



Universiteit
Leiden
The Netherlands

Politiële gegevensverwerking en Privacy. Naar een effectieve waarborging

Kielman, H.H.

Citation

Kielman, H. H. (2010, April 14). *Politiële gegevensverwerking en Privacy. Naar een effectieve waarborging. Meijers-reeks*. E.M. Meijers Institute for Legal Research, Leiden. Retrieved from <https://hdl.handle.net/1887/15221>

Version: Not Applicable (or Unknown)

License: [Licence agreement concerning inclusion of doctoral thesis in the Institutional Repository of the University of Leiden](#)

Downloaded from: <https://hdl.handle.net/1887/15221>

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

Politiegegevensverwerking en Privacy

Naar een effectieve waarborging

Politiële gegevensverwerking en Privacy

Naar een effectieve waarborging

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,
hoogleraar in de faculteit der Rechtsgeleerdheid,
volgens besluit van het College voor Promoties
te verdedigen op woensdag 14 april 2010
klokke 13.45 uur

door

Hugo Hendrik Kielman

Geboren te Maassluis in 1981

Promotiecommissie:

Promotores: Prof. dr. H.J. van den Herik
Prof. mr. A.H.J. Schmidt

Co-promotor: Dr. L. Mommers

Overige leden: Prof. mr. H. Franken
Prof. mr. A.W. Hins
Prof. dr. J-J.Ch. Meyer (Universiteit Utrecht)
Prof. mr. Th.A. de Roos (Universiteit van Tilburg)
mr. dr. C.N.J. de Vey Mestdagh (Rijksuniversiteit Groningen)
mr. dr. G.J. Zwenne



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. 2010-09
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

© 2010, H.H. Kielman
Geprint door Wöhrmann Print Service

Behoudens de in of krachtens de Auteurswet van 1912 gestelde uitzonderingen mag niets uit deze uitgave worden veeleelvoudigd, 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.
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.

Voorzover het maken van reprografische veeleelvoudingen uit deze uitgave is toegestaan op grond van artikel 16h Auteurswet 1912 dient men de daarvoor wettelijk verschuldigde vergoedingen te voldoen aan de Stichting Reprerecht (Postbus 3060, 2130 KB Hoofddorp, www.reprerecht.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

Dit proefschrift gaat over politieke gegevensverwerking en privacy. Het onderzoek is een onderdeel van een interdisciplinair onderzoek naar de ondersteuning van de uitwisseling van politiegegevens door ICT. De doelstelling van het ANITA-project (Administrative Normative Information Transaction Agents) is het ontwikkelen van een juridisch verantwoorde regulering voor de elektronische uitwisseling van politiegegevens met behulp van agenttechnologie. Het onderhavige onderzoek vormt de juridische component van het ANITA-project en brengt in kaart (1) welke veranderingen de wetgever heeft aangebracht in het normatief kader voor de politieke gegevensverwerking en (2) welke gevolgen dat heeft voor de bescherming van de politietaken en de persoonlijke levenssfeer van betrokkenen. Met dit proefschrift wordt een juridische basis gelegd voor de overige onderzoeken die binnen het ANITA-project zijn uitgevoerd.

Privacy is een inspiratie voor velen. Het misschien wel meest bekende voorbeeld uit de moderne geschiedenis is de film *de Matrix*. De boodschap van de film wordt kernachtig samengevat door bijrolspeler Morpheus met de woorden “What is real. How do you define real?”. Het krachtige beeld van vallende enen en nullen maakt in de film duidelijk dat wij afhankelijk zijn van de computer in plaats van andersom. Zo is het ook met politiegegevens, zij vormen een weerspiegeling van de werkelijkheid die de basis vormt voor veel politieoptredens. Bij het gebruik van die gegevens behoort ook de vraag gesteld te worden wat de waarheid is en hoe je deze uit de beschikbare gegevens destilleert. Inspiratie voor mijn onderzoek is te voorkomen dat we als burger worden onderworpen aan een *politieke Matrix*. Daarbij gaat het allereerst om een zoektocht naar welke grondrechten in het geding komen als politiegegevens worden verwerkt; een eerzame burger heeft toch zeker niets te verbergen. In het verlengde daarvan ligt de vraag welke maatregelen ervoor zorgen dat politiegegevens door de politie zo efficiënt mogelijk worden gebruikt, waarbij tegelijkertijd de grondrechten van de burger in voldoende mate worden gerespecteerd. Deze vraagstukken zijn, als het gaat om de verwerking van politiegegevens, in de afgelopen jaren onderbelicht gebleven. Dit onderzoek maakt duidelijk dat deze onderbelichting onterecht is.

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 (het 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. Het College van procureurs-generaal ben ik ten slotte dank verschuldigd voor hun medewerking.

