand van de vier eigenschappen het concept softwareagent. De eigenschappen worden binnen de AI doorgaans gebruikt om softwareagenten te onderscheiden van 'normale' softwareprogramma's. De eigenschappen zijn: (1) autonomie, (2) reactiviteit, (3) adaptief gedrag en (4) communicatie. Zij geven een goed inzicht in de (theoretische) mogelijkheden en toepassingen van softwareagenten.

Vervolgens worden de multi-agentsystemen behandeld. Dit zijn computersystemen waarin verschillende softwareagenten op basis van een bepaalde taakverdeling en door middel van een interactie, gezamenlijk in staat zijn complexe taken uit te voeren. Afhankelijk van de omvang en complexiteit van het systeem kan dat leiden tot zogenaamd *emergent gedrag*. Het gaat dan om de uitkomst van de collectieve interactie tussen verschillende softwareagenten. Dergelijk gedrag kan onverwachte voordelen met zich meebrengen, maar ook onverwachte nadelen. Wij menen dat binnen het domein van de uitwisseling van politiegegevens emergent gedrag kan leiden tot onwenselijke afbreukrisico's. Om die reden is er in multi-agentsystemen ook behoefte aan toepassingen die negatief emergent gedrag corrigeren. Binnen het ANITA-project heeft Aldewereld (2007) zich onder meer bezig gehouden met dit probleem en voorstellen gedaan hoe dit negatieve gedrag zou kunnen worden gecorrigeerd. Wij bespreken daarom tevens de verschillende toepassingen die binnen het ANITA-project zijn ontwikkeld. Daarmee geeft het hoofdstuk antwoord op de eerste onderzoeksvraag naar de (theoretische) mogelijkheden van softwareagenten en multi-agenttechnieken.

In hoofdstuk 3 beschrijven wij het juridisch kader waarbinnen de uitwisseling van politiegegevens is genormeerd. Wij merken hierbij op dat tijdens de onderzoeksperiode de Wet Politieregisters werd vervangen door de Wet Politiegegevens. Om inzicht te geven in de ontwikkelingen en veranderingen van dit juridisch kader worden in hoofdstuk 3 allereerst enkele historische achtergronden besproken. Voorts is een internationaal juridisch kader uitgewerkt, omdat op de bescherming van de persoonlijke levenssfeer en de verwerking van politiegegevens niet alleen nationale, maar ook rechtstreeks werkende internationale normen van toepassing zijn. Dit kader vormt het raamwerk waarbinnen op nationaal niveau de nieuwe Wet Politiegegevens is vastgesteld. Vanwege de omstandigheid dat gedurende de eerste helft van het onderzoek de oude Wet Politieregisters nog van toepassing was, geven

wij bij de bespreking van de nieuwe normen uit de Wet Politiegegevens tevens aan in hoeverre er sprake is van een verandering van het juridisch kader ten opzichte van de Wet Politieregisters. Met deze gedetailleerde bespreking van het juridisch kader geven wij antwoord op de tweede onderzoeksvraag.

In hoofdstuk 4 beschrijven wij de criminele inlichtingeneenheden (CIE-en) die binnen de regiokorpsen verantwoordelijk zijn voor de verwerking van 'bijzondere' politiegegevens te weten: criminele inlichtingen. Omdat het domein van de verwerking en uitwisseling van politiegegevens omvangrijk is hebben wij ons onderzoek beperkt tot deze categorie van politiegegevens. De beperking heeft twee redenen. De eerste reden is gelegen in het feit dat uit verschillende onderzoeken naar voren is gekomen dat CIE-ambtenaren de van toepassing zijnde wet- en regelgeving als lastig en complex ervaren. Op zichzelf is dit gegeven al aanleiding om aan te nemen dat er mogelijkheden aanwezig zijn voor de inzet van normatieve multi-agenttechnieken. De tweede reden heeft betrekking op de complexiteit van de (tegengestelde) belangen in dit domein. De regionale opsporingsbelangen enerzijds en de (informationele) privacybelangen van de betrokkenen anderzijds maken de uitwisseling van criminele inlichtingen tot een interessant onderzoeksomein voor juristen en AI-onderzoekers. Daarom beschrijven wij zowel de wijze waarop de CIE zich heeft ontwikkeld tot de hedendaagse organisatie als het gebruik van de diverse informatiesystemen. De belangrijkste taak van de CIE is het opbouwen en onderhouden van de informatievoorziening in het kader van de uitvoering van de politietaak, voor zover het bepaalde ernstige vormen van criminaliteit betreft. Het hoofdstuk beschrijft op welke wijze door de CIE-en informatie wordt ingewonnen en hoe deze wordt verwerkt en uitgewisseld. Ten aanzien van de uitwisseling onderscheiden wij (1) het elektronisch verstrekken van informatie via gekoppelde systemen en (2) het handmatig verstrekken inlichtingen. Het hoofdstuk maakt daarmee de huidige werkwijze en actuele ontwikkelingen op het gebied van de informatiehuishouding binnen de CIE inzichtelijk.

In hoofdstukken 5 wordt een begin gemaakt met de beantwoording van de derde onderzoeksvraag. Wij behandelen daartoe vijf evaluatieonderzoeken naar de uitwisseling van politiegegevens die sinds het midden van de jaren negentig zijn uitgevoerd. Vervolgens bespreken wij de bevindingen van ons eigen veldwerk. Wij stellen vast dat in de loop van de jaren de volgende vijf immer terugkerende knelpunten zijn te onderscheiden.

1. *Moeilijk toegankelijke juridische kennis;*
2. *ontoereikende gegevenscontrole*;
3. *onvoldoende standaardisatie;*
4. *gesloten bedrijfscultuur;*
5. *ontoereikende privacywaarborgen*.

In hoofdstuk 6 analyseren wij met behulp van de CommonKads-methode de wijze waarop de huidige informatie-uitwisseling binnen de CIE plaatsvindt. In de analyse laten wij zien dat het huidige bedrijfsproces met betrekking tot de informatie-uitwisseling binnen de CIE kan worden onderverdeeld in zes deeltaken. Geen van deze deeltaken is geautomatiseerd. Zo bezien is er in beginsel voldoende ruimte voor automatiseringstoepassingen. Aangezien het doel van het ANITA-project onderzoek evenwel is gelegen in de vraag waar in dit proces van informatie-uitwisseling normatieve beperkingen zouden kunnen worden ingebouwd hebben wij de analyse toegespitst op (1) het nader ontleden van de zes deeltaken en (2) het analyseren van de kennis die nodig is voor de uitvoering van deze deeltaken.

De analyse heeft tot het inzicht geleid dat tenminste drie deeltaken (controle ontvangstgerechtigde, vaststellen informatiedoel, beoordelen afbreukrisico's) verhoudingsgewijs kennisintensief zijn. De overige drie deeltaken (selecteren relevante informatie, bepalen informatieproduct, registreren verstrekking) zijn dat niet. Voor de uitvoering van de kennisintensieve deeltaken is (moeilijk toegankelijke) juridische kennis vereist. Deze drie deeltaken hebben wij vervolgens aan de hand van drie taakmodellen nader onderzocht waarbij wij tot de conclusie zijn gekomen dat de deeltaken aanknopingspunten bieden voor (gedeeltelijke) normatieve agenttechnieken.

Vanuit het perspectief van de rechtshandhaving betogen wij dat normatieve softwareagenten goede mogelijkheden bieden om de informatie-uitwisseling te verbeteren.

Vanuit het perspectief van de rechtsbescherming zien wij verschillende mogelijkheden om in het proces van informatie-uitwisseling de privacy adequaat te waarborgen door middel van normatieve beperkingen. Wij denken daarbij aan (1) het zorgvuldig toepassen van de wettelijke bepalingen, (2) het verbeteren van (geautomatiseerd) toezicht op de registraties, en (3) het vergroten van de transparantie van de gegevensregistratie en -uitwisseling. Wij geven aan waar in het proces van informatie-uitwisseling zich deze mogelijkheden voordoen en waar mogelijkheden zitten om softwareagenten in te zetten die juridische regels kunnen toepassen of daarover kunnen adviseren om zodoende de *compliance* van de uitwisseling te verbeteren. Voorts betogen wij dat de inzet van softwareagenten kan bijdragen aan (1) het verbeteren van de kwaliteit van de registraties en (2) de transparantie van de uitwisseling.

Hoofdstuk 7 geeft antwoord op de vierde onderzoeksvraag. Wij laten zien multi-agenttechnieken de uitwisseling op verschillende wijzen kan ondersteunen en ook toekomstbestendig kan maken. Toekomstbestendigheid is volgens ons van belang omdat informatie de komende decennia hoe langer hoe meer digitaal beschikbaar zal zijn.

Vanuit het perspectief van de rechtsbescherming betogen wij aan de hand

van enkele binnen het ANITA-project ontwikkelde conceptuele voorbeelden van softwareagenten en multi-agenttoepassingen dat de verticale uitwisseling met ketenpartners vergaand zinvol kan worden geautomatiseerd. Zo laat de toepassing van de door Teepe (2006) ontwikkelde *information designator* zien dat de uitwisseling kan worden verbeterd vanwege de omstandigheid dat het beheer en de controle over de informatie geheel bij de verantwoordelijke regio blijft, ook tijdens het zoekproces. Daarmee wordt voorkomen dat de verantwoordelijke van de informatie controle over 'zijn' informatie verliest. Juist in het domein van de criminele inlichtingen lijkt dat een goede oplossing omdat actualiteit en controle over de informatie van groot belang zijn.