Hugo H. Kielman
Den Haag, januari 2010

Inhoudsopgave

	VOORWOORD	5
	LIJST VAN GEBRUIKTE AFKORTINGEN	13
	LIJST VAN INGANGSDATA REGELINGEN AANGAANDE POLITIËLE GEGEVENSVERWERKING	15
1	ONDERZOEK EN PROBLEEMSTELLING	17
	1.1 Aanleiding tot het onderzoek	17
	1.1.1 Het gebruik van politiegegevens	18
	1.1.2 Waarborging van de bescherming van de privacy	20
	1.1.3 Waarborging van de politietaak	22
	1.1.4 'Verwerken' is het nieuwe aangrijpingspunt	23
	1.2 Waarborgen voor uitvoering en bescherming	24
	1.2.1 Probleemstelling	24
	1.2.2 OV1: het verwerken van politiegegevens	24
	1.2.3 OV2: knelpunten ten aanzien van de waarborgende werking	25
	1.2.4 OV3: tegemoetkoming in de Wet politiegegevens	25
	1.3 Drie beperkingen van het onderzoek	26
	1.4 De methodologie van het onderzoek	27
	1.4.1 Methoden van analytisch onderzoek	28
	1.4.2 Methoden van verkennend veldwerk	28
	1.5 Plan van behandeling	29
2	CRIMINELE INLICHTINGEN EENHEDEN	31
	2.1 Ontstaansgeschiedenis	31
	2.1.1 De Criminele Inlichtingen Dienst	31
	2.1.2 De Criminele Inlichtingen Eenheid	34
	2.2 De taak van de CIE: informatievoorziening	37
	2.2.1 Het inwinnen van informatie	37
	2.2.2 Het veredelen van informatie	40
	2.2.3 Het verwerken van informatie	42
	2.3 Bevoegdheid tot inwinnen van informatie	43
	2.3.1 Art. 2 Politiewet 1993	43
	2.3.2 Art. 126v Sv	44
	2.4 Organisatorische samenstelling van de CIE	47
	2.4.1 De CIE nationaal gezien	48
	2.4.2 De CIE regionaal gezien	48
	2.5 Hoofdstukconclusie	49

3	BETROKKEN BELANGEN	51
3.1	Instrumentalisme en rechtsbescherming	51
3.1.1	Theorie van het instrumentalisme	52
3.1.2	Theorie van de rechtsbescherming	53
3.1.3	Het spanningsveld tussen instrumentalisme en rechtsbescherming	55
3.2	De Wpolg en instrumentalisme	56
3.2.1	De politietaak	56
3.2.2	Formele verstrekkingen van politiegegevens	58
3.2.3	Informele verstrekkingen van politiegegevens	60
3.2.4	De Wpolg als instrument	61
3.3	De Wpolg en rechtsbescherming	64
3.3.1	De klassieke elementen van het grondrechtelijk privacyrecht	65
3.3.2	Informationele privacy	67
3.3.3	De Wpolg als gegevensbeschermer	71
3.3.4	Meer dan privacy	73
3.4	Internationale en nationale politieke gegevensverwerking	74
3.4.1	Internationale gegevensverwerking	75
3.4.2	Nationale regelgeving	80
3.4.3	Naar een zelfstandig grondrecht?	82
3.5	Gegevensverwerking en technologie	83
3.5.1	Uitbreiding van het gegevensbeschermingsrecht	85
3.5.2	Verschuivingen in het gegevensbeschermingsrecht	86
3.5.3	Technologie stuurt	87
3.6	Beantwoording OV1	89
4	DE WET IN THEORIE EN PRAKTIJK	91
4.1	Drie wettelijke regelingen en hun doelstellingen	91
4.2	Sectorale wetgeving versus omnibuswetgeving	94
4.3	Verschil in wijze van regulering tussen de Wpolr en Wpolg	96
4.4	Driestappenbehandeling	99
4.4.1	De ontwikkeling van het politieke gegevensbeschermingsrecht	100
4.4.2	De inhoud van de stappen	101
4.5	Opslaan	102
4.5.1	Theoretisch kader	102
4.5.2	De knelpunten beschreven	106
4.5.3	Uitwerking onder de Wpolg	109
4.5.4	Tussenconclusie aangaande het opslaan	114
4.6	Bewaren	115
4.6.1	Theoretisch kader	116
4.6.2	De knelpunten beschreven	118
4.6.3	Uitwerking onder de Wpolg	121
4.6.4	Tussenconclusie aangaande het bewaren	125

4.7	Verstrekken	126
4.7.1.	Theoretisch kader	127
4.7.2.	De knelpunten beschreven	131
4.7.3	Uitwerking onder de Wpolg	134
4.7.4	Tussenconclusie aangaande het verstrekken	137
4.8	Koppelen	140
4.8.1	Theoretisch kader	140
4.8.2	De knelpunten beschreven	142
4.8.3	Uitwerking onder de Wpolg	143
4.8.4	Tussenconclusie aangaande het koppelen	144
4.9	Analyseren	145
4.9.1	Theoretisch kader	145
4.9.2	De knelpunten beschreven	146
4.9.3	Uitwerking onder de Wpolg	147
4.9.4	Tussenconclusie aangaande het analyseren	148
4.10	Vergelijking met Wbp	150
4.11	Beantwoording OV2 en OV3 aangaande de wet	151
5	HET KENNISNEMINGSRECHT IN THEORIE EN PRAKTIJK	155
5.1	Theoretisch kader	155
5.1.1	Afhandeling van het kennisnemingsverzoek	157
5.1.2	De wijze van kennisneming	159
5.2	De knelpunten beschreven	160
5.2.1	Het gehonoreerd krijgen van het verzoek	162
5.2.2	Kennisneming van politiegegevens door de rechter	163
5.2.3	Verschil in procedures	165
5.3	Uitwerking onder de Wpolg	166
5.4	Tussenconclusie	167
5.5	Het kennisnemingsrecht ter discussie	168
5.5.1	Zelfreinigend vermogen	170
5.5.2	Mogelijke afschaffing?	170
5.6	Beantwoording OV2 en OV3 aangaande het kennisnemingsrecht	171
6	CONTROLE EN TOEZICHT IN THEORIE EN PRAKTIJK	173
6.1	Controle- en toezichtmechanismen uit de Wpolr	173
6.2	De beheerder	175
6.2.1	Theoretisch kader	175
6.2.2	De knelpunten beschreven	176
6.2.3	Uitwerking onder de Wpolg	178
6.2.4	Tussenconclusie aangaande de beheerder	179
6.3	De privacyfunctionaris	179
6.3.1	Theoretisch kader	180
6.3.2	De knelpunten beschreven	180
6.3.3	Uitwerking onder de Wpolg	181
6.3.4	Tussenconclusie aangaande de privacyfunctionaris	183

6.4	Het College Bescherming Persoonsgegevens	185
6.4.1	Theoretisch kader	185
6.4.2	De knelpunten beschreven	186
6.4.3	Uitwerking onder de Wpolg	188
6.4.4	Tussenconclusie aangaande het College bescherming persoonsgegevens	189
6.5	Protocollering en auditing	190
6.5.1	Theoretisch kader	191
6.5.2	De knelpunten beschreven	192
6.5.3	Uitwerking onder de Wpolg	192
6.5.4	Tussenconclusie aangaande protocollering en auditing	193
6.6	De CIE-officier van justitie	195
6.6.1	Theoretisch kader	196
6.6.2	De knelpunten beschreven	197
6.6.3	Uitwerking onder de Wpolg	198
6.6.4	Tussenconclusie aangaande de CIE-officier van justitie	199
6.7	De strafrechter	200
6.7.1	Theoretisch kader	200
6.7.2	De knelpunten beschreven	201
6.7.3	Uitwerking onder de Wpolg	202
6.7.4	Tussenconclusie aangaande de strafrechter	202
6.8	Beantwoording OV2 en OV3 aangaande controle en toezicht	203
7	CONCLUSIES EN AANBEVELINGEN	205
7.1	De belangen bij politieke gegevensverwerking	205
7.2	Knelpunten aangaande de waarborgende werking van de Wpolr	207
7.2.1	Instrumentele knelpunten	207
7.2.2	Vaagheid in de regelgeving	207
7.2.3	Capaciteitstekort	208
7.2.4	Versnippering	209
7.3	Tegemoetkomingen in de Wpolg	209
7.3.1	Instrumentele knelpunten	210
7.3.2	Vaagheid in de regelgeving	210
7.3.3	Capaciteitstekort	211
7.3.4	Versnippering	212
7.4	Beantwoording probleemstelling	213
7.4.1	De politietaak	213
7.4.2	De grondrechten van de burger	214
7.4.3	Conclusies	215
7.5	Discussie	215
7.5.1	Vaagheid in de regelgeving	216
7.5.2	Capaciteitstekort	217
7.5.3	Versnippering	218

<i>Inhoudsopgave</i>	11
7.6 Aanbevelingen	219
7.6.1 Aan de wetgever	219
7.6.2 Aan politie en justitie	220
7.6.3 Aan de toezichthouders	221
7.7 Slotbeschouwing	221
REFERENTIES	223
SAMENVATTING	231
SUMMARY	237
CURRICULUM VITAE	243
SIKS DISSERTATIEREKS	245
VERSCHENEN IN DE MEIJERS-REEKS	252

Lijst van gebruikte afkortingen

AA	Ars Aequi
ABRIO	Aanpak Bedrijfvoering Recherche Informatiehuishouding en Opleidingen
ABRvS	Afdeling bestuursrechtspraak van de Raad van State
AID	Algemene inspectiedienst
AIVD	Algemene Inlichtingen- en Veiligheidsdienst
AMvB	Algemene Maatregel van Bestuur
ANITA	Administrative Normative Information Transaction Agents
Art.	Art.
Artt.	Artikelen
Awb	Algemene wet bestuursrecht
Bbrp	Besluit beheer regionale politiekorpsen
BIBOB	Bureau Bevordering Integriteitsbeoordelingen door het Openbaar Bestuur
Blz.	Bladzijde
BOB	Bijzondere opsporingsbevoegdheden
Bpolr	Besluit politieregisters
Bpolg	Besluit politiegegevens
CBP	College Bescherming Persoonsgegevens
CID	Criminele Inlichtingen Dienst
CIE	Criminele Inlichtingen Eenheid
Cpa	Centrale personenadministratie
CRI	Centrale Recherche Informatiedienst
CT infobox	Contra Terrorisme infobox
Diss.	Dissertatie
DNRI	Dienst Nationale Recherche Informatie
EG	Europese Gemeenschap
EHRM	Europees Hof voor de Rechten van de Mens
EVRM	Europees Verdrag voor de Rechten van de Mens
EU	Europese Unie
Ex.	Ex ante
FIOD-ECD	Fiscale Inlichtingen- en Opsporingsdienst – Economische Controledienst
fte	full time equivalent
GBA	Gemeentelijke basisadministratie
Gw	Grondwet
HKS	Herkenningsdienstsysteem
HR	Hoge Raad
ICS	Informanten Coderings Systeem
IGO	Informatie Gestuurde Opsporing
IRT	Interregionaal Recherche Team

IVBPR	Internationaal Verdrag inzake Burgerlijke en Politieke Rechten
Jo.	Juncto
KLPD	Korps landelijke politiediensten
KMAR	Koninklijke Marechaussee
LJN	Landelijk Jurisprudentie Nummer
LPC	Landelijk Platform CIE-officieren
MIVD	Militaire Inlichtingen- en Veiligheidsdienst
MOT	Meldpunt Ongebruikelijke Transacties
NCIE	Nationale Criminele Inlichtingen Eenheid
Nr.	Nummer
OM	Openbaar Ministerie
ovj	Officier van Justitie
OV	Onderzoeksvraag
p.	pagina
PbEG	Publicatieblad Europese Gemeenschap
PbEU	Publicatieblad Europese Unie
PEC	Parlementaire Enquete Commissie
PS	Probleemstelling
PSO2	Police Suite Opsporing 2
Pw1993	Politiewet 1993
PZU	Platform Zwacri-Uitwisseling
RDW	(Rijks) Dienst Wegverkeer
RFID	Radio Frequency Identification
RID	Regionale Inlichtingen Dienst
SIOD	Sociale Inlichtingen- en Opsporingsdienst
Sr	Wetboek van Strafrecht
Stcrt.	Staatscourant
Sv	Wetboek van Strafvordering
Trb.	Tractatenblad
VROM-IOD	Inlichtingen- en opsporingsdienst van het ministerie van Volkshuisvesting, Ruimtelijke Ordening en Milieubeheer
VROS	Verwijsindex Recherche Onderzoeken en Subjecten
Vs.	versus
Wbob	Wet bijzondere opsporingsbevoegdheden
Wbp	Wet bescherming persoonsgegevens
Wbpolr	Wet bijzondere politieregisters
Wgba	Wet gemeentelijke basisadministratie
Wiv	Wet op de inlichtingen- en veiligheidsdiensten
Wjs	Wet justitiële en strafvorderlijke gegevens
Wob	Wet openbaarheid van bestuur
WODC	Wetenschappelijk Onderzoek- en Documentatiecentrum
Wpr	Wet persoonsregistraties
Wpolr	Wet politieregisters
Wpolg	Wet politiegegevens
WVW	Wegenverkeerswet 1994
WWW	World Wide Web