Vanuit het perspectief van de rechtsbescherming laten wij zien dat softwareagenten een adequaat (rechts)waarborgingsmechanisme kunnen zijn door de mogelijkheid van implementatie van juridische regels in de softwarecode. Gebruikers van de politiële informatiesystemen worden daardoor als het ware gedwongen om de relevante rechtsregels na te leven omdat het systeem hen geen andere mogelijkheden geeft. Op die manier wordt onder meer een technische oplossing gevonden voor het knelpunt dat de rechtsregels door de politieambtenaren als moeilijk toepasbaar en onduidelijk worden ervaren. Automatische toepassing van deze regels betekent immers dat de gebruikers deze regels niet noodzakelijkerwijs behoeven te begrijpen, terwijl zij wel worden toegepast.

In hoofdstuk 8 formuleren wij onze antwoorden op de onderzoeksvragen en de probleemstelling. Wij plaatsen onze conceptuele voorbeelden van multiagenttoepassingen voorts in het bredere perspectief van de rechtsbescherming, in het bijzonder waar het gaat om de waarborging van het recht op privacy. Vanwege de steeds verder toenemende technologische mogelijkheden betogen wij dat daarmee het recht op privacy hoe langer hoe meer dreigt te worden uitgehold. Vanuit dit perspectief kunnen softwareagenten ingezet worden als zogenaamd reguleringsinstrument teneinde de privacy effectief te waarborgen.

Omdat de politieorganisatie vooral vanuit haar eigen perspectief en de taakopvatting informatiesystemen ontwikkelt stellen wij dat er een taak ligt voor de wetgever om 'kunstmatig' een prikkel te creëren met als doel de normatieve beperkingen in informatiesystemen te ontwikkelen. Wij bevelen onder meer aan om de onafhankelijke toezichthouder, het College bescherming persoonsgegevens (Cbp), een wettelijk verankerde adviserende taak te geven bij de ontwikkeling van nieuwe politiële informatiesystemen. Daarnaast betogen wij dat als sluitstuk van het onafhankelijk toezicht, het Cbp een goedkeuringsbevoegdheid moet krijgen met betrekking tot de ingebruikname van nieuwe informatiesystemen. Indien goedkeuring onthouden wordt, of wanneer nadere voorschriften aan het systeem worden gesteld,

kan zo'n besluit uiteindelijk ter toetsing aan de bestuursrechter worden voorgelegd. Tenslotte formuleren wij enkele vervolgvragen die ons onderzoek oproept.

Summary

This dissertation forms part of the interdisciplinary research (ANITA project) into the possibilities for supporting the electronic exchange of police information by intelligent ICT applications. The general purpose of this research is to develop software agents that are able to make decisions concerning whether police information can be exchanged.

The research has a legal part which maps out the existing (legal) bottlenecks in the process of information exchange. In addition, the research has a technical part in which researchers with a background in Artificial Intelligence (AI) concern themselves with the actual development of software agents. An important question is how software agents can contribute to solving the bottlenecks. This dissertation concentrates on the last part of the research. The central definition of the problem reads as follows.

To what extent can the deployment of software agents and normative multi-agent techniques contribute to the improvement and regulation of the electronic exchange of police information?

Within the context of this definition of the problem and in view of the general objective of the ANITA project, this dissertation discusses four research questions. These questions are defined as follows.

1. *What are the theoretical possibilities of software agents and multi-agent techniques?*

2. *How does legislature regulate the exchange of criminal intelligence?*

3. *How is the current exchange of criminal intelligence organized and what are the legal bottlenecks?*

4. *How can software agents and multi-agent techniques be deployed to improve the process of information exchange from the perspective of law enforcement and legal protection.*

Chapter 2 discusses the first research question. To gain an insight into the possibilities of agent techniques, we describe some background of the development of software agents and multi-agent techniques. The chapter gives a brief historical overview of AI in general and software agents in particular. We signal a trend, with some qualification, from which a direction can be made in the context of computer and information systems' developments in

the coming decades. We also discuss the concept software agent on the basis of four qualities. The qualities are normally used within the AI to distinguish the software agents from 'normal' software programs. The qualities are: (1) autonomy, (2) reactivity, (3) adaptive behaviour and (4) communication. They give insight into the (theoretical) possibilities and applications of software agents.

Then the multi-agent systems are discussed. These are computer systems in which various interacting software agents are jointly capable of executing complex tasks based on a defined task division. This can lead to so called *emergent behaviour* depending on the magnitude and complexity of the system. This involves the outcome of the collective interaction between various software agents. Such behaviour can entail unexpected advantages but also unexpected disadvantages. We think that emergent behaviour can lead to unwelcome risk factors within the domain of the exchange of police information. Because of that reason there is also a need for multi-agent systems that correct negative emergent behaviour. Aldewereld (2007) has dealt with this problem, amongst others, in the ANITA project and made suggestions for how this negative behaviour could be corrected. We therefore also discuss the various applications that are developed within the ANITA project. The chapter therefore answers the first research question regarding the (theoretical) possibilities of software agents and multi-agent techniques.

In chapter 3 we describe the legal framework in which the exchange of police information is regulated. We note that the Data Protection (Police Files) Act was replaced by the Data Protection (Police Information) Act during the research period. In order to gain an insight into the developments and changes of this legal framework, chapter 3 first discusses some historical backgrounds. Then the international legal framework is examined. Both national and directly applicable international norms apply to the privacy protection and the processing of police information. This framework forms the outline in which the new Data Protection (Police Information) Act is determined at a national level. Because of the fact that the old Data Protection (Police Files) Act still applied during the first half of the research, we will also discuss whether there is a change of the legal framework with the new norms of the Data Protection (Police Information) Act in comparison to the Data Protection (Police Files) Act. We answer the second research question with this detailed discussion of the legal framework.

In chapter 4 we describe the criminal intelligent units (CIU's), which are responsible within the regional police forces for the processing of 'special' police information, i.e.: criminal intelligence. Because the domain of the processing and exchange of police information is extensive, we have limited our research to this category of police information. There are two reasons for this limitation. The first reason is because of the fact that several researches show that Criminal Intelligence Unit (CIU) officials find the applicable legislation

difficult and complex. This fact in itself is already reason to assume that there are possibilities present for the deployment of normative multi-agent techniques. The second reason relates to the complexity of the (opposite) interests in this domain. The regional investigation interests on one hand, and the (informational) privacy interests of the involved on the other, make the exchange of criminal intelligence an interesting research domain for jurists and those involved with AI. That is why we describe both how the CIU has developed itself into the current organisation, and the use of several information systems. The most important task of the CIU is to construct and maintain the information supply in the context of carrying out the police task, as far as it concerns certain serious forms of criminality. The chapter describes how the CIU obtains information and how this is processed and exchanged. With regard to the exchange we make a distinction between the electronic distribution of information through linked systems and manually distributing information. The chapter provides insight into the present working method and current developments in the field of information management within the CIU.

In chapters 5 we start with the third research question. In order to answer this question we review five (evaluation) research projects focussing on the exchange of police information. We then discuss the findings from our own field work. We conclude that the following five recurring bottlenecks can be distinguished from the research results over the years.

1. *Difficulty accessing legal knowledge;*
2. *inadequate information check*;
3. *insufficient standardization;*
4. *Closed company culture;*
5. *Inadequate privacy guarantees.*

In chapter 6 we analyze the way in which the current information exchange takes place within the CIU with the help of the CommonKads method. In these analyses we show that the current business process for the information exchange within the CIU can be divided into six sub-tasks. None of these tasks are automated in the current information exchange system. Seen in this light, there is enough room for automating applications in principle. Because of the fact that the objective of the ANITA project is concerned with the question of where normative limitations could be implemented in this process of information exchange, we have concentrated the analyses on the further examination of (1) the six sub-tasks and (2) the knowledge that is required to execute these sub-tasks.

The analysis have lead to the insight that at least three sub-tasks (checking qualified recipient, establishing information purpose, assessing risk factors) are relatively knowledge intensive. The other three sub-tasks (selecting relevant information, determining information product, registering distribution)

are not. In order to execute the knowledge intensive sub-tasks (difficult accessible) legal knowledge is required. Next we analyzed the three sub-tasks on the basis of three task models which lead us to the conclusion that the sub-tasks offer starting points for (partly) normative agent techniques.

From the perspective of law enforcement we argue that the normative software agents offer good possibilities for improving the information exchange.

From the perspective of legal protection we see various possibilities for better safeguarding of the privacy in the information exchange process by means of normative limitations. We think of (1) a more precise application of the legal stipulations, (2) improving the (automated) supervision on the registrations, and (3) enlarging the transparency of the information registration and exchange. In the task models we (a) indicated where these difficulties might occur in the process of information exchange and (b) where there are possibilities for deploying software agents that can apply legal regulations or advise about this in order to improve the *compliance* of the exchange. We also argue that the deployment of software agents can contribute to (1) improving the quality of the registrations and (2) the transparency of the exchange.

Chapter 7 answers the fourth research question. In this chapter we show that multi-agent techniques can support the exchange in several ways and can make it future-proof. In our opinion it is important to be future-proof because information will become increasingly more digitally available in the coming decades.

From the prespective of law enforcement we argue that the vertical exchange with chain partners can be automated significantly. The application of the *information designator* developed by Teepe (2006) shows that the exchange can be improved because of the circumstance that the management and checking of the information will remain completely with the responsible region, also during the search process. This prevents the person responsible for checking the information from losing control of 'their' information. This seems a good solution, especially in the domain of criminal intelligence, because topicality and control over the information are very important.