Lijst van ingangsdata regelingen aangaande politieke gegevensverwerking

In de onderstaande lijst is een overzicht gegeven van de ingangsdata van de (wettelijke) regelingen die bij de uitvoering van dit onderzoek van belang zijn gebleken. We hebben ervoor gekozen om niet de ingangsdata van alle regelingen weer te geven die sinds de invoering van de Wet politieregisters (Wpolr) zijn ingesteld. Het gaat om de lijn van het betoog. Tevens is dit gedaan ter bevordering van de leesbaarheid van de lijst. Zo is er voor gekozen om de verschillende modelreglementen, die voor de registers bij de CIE-en zijn afgegeven niet te vermelden, evenmin als de diverse instellingsbesluiten van de CIE-en bij de bijzondere opsporingsdiensten.

Datum van inwerkingtreding	Regeling	Vervallen
1 juli 1989	Wet persoonsregistraties (Wpr)	ja
22 juni 1990	Wet politieregisters (Wpolr)	ja
16 februari 1991	Besluit politieregisters (Bpolr)	ja
1 februari 2000	Wet bijzondere politieregisters (Wbpolr)	ja
1 november 2000	Regeling criminele inlichtingen eenheden	–
1 september 2001	Wet bescherming persoonsgegevens (Wbp)	–
14 maart 2002	Toezicht op beheer bijzonder politieregisters	ja
1 maart 2006	Instructie CIE-officier van justitie	ja
1 januari 2008	Besluit politiegegevens (Bpolg)	–
1 januari 2008	Wet politiegegevens (Wpolg)	–
1 maart 2008	Aanwijzing afloopberichten aan verantwoordelijke	–
1 augustus 2008	Aanwijzing Wet politiegegevens	–
1 juli 2009	Instructie controle CIE-gegevensverwerking	–
1 juli 2009	Instructie CIE-officier van justitie	–

Dit proefschrift gaat over politieke gegevensverwerking en privacy. Technologische ontwikkelingen en een toenemend belang dat wordt gehecht aan veiligheid hebben in het laatste decennium onmiskenbaar geleid tot verschuivingen in het privacyrecht. Omdat stringent privacyrecht effectief optreden tegen onder meer terroristen, fraudeurs en veelplegers mogelijk in de weg staat, worden ruimere bevoegdheden tot het gebruik van persoonsgegevens¹ door politie en justitie noodzakelijk geacht. Maar hoe ruim moeten die bevoegdheden zijn? De toegenomen complexiteit van het politiewerk noopt weliswaar aan de ene kant tot een herziening van het huidige regime, met als doel een kwalitatieve verbetering van de gegevensverwerking, maar aan de andere kant doen de ontwikkelingen eveneens de vraag rijzen welke tegenkrachten er zijn om de gegevensverwerking te reguleren en normeren.

De wetgever heeft drie waarborgen geïntroduceerd die ervoor moeten zorgen dat het gebruik van persoonsgegevens plaatsvindt in overeenstemming met de regels en normen uit het wettelijk regime. In dit hoofdstuk worden deze drie waarborgen besproken. De uitkomst van de bespreking vormt de aanleiding voor het onderzoek en de te beantwoorden probleemstelling.

Derhalve is de inhoud van hoofdstuk 1 als volgt. In sectie 1.1 wordt de aanleiding van het onderzoek besproken. Sectie 1.2 bevat de probleemstelling en drie onderzoeksvragen. In sectie 1.3 bespreken we de beperkingen van het onderzoek. De methodologie van het onderzoek is beschreven in sectie 1.4. Sectie 1.5 beschrijft het plan van behandeling.

1.1 AANLEIDING TOT HET ONDERZOEK

Het gebruik van persoonsgegevens levert een belangrijke bijdrage aan (1) de voorkoming en (2) de opsporing van georganiseerde criminaliteit en terrorisme.² In de politiepraktijk maken duizenden politieambtenaren dagelijks gebruik van misschien wel evenzoveel gegevensverzamelingen.³ Een voor-

1 Onder het begrip persoonsgegevens wordt verstaan: "elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon". Art. 1 lid 1 onder i Wpolr jo. Art. 1 onder a Wbp.

2 Zie bijvoorbeeld Corstens, 2008, p. 299.

3 De precieze hoeveelheid databestanden waarin politiegegevens worden verwerkt is onbekend nu registratie daarvan niet verplicht is. Ter illustratie: onder het regime van de Wet politieregisters heeft het Cbp voor 45 politieregisters modelreglementen opgesteld. Iedere politieregio zal minimaal één van deze registers voeren. Daarnaast zijn er registers waarvan iedere regio er meerdere voert. Zo waren er van de tijdelijke registers in 2002 1229 aangemeld bij het Cbp. Schreuders e.a., 2005, p. 88.

beeld van een dergelijke gegevensverzameling is het kentekenregister, dat wordt beheerd door de (Rijks)Dienst Wegverkeer (RDW).⁴ Hierin⁵ wordt onder meer de tenaamstelling opgenomen van een voertuig, dat gekarakteriseerd wordt door het kenteken. Het gebruik biedt een belangrijke ondersteuning voor de politie, met name waar het gaat om de handhaving van de verkeersvoorschriften. De Wet bescherming persoonsgegevens (Wbp), die op dit register van toepassing is, legitimeert de politie om informatie uit dit register te gebruiken.⁶ Wanneer een gegevensverzameling door de politie zelf wordt gevoerd en deze ten dienste staat van de politietaak, dan reguleren en normeren de bepalingen uit de Wet politiegegevens (Wpolg) het gebruik van deze zogenaamde politiegegevens. In subsectie 1.1.1 bespreken we kort het gebruik van politiegegevens. Tot 1 januari 2008 werd het gebruik van politiegegevens gereguleerd en genormeerd door de Wet politieregisters (Wpolr). In de Wet politiegegevens, die vanaf 1 januari 2008 van kracht is, zijn drie waarborgen opgenomen die ervoor moeten zorgen dat deze regels en normen worden nageleefd (subsectie 1.1.2). Vanzelfsprekend moet er ook een waarborging zijn van de politietaak (zie subsectie 1.1.3). Verder stellen we vast dat per 1 januari 2008 in de ontwikkeling van de wetgeving gekozen is voor een nieuw aangrijpingspunt: het verwerken van gegevens (subsectie 1.1.4).

1.1.1 Het gebruik van politiegegevens

In de praktijk maakt de politie gebruik van honderden politieke gegevensverzamelingen. Een bekend voorbeeld van zo'n gegevensverzameling is het Herkenningsdienstsysteem (HKS), waarin voornamelijk verdachtenkenmerken en aangiftegegevens worden opgenomen. Met het opslaan van de modi operandi van verdachten en hun uiterlijke kenmerken worden rechercheurs ondersteund bij de opsporing van verdachten van misdrijven.

Sinds 1990 zijn er regels en normen voor het gebruik van politieke gegevensverzamelingen. Aanvankelijk waren ze opgenomen in de Wpolr; vanaf 1 januari 2008 is de Wpolg van kracht. Het gebruik van politiegegevens⁷

4 Respectievelijk artt. 42–46 WvW en artt. 126–129 WvW. De Wet bescherming persoonsgegevens is op deze registers van toepassing.

5 Art. 42 lid 2 WvW.

6 Art. 9 lid 1 Wbp vereist voor elke verwerking van persoonsgegevens dat dit in overeenstemming is met het doel waarvoor ze zijn verkregen. Gebruik van persoonsgegevens uit het kentekenregister door de politie is toegestaan omdat dit verenigbaar is met het doel waarvoor de gegevens zijn verkregen. Het doel van het kentekenregister is neergelegd in art. 42 lid 3 WvW. De Wbp biedt voorts ruimte voor het gebruik van gegevens buiten de doelbinding van het register waarin deze zijn opgenomen. In art. 43 sub b Wbp wordt de verantwoordelijke van een register toegestaan gegevens te verwerken buiten het doel van het register, indien dit noodzakelijk is in het belang van de voorkoming, opsporing en vervolging van strafbare feiten.

7 Als politiegegeven is in artikel 1 aanhef onder a Wpolg gedefinieerd: “elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon dat in het kader van de uitoefening van de politietaak wordt verwerkt”.

werd door de wetgever dusdanig bijzonder geacht dat er een afzonderlijke wet voor het gebruik van politiegegevens noodzakelijk was.⁸ Hiervoor zijn drie redenen aan te geven. Ten eerste is het soort informatie dat de politie gebruikt van gevoelige aard. Het betreft doorgaans informatie die duidt op enige vorm van betrokkenheid bij criminaliteit. Ten tweede heeft de persoon op wie de politiegegevens betrekking hebben geen toestemming gegeven voor het gebruik van zijn⁹ gegevens, hetgeen bij het gebruik van persoonsgegevens op grond van de Wbp (al dan niet expliciet) veelal wel het geval zal zijn.¹⁰ Ten derde brengt de bijzondere verhouding tussen de overheid en burger met zich mee dat specifieke wetgeving voor het gebruik van politiegegevens wenselijk is. Na de IRT-affaire is aan de Wet politieregisters in 2000 de Wet bijzondere politieregisters toegevoegd (Wbpolr). Immers, in 1996 constateerde de commissie-Van Traa een zodanige wanorde, onder andere met betrekking tot het aantal geregistreerden, dat aanvullende wetgeving over politieel gegevensgebruik noodzakelijk werd geacht.¹¹ De doelstelling van de Wet bijzondere politieregisters was logischerwijs dan ook gericht op een striktere regulering en normering van de door de commissie-Van Traa geconstateerde knelpunten dan voorheen. Met de invoering van de Wet politiegegevens heeft de wetgever tegemoet willen komen aan de knelpunten die bij de uitvoering van de Wet politieregisters en de Wet bijzondere politieregisters naar voren zijn gekomen.

De toepasselijke wet- en regelgeving regelt de belangenafweging tussen de goede uitvoering van de politietaak en het belang van de bescherming van de persoonlijke levenssfeer. De inbreuk op de persoonlijke levenssfeer, door het gebruik van politiegegevens, acht de wetgever gerechtvaardigd zolang deze plaatsvindt binnen de gegeven wettelijke mogelijkheden. Privacy-wetgeving heeft, vanuit de wetgever gezien, geenszins tot doelstelling effectief optreden van de overheid in de weg te staan, maar stelt regels en normen die bepalen welke privacy-inbreuken gerechtvaardigd worden door het nagestreefde doel. Dit brengt met zich mee dat voor ieder afzonderlijk doel een afweging dient te worden gemaakt over welke privacy-inbreuk wel toelaatbaar is en welke privacy-inbreuk niet.