From the perspective of legal protection software agents also offers an adequate (legal) guarantee mechanism because of the possibility of implementing legal regulations in the software code. Because of this, users of the police information systems are actually forced to comply with the relevant legal regulations because the system will not give them any other possibilities. This means a technical solution is found for the bottleneck of legal regulations being experienced as difficult to apply and unclear by police officials.

Automatic application of these rules means that the users will not necessarily have to understand these rules while they are being applied.

In chapter 8 we summarise the research and answer the problem statement. We place our conceptual examples of multi-agent applications in the wider perspective of the legal protection, more specifically where it concerns safeguarding the right to privacy. Because of increasingly more technological possibilities we argue that undermining the right to privacy is more and more of a threat. Because of this it will become increasingly necessary in the coming decades to safeguard this right more effectively and adequately than is done at this point in time.

Because of the fact that the police organisation develops the information systems mostly from its own perspective and its own understanding of the task, we argue that the legislator has a duty to 'artificially' create an incentive with the purpose of developing normative limitations in information systems. We advise, amongst other things, to give the Dutch Data Protection Authority a legally anchored advisory duty with the development of new police information systems. We also argue that the Dutch Data Protection Authority should obtain a consent authority with regard to the use of new information systems as a final piece for the independent supervision. If consent is withheld or when further regulations are attached to the system such a decision can be submitted for review by the judge in administrative law. Finally we formulates further research questions that arise from our findings.

Referenties

Aalbersberg e.a., 1993
P.J. Aalbersberg, B.N. Barendregt en J.B.A. de Wit, De ontwikkeling van het CID-werk, in: A.W.M. van der Heijden (red.), *Criminele inlichtingen: de rol van Criminele Inlichtingendiensten bij de aanpak van de georganiseerde misdaad*, 's-Gravenhage: VUGA Uitgeverij, 1993.

Agotnes, van der Hoek en Wooldridge, 2008
T. Agotnes, W. van der Hoek, M. Wooldridge, Quantifying over coalitions in epistemic logic, *Proceedings of AAMAS* 2008, pp. 665~672 .

Albert, 1976
H. Albert, Rationaliteit in wetenschap en samenleving: opstellen over wetenschap politiek en ideologie, Alphen a/d Rijn: Samson, 1976.

Alchouron en Bulygin, 1971
C.E. Alchouron en E. Bulygin, *Normative Systems*, New York en Wenen: Springer-Verlag, 1971.

Aldewereld, 2007
H.M. Aldewereld, Autonomy vs. Conformity. An Institutional perspective on Norms and Protocols, (diss. Utrecht) Enschede: Gildeprint drukkerijen B.V. 2007.

Asscher, 2006
L. Asscher, Code as Law. Using Fuller to asses code rules, in: E. Dommering en L. Asscher, *Coding Regulation, Essays on the Normative Role of Information Technology*, Den Haag: T.C.M. Asser Press 2006

Bex, Prakken en Verheij, 2007
F.J. Bex, H. Prakken en B. Verheij, *Formalising argumentative story-based analysis of evidence*. Proceedings of the 11th International Conference on Artificial Intelligence and Law, Stanford USA, New York: ACM Press, pp. 1-10.

Borking e.a., 1999
J.J. Borking, B.M.A. van Eck en P. Siepel, *Intelligent software agents and privacy,* Achtergrondstudies en Verkenningen nr. 13, Den Haag: Registratiekamer, januari 1999.

Borking en Raab, 2000
J.J. Borking en C.D. Raab, Law, PETs and other Technologies, *Journal of Information, Law and Technology (JILT)* 2000.

Buruma, Goos en Michels, 2003
Y. Buruma, M. Goos, G.W.T.J. Michels (red), *Jaarboek wet politieregisters: leidraad voor de praktijk*, Alphen aan de Rijn: Kluwer, 2003.

Buruma, 2008
Y. Buruma, Privacy en veiligheid: de passie voor de werkelijkheid, Den Haag: College bescherming persoonsgegevens, 2008.

Bradshaw 1998
J. Bradshaw, *Software Agents*, Menlo Park, California: AAArtificial-intelligence Press.

Brazier e.a. 2002
F.M.T. Brazier, O. Kubbe, A. Oskamp, N.J.E. Wijngaards, Are Law-Abiding Agents Realistic? In: *Proceedings of the workshop on the law of Electronic Agents (LEA02), juli 2002.*

Brazier e.a. 2003
M.T. Brazier, A. Oskamp, J.E.J. Prins, M.H.M Shellekens, N.J.E. Wijngaards, M. Apistola, M. Voulon, O. Kubbe, *Analysing Legal Implications and Agent Information Systems,* Technical Report No. IR CS 004, Amsterdam, Vrije Universiteit.

Brooks 1991
R.A. Brooks, Intelligence without representation, in: *Artificial-intelligence, 47,* p. 139-159.

Brownsword, 2004
R. Brownsword, What the World Needs Now: Techno-regulation, Human Rights and Human Dignity, in: R. Brownsword, *Global Governance and the Quest for Justice, vol. 4,* Oxford: Hart 2004.

Campell, Hoane en Hsu, 2001
M. Campell, A.J. Hoane en F. Hsu, Deep Blue, Artificial Intelligence 2002 , Vol. 134, pp. 57-83.

Clark, 2003
I. Clark, Legitimacy in a Global Order, *Review of International Studies* 29, pp. 75-95.

Cleiren, 1989
C.P.M. Cleiren, Beginselen van een goede procesorde: een analyse van rechtspraak in strafzaken, (diss.: Leiden) Arnhem: Gouda Quint, 1989.

Cleiren, 2004
C.P.M. Cleiren 2004, Toezicht op rechtshandhaving, in: *Veiligheid, Studies over inhoud, organisatie en maatregelen,* E.R. Muller, Deventer: Kluwer 2005, pp. 503-539.

Corstens, 2008
G.J.M. Corstens, *Het Nederlandse strafprocsrecht,* (zesde druk) Deventer: Kluwer, 2008.

Cozijn, 1996
C. Cozijn, Wet en Besluit politieregisters: een inventarisatie van knelpunten in de politiepraktijk, 's-Gravenhage: Wetenschappelijk Onderzoek- en Documentatiecentrum 1996.

Van Dartel, 2005
M. van Dartel, *Situated Representation,* SIKS Dissertation Series No. 2005-19, Maastricht: Universiteit van Maastricht.

Dijkstra e.a., 2006
P. Dijkstra, F.J. Bex, H. Prakken, en C.J.N. De Vey Mestdagh, Towards a multi-agent system for regulated information exchange in crime investigations. *Artitcial Intelligence and Law 2006 nr.* 13, p. 133-151.

Dijkstra e.a., 2007
P. Dijkstra, H. Prakken en C.J.N. De Vey Mestdagh, An Implementation of Norm-based Agent Negotiation, Proceedings of the 11th international conference on Artificial intelligence and law, Standford (USA): 2007, p. 167-175.

De Hert en Gutwirth, 2004
P.J.A. De Hert en S. Gutwirth, Veiligheid en grondrechter: het belang van een evenwichtige privacypolitiek, in: E.R. Muller, *Veiligheid, Studies over inhoud, organisatie en maatregelen,* Deventer: Kluwer 2005, PP. 587-630.

Dommering 2006
E. Dommering, Regulation Technology: Code is not Law, in: E. Dommering en L. Asscher, *Coding Regulation, Essays on the Normative Role of Information Technology*, Den Haag: T.C.M. Asser Press 2006.

Dommering en Asscher, 2006
E. Dommering en L. Asscher, Coding Regulation, Essays on the Normative Role of Information Technology, Den Haag: T.C.M. Asser Press 2006.

Dyson, 1997
G.B. Dyson, Darwin Among the Machines: The Evolution of Global Intelligence, New York: Perseus Books Group, 1998

Eling, 2003
A.M. Eling (Algemene Rekenkamer), Uitwisseling opsporings- en terrorisme-informatie, Den Haag: SDU uitgevers, 2003

Ellul, 1964
J. Ellul, The technological society. New York: Vintage Books, 1964.

Enschedé, 1966
Ch. Enschedé, Bewijzen in het strafrecht, *RM Themis* 1966, p. 516.

Fuller, 1964
L.L. Fuller, Morality of Law, (New Haven, Yale University Press, 1964.

Grimmelmann, 2005
J, Grimmelmann, Regulation by software, *Yale Law Journal* 114, p. 1719-1758.

Groothuis, 2004
M.M. Groothuis, Beschikken en digitaliseren. Over normering van de elektronische overheid, (diss.: Leiden), Den Haag: SDU Uitgevers, 2004.

Van Gunsteren, 2004
H. van Gunsteren, Gevaarlijk veilig. Terreurbestrijding in de democratie, Van Gennep 2004.

Feenstra-Schellekens e.a., 2007
L.M. Feenstra-Schellekens (red), D. van der Bel, A.M. van Hoorn, J.J.T.M. Pieters, *Informatie en opsporing: handboek informatieverwerving, -verwerking en -verstrekking ten behoeve van de opsporingspraktijk,* Zutphen: Studiecentrum Rechtspleging, 2007.

Franken, 1992
H. Franken, Overheid, informatietechnologie en recht – een gevarendriehoek?, in: P.H. Frissen, A.W. Koers en I. Th. M. Snellen, Orwell of Athene, *Democratie en informatiesamenleving*, Den Haag: NOTA 1992, pp. 165-177.

Franken, 2004
H. Franken, Juridische en theoretische achtergronden, in: H. Franken, H.W.K. Kaspersen en A.H. de Wild, *Recht en Computer,* Deventer: Kluwer, 2001.

Fukuyama, 2002
F. Fukuyama, de nieuwe mens: onze wereld na de biotechnische revolutie. Amsterdam/Antwerpen: Contact 2002.

Hamburg, 2005
F. Hamburg, Een computermodel voor het ondersteunen van euthanasiebeslissingen, (diss: Leiden), Antwerpen: Maklu-Uitgevers, 2005.

In-pact, 1991
Adviesbureau In-pact, Advies inzake onderzoek naar huidige en toekomstige ontwikkelingen van CID-applicaties, Utrecht 1991.

Van den Herik, 1983
H.J. van den Herik, Computerschaak, schaakwereld en kunstmatige intelligentie, (diss. Delft), 's-Gravenhage: Academic Service 1983.

Van den Herik, 1991
H.J. van den Herik, *Kunnen computers* Rechts*preken*, (oratie, Leiden), Arnhem: Gouda Quint, 1991

De Hert en Gutwirth
P.J.A. De Hert en S. Gutwirth, Veiligheid en grondrechten; het belang van een evenwichtige privacypolitiek, in: E.R. Muller, V*eiligheid. Studies over inhoud, organisatie en maatregelen*, Deventer: Kluwer, 2005.

De Hert en Koops, 2001
P.J.A. De Hert en B.J. Koops, Privacy is nog steeds een grondrecht. Pleidooi voor de uitsluiting van onrechtmatig bewijs, *Ars Aequi*, 2001 vol. 50, 972-975.

Hildebrandt en Koops, 2007
M. Hildebrandt en B.J. Koops, A Vision of Ambient Law, FIDIS Deliverable, Oktober 2007, te downloaden op: <http://www.fidis.net/fidis-del>.

Hughes, 1994
T.P. Hughes, Technological momentum, in: R.M. Smith en L. Marx (red.) *Does Technology Drive History? The Dilemma of Technological Determinism,* Massachusetts: Massachusetts Institut of Technology, 1994.

Ignatieff, 2002
M. Ignatieff, *Mensenrechten en terreur*, Thomas More-lezing 2002, Bundel 2002.

IME Consult, 1989
IME Consult (in samenwerking met het Ministerie van Justitie), Bedrijfskundig vooronderzoek recherche; eindrapport, Nijmegen: IME Consult Organisatie Adviesbureau, 1989.

Jones en Carmo, 2001
A. Jones and J. Carmo. Deontic logic and contrary-toduties, in D. Gabbay, editor, *Handbook of Philosophical Logic*, page 203279, Kluwer, 2001.

Keizerwaard, 1988
M.M. Keizerwaard, Rapportage project/werkgroep automatisering CID, Hellevoetsluis (s.n.) 1988.

Kelk, 1998
C. Kelk, *Materieel strafrecht*, Arnhem: Gouda Quint, 1998.

Kielman en Koelewijn, 2005
Kielman & Koelewijn, 'Privacy als tunnelvisie', *Privacy & Informatie* 2005.

Kielman 2009
H.H. Kielman, Politiële gegevensverwerking en Privacy. Naar effectieve waarborging, (diss. Leiden) (nog te verschijnen).

Kievit, 2004
A. de Kievit, Veilig stellen van restinformatie, gewoon doen! Eindrapportage van de landelijke werkgroep Restinformatie, Programmabureau Abrio, Project Restinformatie, juni 2004.

Klerks e.a., 2002
P.P.H.M. Klerks, De voorhoede van de opsporing: evaluatie van de kernteams als instrument in de aanpak van zware georganiseerde criminaliteit, Doetinchem: Reed Business Information, 2002.

Van Klink, Prins en Witteveen, 2000
B. Van Klink, C. Prins, en W. Witteveen, Het conceptuele tekort. Een surveyonderzoek naar de wisselwerking tussen ICT en het recht, Amsterdam: Infodrome, 2000.

Klusch, 2001
M. Klusch (ed.) Special issue on Intelligent Information Agents: Theory and Applications, Intelligent Cooperative Information Systems, vol. 10 (1&2), March 2001.

Koelewijn en Kielman, 2006
W.I. Koelewijn en H.H. Kielman, Agenten voor agenten. Slimme software ter ondersteuning van menselijk handelen, in: W. Huisman, L. M. Moerings, A. M. Beukelman, *Veiligheid en recht: nieuwe doelwitten en strategieën*, Den Haag: Boom Juridische uitgevers, 2006.

Kooijmans, 2008
P.H. Kooijmans, Internationaal Publiekrecht in vogelvlucht, Deventer: Kluwer, 2008.

Koolen en Moonen, 2004
L.J.M. Koolen en E.P.H. Moonen, Landelijke coördinatie en uitwisseling van politie-informatie, Een evaluatie van het project landelijke informatiecoördinatie DNP, december 2004.

Koops e.a., 2006
B-J. Koops, M. Lips, B. van Klink, C. Prins, M. Schellekens, Starting Points for ICT Regulation Deconstructing Prevalent Policy One-liners, *IT & Law,* Series 9, The Hague: TMC Asser Press.

Koops, 2007
B.J. Koops, Criteria for Normative Technology. An essay on the acceptability of ' code as law' in light of democratic an constitutional values, *TILT Law & Technology Working Paper No. 005/2007 & Tilburg University Legal Studies Working Paper No. 007/2007, versie 7 december 2007, te downloaden op: <http://ssrn.com/abstract=1071745>.*

Van Kralingen, 1996
R.W. van Kralingen, *Frame-based Conceptual Models of Statute Law,* (diss. Leiden), 's-Gravenhage: Kluwer Law International, 1996.

Kuitenbrouwer, 1991
F. Kuitenbrouwer, *Het recht om met rust gelaten te worden. Over privacy,* Amsterdam: Uitgeverij Balans 1991, p. 65-79.

Kurzweil, 1990
R. Kurzweil, *The age of intelligent machines*, Cambridge: MIT Press, 1990.

Kurzweil, 2001
R. Kurzweil, Law of accelerating returns, *Lifeboat Foundation Special Report*, 2001.

Kurzweil, 2005
R. Kurzweil, The Singularity is Near: When Humans Transcend Biology, New York: Viking, 2005

Kranenburg e.a., 1988
W.J. Kranenburg, J.G.A. Nouwens en C.L. Venrooij, 'Automatiseren van CID-bestanden', *Algemeen Politieblad,* nr. 17, 20 augustus 1988, p. 394-396.

Lai, Sycara en Li, 2007
G. Lai, K. P. Sycara, C Li, A pareto optimal model for automated multi-attribute negotiations, *International Joint Conference on Autonomous Agents and Multiagent Systems:* nr. 246, 2007.

Langendoen en Vierboom, 1998
K. Langendoen en A. Vierboom, Het koningskoppel, Klaas Langendoen en de oorlog rond zijn criminele inlichtingendienst (CID) Amsterdam: Uitgeverij Balans, 1998, p. 235.

Leenes en Prins, 2006
R. Leenes en C. Prins, Techniek al alternatief reguleringsinstrument, Implicaties voro privaatrechtelijke verhoudingen, in: B. Dorbeck-Jung en M. Oude Vrielnk-van Heffen, *Op weg naar bruikbare regulering?* 's-Gravenhage: Reed Business Information, 2006, pp.117-134.

Lessig, 1996
L. Lessig, The Zone of Cyberspace, *Standford Law Review* 48, p. 1408 e.v.

Lessig, 1999
L. Lessig, *Code and other Laws of Cyberspace,* New York, Basic Books 1999.

Levy, 2007
D. Levy, Love and Sex with Robots: The Evolution of Human-Robot Relationships, Harper Collins, 2007.

Li e.a., 2006
Z. Li, Ch.H. Sim M.Y.H. Low, A Survey of Emergent Behavior and Its Impacts in Agent-based Systems, IEEE International Conference on Industrial Informatics, augustus 2006.

Meesters, Kortekaas en Tragter, 2000
P. Meesters, J. Kortekaas en M. Tragter, Intelligence Led Policing: nieuw concept voor integratie van oude adagia, *Tijdschrift voor Criminologie,* 2000, vol. 41, nr. 4.

Meyer en Wieringa 1993
J.-J. Ch. Meyer en R.J. Wieringa, *Deontic Logic in Computer Sience,* Chichester: J. Wiley, 1993.

Melai, 1975
A.L. Melai, Foullering en onrechtmatig verkregen bewijs, in: *Praesidium Libertatis* (1975).

Minsky, 1988
M.L. Minsky, *The Society of Mind,* London: Pan Books, 1988.

Mommers, Koelewijn en Kielman, 2007
L. Mommers, W.I. Koelewijn en H.H. Kielman, 'Understanding the Law: a method for legal knowledge dissemination', in: *Proceedings of the Eleventh International Conference on Artificial* Intelligence and Law, Stanford University, Palo Alto, California, June 2007, p. 195-203.

Mommers, Voermans, Koelewijn en Kielman, 2009
L. Mommers, W.J.M. Voermans, W.I. Koelewijn en H.H. Kielman, Understanding the law: improving Legal knowledge dissemination by translating the contents of formal sources, *Artificial Intelligence and Law,* 17 (1) pp. 51-78.

Muller, 2005
E.R. Muller, Toekomst veiligheid en veiligheidszorg, in: *Veiligheid, Studies over inhoud, organisatie en maatregelen,* E.R. Muller, Deventer: Kluwer 2005, pp. 779–789.