In de Wet politiegegevens is door de wetgever een nieuw evenwicht gezocht in deze afweging. De politie heeft enerzijds meer mogelijkheden gekregen dan louter registratie en verstrekking (eventueel met inbegrip van vergelijking) van persoonsgegevens, anderzijds voorziet de wet in de drie hierna te noemen waarborgen die de bescherming van de persoonlijke

8 *Kamerstukken II*, 1985/86, 19 589, nr. 3, p. 2-4.

9 Korthedshalve schrijven wij in dit proefschrift 'hij' en 'zijn'. Dit dient gelezen te worden als 'hij of zij' en 'zijn of haar'.

10 Art. 8 onder a Wbp eist dat de 'ondubbelzinnige toestemming' van de geregistreerde moet zijn gegeven willen zijn persoonsgegevens mogen worden verwerkt op grond van de Wbp.

11 *Kamerstukken II*, 1995/96, 24 072, nr. 10-11, p. 313.

levenssfeer¹² waarborgen.¹³ Er bestaan, net als onder de Wet politieregisters, drie waarborgen (zie 1.1.2) die ervoor moeten zorgen dat het gebruik van politiegegevens zoveel mogelijk tegemoet komt aan de volgende twee belangen: (A) de goede uitvoering van de politietaak en (B) de bescherming van de persoonlijke levenssfeer. In het vervolg zullen we korthedshalve dan ook spreken over belang A en belang B. De drie waarborgen worden hieronder besproken.

1.1.2 Waarborging van de bescherming van de privacy

Zowel onder het huidige wettelijke regime (Wpolg) als onder het oude regime van de Wet politieregisters (Wpolr) zijn er drie waarborgen voor de bescherming van de persoonlijke levenssfeer. Deze drie waarborgen zijn als volgt opgebouwd.

- (1) **Wet:** de wettelijke beperkingen in het gebruik van persoonsgegevens zelf.
- (2) **Kennisnemingsrecht:** het recht van iedere individuele burger om in beginsel kennis te nemen van de gegevens die over hem zijn opgenomen in een politieregister.
- (3) **Controle en toezicht:** de controle en het toezicht op het gebruik van persoonsgegevens.

Voor een adequate uitvoering van deze drie waarborgen heeft de wetgever een aantal maatregelen geïntroduceerd. Elke waarborg kent zijn eigen specifieke maatregelen.¹⁴ Bij de effectiviteit van deze maatregelen zijn in de loop des tijds in de literatuur (en in de praktijk) vraagtekens geplaatst. Omdat de precieze uitwerking van de Wet politiegegevens eerst in de tweede helft van 2008 onderwerp van publicatie is geworden, richtte de beschikbare literatuur op dit gebied zich voor ons onderzoek met name op de maatregelen zoals deze hun uitwerking hadden onder de Wet politieregisters.

Wat de maatregelen betreft die uitwerking geven aan de eerste waarborg bleek reeds in 1996 en later in 2005 dat bij de politie over het algemeen slechts een beperkt aantal personen op hoofdlijnen bekend is met de regelgeving die op het gebruik van politiegegevens van toepassing is.¹⁵ Met deze constatering lijkt de eerste waarborg niet erg effectief.

De klasse maatregelen van de tweede waarborg lijken even ineffectief. Zo constateerde Van Stratum dat zelfs advocaten nauwelijks op de hoogte

12 In het proefschrift gebruiken we de termen privacy en persoonlijke levenssfeer als synoniemen.

13 *Kamerstukken II*, 2005/06, 30 327, nr. 3, p. 17.

14 De maatregelen die tezamen uitvoering geven aan één waarborg duiden we aan met een klasse maatregelen.

15 Schreuders e.a., 2005, p. 93. Zie voor een soortgelijke conclusie ook Cozijn, 1996, p. 7.

zijn van de mogelijkheden tot een kennisnemingsverzoek.¹⁶ Het relatief geringe aantal kennisnemingsverzoeken blijkt ook uit het WODC-evaluatieonderzoek in 2005.¹⁷ Dit beeld was reeds opgeroepen door Van de Pol. Hij stelde al in 1996 dat het niet veel moeite kostte de politieorganisatie lam te leggen met een kennisnemingsverzoek.¹⁸

Ook had Van de Pol stevige kritiek op maatregelen die uitwerking geven aan de derde waarborg; controle en toezicht. Onder de Wet politieregisters viel dit uiteen in controle en toezicht door (1) het CBP (College bescherming persoonsgegevens) en (2) een privacyfunctionaris. Het CBP is volgens Van de Pol niet in staat adequaat toezicht te houden en komt niet verder dan steekproefsgewijze controle. De privacyfunctionaris lijkt zelfs de formele bevoegdheden te ontberen om adequaat toezicht te kunnen houden op het gebruik van persoonsgegevens.¹⁹ In dit kader moet ook worden gewezen op de in 2002 bij circulaire ingevoerde jaarlijkse zelfevaluatie en de voorgenomen reviews na de eerste zelfevaluatie. Hiermee werd beoogd een kwalitatieve verbetering van het gebruik van politiegegevens te bewerkstelligen.²⁰ Uit het WODC-evaluatierapport lijkt evenwel te kunnen worden opgemaakt dat deze zelfevaluatie pas één keer is uitgevoerd sinds de invoering ervan.²¹ Misschien zijn om deze reden de regels met betrekking tot *auditing* onder de Wet politiegegevens aangescherpt. Voorts zijn er in de loop der jaren andere controle- en toezichtmethoden ingevoerd. Zij hadden evenwel geen expliciete wettelijke grondslag in de Wet politieregisters, maar waren het gevolg van de rechtsstatelijke verhoudingen.²² Voorbeelden hiervan zijn: (1) de rechterlijke controle, zowel nationaal als internationaal, en (2) de verantwoordelijkheid van het Openbaar Ministerie (OM) voor het politieoptreden. Ten aanzien van de rechterlijke controle stelde De Hert dat deze met betrekking tot de bescherming van de persoonlijke levenssfeer tekort schiet.²³ De gezagsverhouding tussen het OM en de politie lijkt in potentie op een effec-