Muller, Krummeling en Bron, 2007
E.R. Muller, H.R.B.M. Kummeling en R.P. Bron, Veiligheid en Privacy. Een zoektocht naar een nieuwe balans, Den Haag: Boom Juridische uitgevers, 2007.

Mumford, 1963
L. Mumford, Technics and civilization, New York: Harcourt Brace Jovanovich, 1963.

Nijssen, 1977
G.M. Nijssen, 'On the Gross Architecture of the Next Generation Data Base management Systems, ' Proceedings 1977 IFIP Congress, Toronto.

Plaza en Ontañón 2007
E. Plaza en S. Ontañón, Learning and Joint Deliberation through Argumentation in Multi-Agent Systems, Proceedings of the 6th international joint conference on Autonomous agents and multiagent systems nr. 159, 2007.

Postma 2003
E.O. Postma, *De onderste steen boven* (oratie Maastricht), Maastricht: Universiteit Maastricht, 2003.

De Poot e.a., 2004
C.J. de Poot, R.J. Bokhorst, P.J. van koppen en E.R. Muller, Rechercheportret. Over dillema's in de opsporing, Deventer: Kluwer 2004.

Prakken, 2003
T. Prakken, Veiligheid of vergelding? Een bezinning over aard en functie van het strafrecht in de postmoderne risicomaatschappij, Nederlandstalige Strafrechtdag, Maastricht, 20 juni 2003.

Reidenberg, 1998
J. R. Reidenberg, Lex Informatica, The Formulation of Information Policy Rules Trough Technology, Tex. Law Review 1998, nr. 3 pp. 553-584.

Reidenberg, 2004
J. R. Reidenberg, States and Internet Enforcement, Law and technology Journal, vol. 1, nr. 213, pp. 213-230.

Reidenberg, 2007
J.R. Reidenberg, The Rule of Intellectual Property Law in the internet Economy, Housten Law Review, vol. 44, nr. 4, pp. 1074-1095.

Rössler, 2008
B. Rössler, *De glazen samenleving en de waarde van privacy,* Socrates-lezing gehouden op 13 november 2008.

Van Ruth en Gunther Moor
A.G.P. van Ruth en L.G.H. Gunther Moor, *Lekken of verstrekken? De informele informatie-uitwisseling tussen opsporingsinstanties en derden,* Nijmegen: Instituut voor Toegepaste Sociale Wetenschappen, 1997.

Van Ruth en Schreuders, 2000
A.G.P. van Ruth & E. Schreuders, Politiegegevens beschermd. Een toelichting op het gesloten verstrekkingenregime van de Wet Politieregister, Registratiekamer, mei 2000.

Schmidt 2007
A.H.J. Schmidt, Ought Computers Adjudicate? in: J. Donkers e.a., *Liber Amicorem ter gelegenheid van de 60e verjaardag van prof. Dr. Jaap van den Herik,* Maastricht: 2007, pp. 132-147.

Schmidt, 2009a
A.H.J. Schmidt, "E-Justisce: No ground for optimism" in: Osterreichische Computer Gesellschaft, *EEeGov Days* 2009.

Schmidt, 2009
A.H.J. Schmidt, Radbruch in cyberspace: about law-system quality and ict innovation, *Masaryk University Journal of Law and Technology,* 2009 Vol. 3:2, p 1-21.

Schreiber e.a., 2000
G. Schreiber e.a. Knowledge engineering and management, London: The MIT Press 2000.

Schermer e.a., 2005
B.W. Schermer, M. Durinck, L. Bijmans, *Juridische aspecten van autonome systemen,* Leidschendam: ECP.nl.

Schermer, 2007
B.W. Schermer, Software agents, and the right to privacy: al legislative framework for agent-enabled surveillance, (diss. Leiden), Leiden: Leiden University Press, 2007.

Schreuders e.a., 2005
E. Schreuders e.a., Evaluatie wet bijzondere politieregisters, 's-Gravenhage: WODC 2005.

Shoham, 1997
Y. Shoham, An overview of Agent-oriented Programming, in *Software Agents,* ed. J.M. Bradshaw, Menlo Park, California.: AAAI Press 1997.

Siemerink, 2007
L.A.R. Siemerink, De overeenkomst van Internet Service Providers met consumenten, (diss.: Leiden), Deventer: Kluwer, 2007.

Smith, 1998
C.E. Smith, *Feit en rechtsnorm,* (diss. Leiden), Maastricht: Shaker Publishing 1998.

Van Straelen, 2002
F.W.M. van Straelen, 'De informant: inwinnen of opsporen' in: B. Andriese, U. van de Pol en J.B.A. de Wit, *Criminele informatie: afscherming of openheid?* Den Haag: Elsevier bedrijfinformatie 2002, p 29-38.

Steffek, 2003
J. Steffek, The Ligitimation of International Governance: A Discourse Approach, *European Journal of International Relations,* 9, p.249-275.

Stolker, 2003
C..J.J.M Stolker, '"Ja, geleerd zijn jullie wel!"; over de status van de rechtswetenschap', *NJB* 2003-15, p. 766 e.v.

Sukthankar en Sycara, 2007
G. Sukthankar and K. Sycara, Policy Recognition for Multi-Player Tactical Scenarios, *Proceedings of the Sixth International Conference on Autonomous Agents and Multi-Agent Systems*, May 2007.

Teepe, 2006
W.G. Teepe, Reconciling Information Exchange and Confidentiality. A Formal Approach, (diss. Groningen) Groningen: December 2006.

Turing, 1950
A. Turing, Computing Machinery and Intelligence, in: R. Epstein, G. Roberts, G. Beber, *Parsing the Turing test : philosophical and methodological issues in the quest for the thinking computer*, Dordrecht: Springer, 2008.

Vanderlooy, 2009
S. Vanderlooy, Ranking and Reliable Classification, (diss: Tilburg), Tilburg 2009.

Vedder e.a., 2007
A.H. Vedder, J.G.L. van der Wees B.J. Koops en P. De Hert, van privacyparadijs tot controlestaat? Misdaad- en terreurbestrijding in Nederland aan het begin van de 21ste eeuw, Den Haag: Rathenau Instituut 2007.

Verbeek, 2004
J.P.G.M. Verbeek, Politie en de nieuwe internationale informatiemarkt, Grensregionale politiële gegevensuitwisseling en digitale expertise, (diss. Maastricht), Den Haag: SDU uitgevers, 2004.

Warren en Brandeis, 1890
S.D. Warren en L.D. Brandeis, *The Right to Privacy,* 4. Harvard Law Review 1890, 193.

Von Wright, 1951
G. von Wright, Deontic Logic, *Mind* 1951, nr. 60.

Wechsler, 1958
D. Wechsler, *The Measurement and Appraisal of Adult Intelligence,* Baltimore: The Williams & Wilkins Company, 1958.

Weizenbaum, 1976
J. Weizenbaum, Computer power and human reason:, From judgement to calculation, San Fransisco: W.H. Freeman, 1976.

Wendt, 2005
J.A.I. Wendt, 'Popper en de rechtswetenschap; kantekeningen bij het huidige debat', *RM Themis* 2005-4.

Wendt, 2008
J.A.I. Wendt, De methode der rechtswetenschap vanuit kritisch-rationeel perspectief (diss: Rotterdam), Zuthpen: Paris, 2008.

Wooldridge, 2002
M. Wooldridge, *An Introduction to Multi-agent Systems,* Chichester: John Wiley & Sons, 2002

Curriculum vitae

Wouter Immánuël Koelewijn is geboren in Baarn op 20 februari 1979. Hij studeerde rechten aan de Universiteit Leiden waar hij zich specialiseerde in het strafrecht en het staats- en bestuursrecht. Vanaf 2004 tot 2007 heeft hij zich voltijds bezig gehouden met zijn promotieonderzoek en was hij tevens als onderzoeker betrokken bij de evaluatie van de Wet bescherming persoonsgegevens. Vanaf 2007 is Wouter als advocaat werkzaam bij Van der Feltz advocaten waar hij adviseert en procedeert op het terrein van privacyrecht, ruimtelijke ordening en vastgoedrecht.

Wouter heeft zijn promotieonderzoek uitgevoerd bij eLaw@Leiden, het centrum voor recht in de informatiemaatschappij en het E.M. Meijers Instituut voor Rechtswetenschappelijk Onderzoek. Via zijn promotor Jaap van den Herik was hij tevens betrokken bij SIKS, de Nederlandse onderzoeksschool voor informatie- en kennissystemen.

SIKS Dissertatiereeks

1998

1 Johan van den Akker (CWI) *DEGAS - An Active, Temporal Database of Autonomous Objects*
2 Floris Wiesman (UM) *Information Retrieval by Graphically Browsing Meta-Information*
3 Ans Steuten (TUD) *A Contribution to the Linguistic Analysis of Business Conversations within the Language/Action Perspective*
4 Dennis Breuker (UM) *Memory versus Search in Games*
5 Eduard W. Oskamp (RUL) *Computerondersteuning bij Straftoemeting*

1999

1 Mark Sloof (VU) *Physiology of Quality Change Modelling; Automated Modelling of Quality Change of Agricultural Products*
2 Rob Potharst (EUR) *Classification using Decision Trees and Neural Nets*
3 Don Beal (UM) *The Nature of Minimax Search*
4 Jacques Penders (UM) *The Practical Art of Moving Physical Objects*
5 Aldo de Moor (KUB) *Empowering Communities: A Method for the Legitimate User-Driven Specification of Network Information Systems*
6 Niek J.E. Wijngaards (VU) *Re-Design of Compositional Systems*
7 David Spelt (UT) *Verification Support for Object Database Design*
8 Jacques H.J. Lenting (UM) *Informed Gambling: Conception and Analysis of a Multi-Agent Mechanism for Discrete Reallocation*

2000

1 Frank Niessink (VU) *Perspectives on Improving Software Maintenance*
2 Koen Holtman (TU/e) *Prototyping of CMS Storage Management*
3 Carolien M.T. Metselaar (UvA) *Sociaal-organisatorische Gevolgen van Kennistechnologie; een Procesbenadering en Actorperspectief*
4 Geert de Haan (VU) *ETAG, A Formal Model of Competence Knowledge for User Interface Design*
5 Ruud van der Pol (UM) *Knowledge-Based Query Formulation in Information Retrieval*
6 Rogier van Eijk (UU) *Programming Languages for Agent Communication*
7 Niels Peek (UU) *Decision-Theoretic Planning of Clinical Patient Management*
8 Veerle Coupé (EUR) *Sensitivity Analysis of Decision-Theoretic Networks*
9 Florian Waas (CWI) *Principles of Probabilistic Query Optimization*
10 Niels Nes (CWI) *Image Database Management System Design Considerations, Algorithms and Architecture*
11 Jonas Karlsson (CWI) *Scalable Distributed Data Structures for Database Management*

2001

1 Silja Renooij (UU) *Qualitative Approaches to Quantifying Probabilistic Networks*
2 Koen Hindriks (UU) *Agent Programming Languages: Programming with Mental Models*
3 Maarten van Someren (UvA) *Learning as Problem Solving*
4 Evgueni Smirnov (UM) *Conjunctive and Disjunctive Version Spaces with Instance-Based Boundary Sets*
5 Jacco van Ossenbruggen (VU) *Processing Structured Hypermedia: A Matter of Style*
6 Martijn van Welie (VU) *Task-Based User Interface Design*
7 Bastiaan Schonhage (VU) *Diva: Architectural Perspectives on Information Visualization*
8 Pascal van Eck (VU) *A Compositional Semantic Structure for Multi-Agent Systems Dynamics*
9 Pieter Jan 't Hoen (RUL) *Towards Distributed Development of Large Object-Oriented Models, Views of Packages as Classes*
10 Maarten Sierhuis (UvA) *Modeling and Simulating Work Practice BRAHMS: a Multiagent Modeling and Simulation Language for Work Practice Analysis and Design*
11 Tom M. van Engers (VU) *Knowledge Management: The Role of Mental Models in Business Systems Design*

2002

1 Nico Lassing (VU) *Architecture-Level Modifiability Analysis*
2 Roelof van Zwol (UT) *Modelling and Searching Web-based Document Collections*
3 Henk Ernst Blok (UT) *Database Optimization Aspects for Information Retrieval*
4 Juan Roberto Castelo Valdueza (UU) *The Discrete Acyclic Digraph Markov Model in Data Mining*
5 Radu Serban (VU) *The Private Cyberspace Modeling Electronic Environments Inhabited by Privacy-Concerned Agents*
6 Laurens Mommers (UL) *Applied Legal Epistemology; Building a Knowledge-based Ontology of the Legal Domain*
7 Peter Boncz (CWI) *Monet: A Next-Generation DBMS Kernel For Query-Intensive Applications*
8 Jaap Gordijn (VU) *Value Based Requirements Engineering: Exploring Innovative E-Commerce Ideas*
9 Willem-Jan van den Heuvel (KUB) *Integrating Modern Business Applications with Objectified Legacy Systems*
10 Brian Sheppard (UM) *Towards Perfect Play of Scrabble*
11 Wouter C.A. Wijngaards (VU) *Agent Based Modelling of Dynamics: Biological and Organisational Applications*
12 Albrecht Schmidt (UvA) *Processing XML in Database Systems*
13 Hongjing Wu (TU/e) *A Reference Architecture for Adaptive Hypermedia Applications*
14 Wieke de Vries (UU) *Agent Interaction: Abstract Approaches to Modelling, Programming and Verifying Multi-Agent Systems*
15 Rik Eshuis (UT) *Semantics and Verification of UML Activity Diagrams for Workflow Modelling*
16 Pieter van Langen (VU) *The Anatomy of Design: Foundations, Models and Applications*
17 Stefan Manegold (UvA) *Understanding, Modeling, and Improving Main-Memory Database Performance*

2003

1 Heiner Stuckenschmidt (VU) *Ontology-Based Information Sharing in Weakly Structured Environments*
2 Jan Broersen (VU) *Modal Action Logics for Reasoning About Reactive Systems*
3 Martijn Schuemie (TUD) *Human-Computer Interaction and Presence in Virtual Reality Exposure Therapy*
4 Milan Petkovic (UT) *Content-Based Video Retrieval Supported by Database Technology*
5 Jos Lehmann (UvA) *Causation in Artificial Intelligence and Law -- A Modelling Approach*
6 Boris van Schooten (UT) *Development and Specification of Virtual Environments*
7 Machiel Jansen (UvA) *Formal Explorations of Knowledge Intensive Tasks*
8 Yong-Ping Ran (UM) *Repair-Based Scheduling*
9 Rens Kortmann (UM) *The Resolution of Visually Guided Behaviour*
10 Andreas Lincke (UT) *Electronic Business Negotiation: Some Experimental Studies on the Interaction between Medium, Innovation Context and Cult*
11 Simon Keizer (UT) *Reasoning under Uncertainty in Natural Language Dialogue using Bayesian Networks*
12 Roeland Ordelman (UT) *Dutch Speech Recognition in Multimedia Information Retrieval*
13 Jeroen Donkers (UM) *Nosce Hostem -- Searching with Opponent Models*
14 Stijn Hoppenbrouwers (KUN) *Freezing Language: Conceptualisation Processes across ICT-Supported Organisations*
15 Mathijs de Weerdt (TUD) *Plan Merging in Multi-Agent Systems*
16 Menzo Windhouwer (CWI) *Feature Grammar Systems - Incremental Maintenance of Indexes to Digital Media Warehouse*
17 David Jansen (UT) *Extensions of Statecharts with Probability, Time, and Stochastic Timing*
18 Levente Kocsis (UM) *Learning Search Decisions*

2004

1 Virginia Dignum (UU) *A Model for Organizational Interaction: Based on Agents, Founded in Logic*
2 Lai Xu (UvT) *Monitoring Multi-party Contracts for E-business*
3 Perry Groot (VU) *A Theoretical and Empirical Analysis of Approximation in Symbolic Problem Solving*

4 Chris van Aart (UvA) *Organizational Principles for Multi-Agent Architectures*
5 Viara Popova (EUR) *Knowledge Discovery and Monotonicity*
6 Bart-Jan Hommes (TUD) *The Evaluation of Business Process Modeling Techniques*
7 Elise Boltjes (UM) *VoorbeeldIG Onderwijs; Voorbeeldgestuurd Onderwijs, een Opstap naar Abstract Denken, vooral voor Meisjes*
8 Joop Verbeek (UM) *Politie en de Nieuwe Internationale Informatiemarkt, Grensregionale Politiele Gegevensuitwisseling en Digitale Expertise*
9 Martin Caminada (VU) *For the Sake of the Argument; Explorations into Argument-based Reasoning*
10 Suzanne Kabel (UvA) *Knowledge-rich Indexing of Learning-objects*
11 Michel Klein (VU) *Change Management for Distributed Ontologies*
12 The Duy Bui (UT) *Creating Emotions and Facial Expressions for Embodied Agents*
13 Wojciech Jamroga (UT) *Using Multiple Models of Reality: On Agents who Know how to Play*
14 Paul Harrenstein (UU) *Logic in Conflict. Logical Explorations in Strategic Equilibrium*
15 Arno Knobbe (UU) *Multi-Relational Data Mining*
16 Federico Divina (VU) *Hybrid Genetic Relational Search for Inductive Learning*
17 Mark Winands (UM) *Informed Search in Complex Games*
18 Vania Bessa Machado (UvA) *Supporting the Construction of Qualitative Knowledge Models*
19 Thijs Westerveld (UT) *Using generative probabilistic models for multimedia retrieval*
20 Madelon Evers Nyenrode *Learning from Design: facilitating multidisciplinary designteams*

2005

1 Floor Verdenius (UvA) *Methodological Aspects of Designing Induction-Based Applications*
2 Erik van der Werf (UM) *AI techniques for the game of Go*
3 Franc Grootjen (RUN) *A Pragmatic Approach to the Conceptualisation of Language*
4 Nirvana Meratnia (UT) *Towards Database Support for Moving Object data*
5 Gabriel Infante-Lopez (UvA) *Two-Level Probabilistic Grammars for Natural Language Parsing*
6 Pieter Spronck (UM) *Adaptive Game AI*
7 Flavius Frasincar (TU/e) *Hypermedia Presentation Generation for Semantic Web Information Systems*
8 Richard Vdovjak (TU/e) *A Model-driven Approach for Building Distributed Ontology-based Web Applications*
9 Jeen Broekstra (VU) *Storage, Querying and Inferencing for Semantic Web Languages*
10 Anders Bouwer (UvA) *Explaining Behaviour: Using Qualitative Simulation in Interactive Learning Environments*
11 Elth Ogston (VU) *Agent Based Matchmaking and Clustering - A Decentralized Approach to Search*
12 Csaba Boer (EUR) *Distributed Simulation in Industry*
13 Fred Hamburg (UL) *Een Computermodel voor het Ondersteunen van Euthanasiebeslissingen*
14 Borys Omelayenko (VU) *Web-Service configuration on the Semantic Web; Exploring how semantics meets pragmatics*
15 Tibor Bosse (VU) *Analysis of the Dynamics of Cognitive Processes*
16 Joris Graaumans (UU) *Usability of XML Query Languages*
17 Boris Shishkov (TUD) *Software Specification Based on Re-usable Business Components*
18 Danielle Sent (UU) *Test-selection strategies for probabilistic networks*
19 Michel van Dartel (UM) *Situated Representation*
20 Cristina Coteanu (UL) *Cyber Consumer Law, State of the Art and Perspectives*
21 Wijnand Derks (UT) *Improving Concurrency and Recovery in Database Systems by Exploiting Application Semantics*