16 Van Stratum, 1999, p. 900-903.

17 Schreuders e.a., 2005, p. 157.

18 Van de Pol, 2002, p. 113.

19 Van de Pol, 2002, p. 113. Het Cbp komt met betrekking tot het concept-wetsvoorstel tot eenzelfde constatering en adviseert de wetgever de privacyfunctionaris dezelfde bevoegdheden te geven als de functionaris gegevensbescherming uit de Wbp. Advies inzake de verwerking van politiegegevens (Wet politiegegevens), advies van 29 maart 2004, Cbp z2004-0467, p. 37-38. Het advies is te downloaden op <http://www.cbpweb.nl>.

20 Circulaire toezicht op beheer bijzondere politieregisters, *Stcrt.* 2002, 51, p. 10-15.

21 De onderzoekers van het evaluatieonderzoek stellen namelijk dat zij bij hun onderzoek gebruik hebben gemaakt van de gehouden zelfevaluaties, maar dat de daarmee verkregen informatie uit 2002 dateert en deze om die reden enigszins gedateerd is. Ondanks dat het rapport in de eerste maanden van 2005 is verschenen, worden de zelfevaluaties die gehouden zouden moeten zijn in de jaren 2003 en 2004 niet besproken of genoemd.

22 De grens hiertussen is niet zo strak te trekken als hier wordt voorgedaan. Zo voorziet art. 23 Wpolr in een verzoekschriftprocedure voor diegene aan wiens kennisneming- (ex. art. 21 Wpolr) of verbeteringverzoek (ex. art. 22 Wpolr) niet door de betreffende beheerder is voldaan.

23 De Hert, 2003, p. 41-54.

tievere uitwerking te kunnen rekenen, bijvoorbeeld door het instellen van een speciale ovj voor Criminele Inlichtingen Eenheden.²⁴ De IRT-affaire heeft ons evenwel geleerd dat het enkele bestaan van een speciale ovj voor CIE-en niet zonder meer resulteert in een effectieve controle en een effectief toezicht door het OM.²⁵

1.1.3 Waarborging van de politietaak

In de wetgeving zijn geen expliciete maatregelen opgenomen die belang A, de goede uitvoering van de politietaak, waarborgen. Wel kan de bevoegdheidstoedeling voor het gebruik van persoonsgegevens op zichzelf als dergelijke maatregel worden aangemerkt. Het is evenwel de vraag of dit de goede uitvoering van de politietaak voldoende waarborgt. Voor deze twijfel zijn drie aanwijzingen. Ten eerste blijkt uit het genoemde Evaluatieonderzoek Wet bijzondere politieregisters dat de ambtenaren van politie veelal niet op de hoogte zijn van de wettelijke regels en normen. Ten tweede doen zich in de praktijk situaties voor waar de politie zichzelf ten onrechte beperkingen oplegt in het gebruik van politiegegevens (zo constateerde de Expertisegroep Privacy van het Instituut voor Criminaliteitsbeheersing en Recherchekunde, dat de wet vaak meer mogelijkheden biedt dan door de praktijk wordt gedacht²⁶). Ten derde kan ook de politiepraktijk belemmerd worden door de wet (het CBP stelt in zijn advies bij het eerste concept van de Wet politiegegevens (toen nog een wetsvoorstel) dat het concept-wetsvoorstel op sommige punten de beoogde 'free flow' van informatie in de weg stond²⁷).

Samenvattend kunnen we stellen dat de toepassing van de regels en normen uit de Wet politieregisters, die de betrokken belangen moesten waarborgen, aan effectiviteit te wensen overliet. Kennelijk bestond er een reeks van knelpunten in de uitvoering van de Wet politieregisters die versturend kon werken op het legitieme evenwicht tussen de uitvoering van de politietaak en het recht op privacy. De vraag rijst nu of met de herziening van het wettelijke regime op een evenwichtige en juiste wijze tegemoet wordt gekomen aan deze knelpunten.

24 Art. 1 onder g CIE-regeling.

25 Een CID-OvJ verklaarde tegenover de commissie-Van Traa geen zicht te hebben op de herkomst van de in de CID-registers opgenomen informatie. Ook verklaarde hij geen inzicht te hebben in de rechtmatigheid van de informatie. *Kamerstukken II*, 1995/96, 24 072, nr. 14, p. 362-363.

26 Rozenbeek, 2003, p. 28-29.

27 CBP, advies conceptwetsvoorstel inzake de verwerking van politiegegevens (Wet politiegegevens), 3 augustus 2004, p. 39. Te downloaden op <http://www.cbpweb.nl>.

1.1.4 ‘Verwerken’ is het nieuwe aangrijpingspunt

Hoewel in de Wet politiegegevens dezelfde drie waarborgen zijn opgenomen als in de Wet politieregisters, is de wijze waarop beide regelingen aan deze waarborgen een invulling geven niet op alle punten gelijk. Daarnaast bestaat er een aanzienlijk verschil in de wijze waarop de Wet politieregisters en de Wet politiegegevens het gebruik van politiegegevens reguleren. De Wet politieregisters gaat uit van een register, waarin gegevens kunnen worden opgeslagen en bewaard en waaruit gegevens kunnen worden verstrekt. Voorts kunnen onder de Wet politieregisters deze verzamelingen van registraties aan elkaar worden gekoppeld en (vervolgens) worden geanalyseerd.