2006

1 Samuil Angelov (TU/e) *Foundations of B2B Electronic Contracting*
2 Cristina Chisalita (VU) *Contextual issues in the design and use of information technology in organizations*
3 Noor Christoph (UvA) *The role of metacognitive skills in learning to solve problems*
4 Marta Sabou (VU) *Building Web Service Ontologies*
5 Cees Pierik (UU) *Validation Techniques for Object-Oriented Proof Outlines*

6 Ziv Baida (VU) *Software-aided Service Bundling - Intelligent Methods & Tools for Graphical Service Modeling*
7 Marko Smiljanic (UT) *XML schema matching -- balancing efficiency and effectiveness by means of clustering*
8 Eelco Herder (UT) *Forward, Back and Home Again - Analyzing User Behavior on the Web*
9 Mohamed Wahdan (UM) *Automatic Formulation of the Auditor's Opinion*
10 Ronny Siebes (VU) *Semantic Routing in Peer-to-Peer Systems*
11 Joeri van Ruth (UT) *Flattening Queries over Nested Data Types*
12 Bert Bongers (VU) *Interactivation - Towards an e-cology of people, our technological environment, and the arts*
13 Henk-Jan Lebbink (UU) *Dialogue and Decision Games for Information Exchanging Agents*
14 Johan Hoorn (VU) *Software Requirements: Update, Upgrade, Redesign - towards a Theory of Requirements Change*
15 Rainer Malik (UU) *CONAN: Text Mining in the Biomedical Domain*
16 Carsten Riggelsen (UU) *Approximation Methods for Efficient Learning of Bayesian Networks*
17 Stacey Nagata (UU) *User Assistance for Multitasking with Interruptions on a Mobile Device*
18 Valentin Zhizhkun (UvA) *Graph transformation for Natural Language Processing*
19 Birna van Riemsdijk (UU) *Cognitive Agent Programming: A Semantic Approach*
20 Marina Velikova (UvT) *Monotone models for prediction in data mining*
21 Bas van Gils (RUN) *Aptness on the Web*
22 Paul de Vrieze (RUN) *Fundaments of Adaptive Personalisation*
23 Ion Juvina (UU) *Development of Cognitive Model for Navigating on the Web*
24 Laura Hollink (VU) *Semantic Annotation for Retrieval of Visual Resources*
25 Madalina Drugan (UU) *Conditional log-likelihood MDL and Evolutionary MCMC*
26 Vojkan Mihajlovic (UT) *Score Region Algebra: A Flexible Framework for Structured Information Retrieval*
27 Stefano Bocconi (CWI) *Vox Populi: generating video documentaries from semantically annotated media repositories*
28 Borkur Sigurbjornsson (UvA) *Focused Information Access using XML Element Retrieval*

2007

1 Kees Leune (UvT) *Access Control and Service-Oriented Architectures}*
2 Wouter Teepe (RUG) *Reconciling Information Exchange and Confidentiality: A Formal Approach*
3 Peter Mika (VU) *Social Networks and the Semantic Web*
4 Jurriaan van Diggelen (UU) *Achieving Semantic Interoperability in Multi-agent Systems: a dialogue-based approach*
5 Bart Schermer (UL) *Software Agents, Surveillance, and the Right to Privacy: a Legislative Framework for Agent-enabled Surveillance*
6 Gilad Mishne (UvA) *Applied Text Analytics for Blogs*
7 Natasa Jovanovic' (UT) *To Whom It May Concern - Addressee Identification in Face-to-Face Meetings*
8 Mark Hoogendoorn (VU) *Modeling of Change in Multi-Agent Organizations*
9 David Mobach (VU) *Agent-Based Mediated Service Negotiation*
10 Huib Aldewereld (UU) *Autonomy vs. Conformity: an Institutional Perspective on Norms and Protocols*
11 Natalia Stash (TU/e) *Incorporating Cognitive/Learning Styles in a General-Purpose Adaptive Hypermedia System*
12 Marcel van Gerven (RUN) *Bayesian Networks for Clinical Decision Support: A Rational Approach to Dynamic Decision-Making under Uncertainty*
13 Rutger Rienks (UT) *Meetings in Smart Environments; Implications of Progressing Technology*
14 Niek Bergboer (UM) *Context-Based Image Analysis*
15 Joyca Lacroix (UM) *NIM: a Situated Computational Memory Model*
16 Davide Grossi (UU) *Designing Invisible Handcuffs. Formal investigations in Institutions and Organizations for Multi-agent Systems*
17 Theodore Charitos (UU) *Reasoning with Dynamic Networks in Practice*

18 Bart Orriens (UvT) *On the development and management of adaptive business collaborations*
19 David Levy (UM) *Intimate relationships with artificial partners*
20 Slinger Jansen (UU) *Customer Configuration Updating in a Software Supply Network*
21 Karianne Vermaas (UU) *Fast diffusion and broadening use: A research on residential adoption and usage of broadband internet in the Netherlands between 2001 and 2005*
22 Zlatko Zlatev (UT) *Goal-oriented design of value and process models from patterns*
23 Peter Barna (TU/e) *Specification of Application Logic in Web Information Systems*
24 Georgina Ramìrez Camps (CWI) *Structural Features in XML Retrieval*
25 Joost Schalken (VU) *Empirical Investigations in Software Process Improvement*

2008

1 Katalin Boer-Sorbàn (EUR) *Agent-Based Simulation of Financial Markets: A modular, continuous-time approach*
2 Alexei Sharpanskykh (VU) *On Computer-Aided Methods for Modeling and Analysis of Organizations*
3 Vera Hollink (UvA) *Optimizing hierarchical menus: a usage-based approach*
4 Ander de Keijzer (UT) *Management of Uncertain Data - towards unattended integration*
5 Bela Mutschler (UT) *Modeling and simulating causal dependencies on process-aware information systems from a cost perspective*
6 Arjen Hommersom (RUN) *On the Application of Formal Methods to Clinical Guidelines, an Artificial Intelligence Perspective*
7 Peter van Rosmalen (OU) *Supporting the tutor in the design and support of adaptive e-learning*
8 Janneke Bolt (UU) *Bayesian Networks: Aspects of Approximate Inference*
9 Christof van Nimwegen (UU) *The paradox of the guided user: assistance can be counter-effective*
10 Wauter Bosma (UT) *Discourse oriented Summarization*
11 Vera Kartseva (VU) *Designing Controls for Network Organizations: a Value-Based Approach*
12 Jozsef Farkas (RUN) *A Semiotically oriented Cognitive Model of Knowlegde Representation*
13 Caterina Carraciolo (UvA) *Topic Driven Access to Scientific Handbooks*
14 Arthur van Bunningen (UT) *Context-Aware Querying; Better Answers with Less Effort*
15 Martijn van Otterlo (UT) *The Logic of Adaptive Behavior: Knowledge Representation and Algorithms for the Markov Decision Process Framework in First-Order Domains*
16 Henriette van Vugt (VU) *Embodied Agents from a User's Perspective*
17 Martin Op't Land (TUD) *Applying Architecture and Ontology to the Splitting and Allying of Enterprises*
18 Guido de Croon (UM) *Adaptive Active Vision*
19 Henning Rode (UT) *From document to entity retrieval: improving precision and performance of focused text search*
20 Rex Arendsen (UvA) *Geen bericht, goed bericht. Een onderzoek naar de effecten van de introductie van elektronisch berichtenverkeer met een overheid op de administratieve lasten van bedrijven*
21 Krisztian Balog (UvA) *People search in the enterprise*
22 Henk Koning (UU) *Communication of IT-architecture*
23 Stefan Visscher (UU) *Bayesian network models for the management of ventilator-associated pneumonia*
24 Zharko Aleksovski (VU) *Using background knowledge in ontology matching*
25 Geert Jonker (UU) *Efficient and Equitable exchange in air traffic management plan repair using spender-signed currency*
26 Marijn Huijbregts (UT) *Segmentation, diarization and speech transcription: surprise data unraveled*
27 Hubert Vogten (OU) *Design and implementation strategies for IMS learning design*
28 Ildiko Flesh (RUN) *On the use of independence relations in Bayesian networks*
29 Dennis Reidsma (UT) *Annotations and subjective machines- Of annotators, embodied agents, users, and other humans*
30 Wouter van Atteveldt (VU) *Semantic network analysis: techniques for extracting, representing and querying media content*
31 Loes Braun (UM) *Pro-active medical information retrieval*

32 Trung B. Hui (UT) *Toward affective dialogue management using partially observable markov decision processes*
33 Frank Terpstra (UvA) *Scientific workflow design; theoretical and practical issues*
34 Jeroen de Knijf (UU) *Studies in Frequent Tree Mining*
35 Benjamin Torben-Nielsen (UvT) *Dendritic morphology: function shapes structure*

2009

1 Rasa Jurgelenaite (RUN) *Symmetric Causal Independence Models*
2 Willem Robert van Hage (VU) *Evaluating Ontology-Alignment Techniques*
3 Hans Stol (UvT) *A Framework for Evidence-based Policy Making Using IT*
4 Josephine Nabukenya (RUN) *Improving the Quality of Organisational Policy Making using Collaboration Engineering*
5 Sietse Overbeek (RUN) *Bridging Supply and Demand for Knowledge Intensive Tasks - Based on Knowledge, Cognition, and Quality*
6 Muhammad Subianto (UU) *Understanding Classification*
7 Ronald Poppe (UT) *Discriminative Vision-Based Recovery and Recognition of Human Motion*
8 Volker Nannen (VU) *Evolutionary Agent-Based Policy Analysis in Dynamic Environments*
9 Benjamin Kanagwa (RUN) *Design, Discovery and Construction of Service-oriented Systems*
10 Jan Wielemaker (UvA) *Logic programming for knowledge-intensive interactive applications*
11 Alexander Boer (UvA) *Legal Theory, Sources of Law & the Semantic Web*
12 Peter Massuthe TU/e, Humboldt-Universtät zu Berlin *Operating Guidelines for Services*
13 Steven de Jong (UM) *Fairness in Multi-Agent Systems*
14 Maksym Korotkiy (VU) *From ontology-enabled services to service-enabled ontologies (making ontologies work in e-science with ONTO-SOA)*
15 Rinke Hoekstra (UvA) *Ontology Representation - Design Patterns and Ontologies that Make Sense*
16 Fritz Reul (UvT) *New Architectures in Computer Chess*
17 Laurens van der Maaten (UvT) *Feature Extraction from Visual Data*
18 Fabian Groffen (CWI) *Armada, An Evolving Database System*
19 Valentin Robu (CWI) *Modeling Preferences, Strategic Reasoning and Collaboration in Agent-Mediated Electronic Markets*
20 Bob van der Vecht (UU) *Adjustable Autonomy: Controling Influences on Decision Making*
21 Stijn Vanderlooy (UM) *Ranking and Reliable Classification*
22 Pavel Serdyukov (UT) *Search For Expertise: Going beyond direct evidence*
23 Peter Hofgesang (VU) *Modelling Web Usage in a Changing Environment*
24 Annerieke Heuvelink (VU) *Cognitive Models for Training Simulations*
25 Alex van Ballegooij (CWI) ``*RAM: Array Database Management through Relational Mapping*''
26 Fernando Koch (UU) *An Agent-Based Model for the Development of Intelligent Mobile Services*
27 Christian Glahn (OU) *Contextual Support of social Engagement and Reflection on the Web*
28 Sander Evers (UT) *Sensor Data Management with Probabilistic Models*
29 Stanislav Pokraev (UT) *Model-Driven Semantic Integration of Service-Oriented Applications*
30 Marcin Zukowski (CWI) *Balancing vectorized query execution with bandwidth-optimized storage*
31 Sofiya Katrenko (UvA) *A Closer Look at Learning Relations from Text*
32 Rik Farenhorst and Remco de Boer (VU) *Architectural Knowledge Management: Supporting Architects and Auditors*
33 Khiet Truong (UT) *How Does Real Affect Affect Affect Recognition In Speech?*
34 Inge van de Weerd (UU) *Advancing in Software Product Management: An Incremental Method Engineering Approach*

In de boekenreeks van het E.M. Meijers Instituut voor Rechtswetenschappelijk Onderzoek van de Faculteit der Rechtsgeleerdheid, Universiteit Leiden, zijn in 2008 en 2009 verschenen:

MI-137 T.C. Leemans, *De toetsing door de bestuursrechter in milieugeschillen. Over rechterlijke toetsingsintensiteit, bestuurlijke beslissingsruimte en deskundigenadvisering* (diss. Leiden), Den Haag: Boom Juridische uitgevers 2008, ISBN 978 90 5454 986 4

MI-138 P. Kuypers, *Forumkeuze in het Nederlands internationaal privaatrecht* (diss. Leiden), Deventer: Kluwer 2008, ISBN 978 90 13 04797 4

MI-139 A. Meuwese, *Impact Assessment in EU Lawmaking* (diss. Leiden), Zutphen: Wöhrmann Printing Service 2008

MI-140 P.C. Adriaanse e.a., *Implementatie van EU-handhavingsvoorschriften*, Den Haag: Boom Juridische uitgevers 2008, ISBN 978 90 5454 862 1

MI-141 S.D. Dikker Hupkes, *What Constitutes Occupation? Israel as the occupying power in the Gaza Strip after the Disengagement,* Leiden: Jongbloed 2008

MI-142 R.A. Visser, E. van Gemerden, P.A. More & R.C.J. de Roon, *Sturing en samenwerking in handhavingsprojecten*, Leiden: Leiden University Press, ISBN 978 90 8728 0383

MI-143 B.M. Dijksterhuis, *Rechters normeren de alimentatiehoogte. Een empirisch onderzoek naar rechterlijke samenwerking in de Werkgroep Alimentatienormen (1975-2007)*, Leiden: Leiden University Press, ISBN 978 90 8728 045 1

MI-144 F.P. Ölçer, *Eerlijk proces en bijzondere opsporing*, Nijmegen: Wolf Legal Publishers 2007, ISBN 978 90 5850 376 3

MI-145 J.H. Crijns, P.P.J. van der Meij & J.M. ten Voorde, *De waarde van waarheid. Opstellen over waarheid en waarheidsvinding in het strafrecht*, Den Haag: Boom Juridische uitgevers 2008, ISBN 978 90 8974 020 5

MI-146 G.K. Schoep, *Straftoemetingsrecht en strafvorming* (diss. Leiden), Deventer: Kluwer 2008, ISBN 978 90 1306 018 8

MI-147 A.R. Spanjer, *Structural and regulatory reform of the European natural gas market – Does the current approach secure the public service obligations?* (diss. Leiden), Amsterdam: Ponsen en Looijen bv, ISBN 978 90 6464 300 2

MI-148 E.-J. Zippro, *Privaatrechtelijke handhaving van mededingingsrecht* (diss. Leiden), Deventer: Kluwer 2008, ISBN 978 90 13 05895 6

MI-149 G. Suurmond, *Enforcing fire safety in the catering industry. An economic analysis*, Leiden: Leiden University Press 2008, ISBN 978 90 8728 061 1

MI-150 J.P. Loof (red.), *Juridische ruimte voor gewetensbezwaren?*, Leiden: NJCM-Boekerij 2008, ISBN 978 90 6750 048 7

MI-151 A.G. Castermans, I.S.J. Houben, K.J.O. Jansen, P. Memelink, J.H. Nieuwenhuis & L. Reurich (red.), *De maatman in het burgerlijk recht*, Deventer: Kluwer 2008, ISBN 978 90 13 05051 6

MI-152 P. Memelink, *De verkeersopvatting* (diss. Leiden), Den Haag: Boom Juridische uitgevers 2009, ISBN 978 90 8974 056 4

MI-153 W. den Ouden, *De terugvordering van Europese subsidies in Nederland: Over legaliteit, rechtszekerheid en het vertrouwensbeginsel*, (oratie Leiden), Kluwer: Alphen aan den Rijn 2008, ISBN 978 90 1306 247 2

MI-154 J. Arnscheidt, *Debating' Nature Conservation: Policy, Law and Practice in Indonesia*, (diss. Leiden), Leiden: Leiden University Press 2009, ISBN 978 90 8728 062 8

MI-155 C. Noichim, *The Asean Space Organization. Legal Aspects and Feasibility*, (diss. Leiden), Leiden: UFB Grafi-Media 2008

MI-156 N.M. Dane, *Overheidsaansprakelijkheid voor schade bij legitiem strafvorderlijk handelen*, (diss. Leiden), Tilburg: Celsus juridische uitgeverij 2009, ISBN 978 90 8863 034 7

MI-157 G.J.M. Verburg, *Vaststelling van smartengeld,* (diss. Leiden), Deventer: Kluwer 2009

MI-158 J. Huang, *Aviation Safety and ICAO*, (diss. Leiden) Montreal 2009

MI-159 J.L.M. Gribnau, A.O. Lubbers & H. Vording (red.), *Terugkoppeling in het belastingrecht*, Amersfoort: Sdu Uitgevers 2008, ISBN 978 90 6476 326 7

MI-160 J.L.M. Gribnau, *Soevereiniteit en legitimiteit: grenzen aan (fiscale) regelgeving*, (oratie Leiden), Sdu Uitgevers 2009, ISBN 978 90 6476 325 0

MI-161 S.J. Schaafsma, *Intellectuele eigendom in het conflictenrecht. De verborgen conflictregel in het beginsel van nationale behandeling*, (diss. Leiden), Deventer: Kluwer 2009, ISBN 978 90 13 06593 0
MI-162 P. van Schijndel, *Identiteitsdiefstal*. Leiden: Jongbloed 2009, ISBN 978 90 70062484
MI-163 W.B. van Bockel, *The* ne bis in idem *principle in EU law,* (diss. Leiden), Amsterdam: Ipskamp Drukkers 2009, ISBN 978 90 9024382 5
MI-164 J. Cartwright, *The English Law of Contract: Time for Review?*, (oratie Leiden)
MI-165 W.I. Koelewijn, *Privacy en politiegegevens. Over geautomatiseerde normatieve informatie-uitwisseling*, (diss. Leiden), Leiden: Leiden University Press, ISBN 978 90 8728070

Zie voor de volledige lijst van publicaties: www.law.leidenuniv.nl/onderzoek