De Wet politiegegevens heeft het registerbegrip losgelaten en gaat uit van het begrip *verwerken* van politiegegevens. Het begrip *verwerken* omvat een *activiteit* met een politiegeven. Hieronder dienen in ieder geval de volgende vijf activiteiten²⁸ te worden begrepen: (1) ‘opslaan’, (2) ‘bewaren’, (3) ‘verstrekken’, (4) ‘koppelen’, en (5) ‘analyseren’²⁹. Er zijn twee uitbreidingen mogelijk: verbreding en verdieping. Verbreding betekent dat het begrip *verwerken* niet tot de genoemde vijf activiteiten beperkt is. Verdieping betekent dat het bereik van een eenmaal gekozen activiteit met politiegegevens onbeperkt is en daardoor onbepaald. Met het begrip verdieping zet de Wet politiegegevens meer dan de Wet politieregisters de deur open voor moderne technieken die meer met gegevens kunnen doen dan menselijke handelingen. Dat is ook een expliciete doelstelling van de wetgever. De ontwikkelingen op het gebied van de informatie- en communicatietechnologie bieden de politie de mogelijkheid hun werk systematischer aan te pakken. Met de centrale positie van het begrip *verwerken* heeft de wetgever aansluiting gezocht bij het systeem van de Wet bescherming persoonsgegevens, dat uitgaat van een techniek-onafhankelijke regulering.³⁰ Door het begrip *verwerken* ruim te definiëren omvat het ook handelingen met politiegegevens die voortkomen uit nieuwe technologische mogelijkheden (om de gedachte te bepalen noemen we hier *datamining* en *machine learning*, twee actuele begrippen in de informatica). Het brengt met zich mee dat de Wet politiegegevens op dit punt meer van de technologische ontwikkelingen afhankelijk is dan de Wet politieregisters. Aangezien het tempo en de richting van deze ontwikkelingen onbekend zijn, is eveneens het bereik van de Wet politiegegevens meer onbepaald dan dat van de Wet politieregisters. De Wet politieregisters staat op dit punt tegenover de Wet politiegegevens als statisch tegenover dynamisch.

28 We geven de voorkeur aan het begrip activiteiten boven het wettelijke begrip handelingen, omdat het begrip handeling te veel aan een menselijke handeling doet denken en het bij het gebruik van politiegegevens juist vooral gaat om activiteiten van computers.

29 In de Wpolr worden (4) en (5) samengenomen als ‘koppelen en analyseren’. In dit proefschrift onderscheiden wij die begrippen als zelfstandige activiteiten.

30 *Kamerstukken II*, 2005/06, 30 327, nr. 3, p. 2-3.

Als we even afzien van de onder de Wet politieregisters geconstateerde knelpunten, dan leidt dit nieuwe dynamische karakter van de Wpolg mogelijk tot nieuwe knelpunten, die we als volgt formuleren. De onbepaalde reikwijdte (of liever diepgang) van de Wet politiegegevens brengt de vraag met zich mee of in de waarborging van belangen A en B kan worden volstaan met dezelfde drie waarborgen als onder de Wet politieregisters. Bij de analyse van de waarborgen alsook in de gehele context van het proefschrift zal daarom het begrip ‘verwerken’ als uitgangspunt worden genomen.

1.2 WAARBORGEN VOOR UITVOERING EN BESCHERMING

In deze sectie formuleren wij de probleemstelling, alsmede drie onderzoeksvragen.

1.2.1 Probleemstelling

In ons onderzoek willen we vaststellen of met de wijziging van het wettelijke regime rond de verwerking van persoonsgegevens door de politie tegemoet is gekomen aan de knelpunten die onder het regime van de Wet politieregisters zijn geconstateerd. Hiermee komen we tot de volgende probleemstelling (PS).

PS: In hoeverre waarborgt de Wet politiegegevens de goede uitvoering van de politietask en de grondrechten van de burger effectiever dan de Wet politieregisters?

Om deze probleemstelling te beantwoorden hebben we drie onderzoeksvragen (OV) geformuleerd. De eerste onderzoeksvraag is gericht op de beschrijving van de twee belangen (A en B) die bij het verwerken van politiegegevens betrokken zijn. In de tweede onderzoeksvraag worden de knelpunten geïnventariseerd die in de literatuur en in de praktijk zijn gerezen rond de toepassing van de Wet politieregisters. De derde onderzoeksvraag ziet op een analyse van de wijze waarop de Wet politiegegevens tegemoet komt aan de bij vraag twee geconstateerde knelpunten.

1.2.2 OV1: het verwerken van politiegegevens

Het verwerken van persoonsgegevens door de politie vindt plaats in het voordurende spanningsveld tussen de goede uitvoering van de politietask en de bescherming van de grondrechten van de burger (belang A tegenover belang B). In essentie komt het belang van de goede uitvoering van de politietask erop neer dat het verwerken van politiegegevens de politie ondersteunt bij de handhaving van de rechtsorde en het verlenen van hulp aan hen die deze behoeven. Daartegenover staat dat het verwerken van per-

soonsgegevens door de politie inbreuk maakt op de grondrechten van de individuele burger. Een dergelijke inbreuk kan worden gerechtvaardigd door de genoemde politietaak. Derhalve luidt onze eerste onderzoeksvraag als volgt.

OV1: *Op welke wijze zijn de politietaak en de grondrechten van de burger betrokken bij het verwerken van politiegegevens?*

Om een gefundeerd antwoord te kunnen geven op de vraag of de Wet politiegegevens de betrokken belangen effectiever waarborgt dan de Wet politieregisters zullen we deze belangen moeten omschrijven. Het gaat hierbij om een onderzoek naar argumenten in (1) de wet, (2) de literatuur, en (3) de jurisprudentie.

1.2.3 OV2: knelpunten ten aanzien van de waarborgende werking

Het onderzoek, zoals geformuleerd in de probleemstelling, vereist een inventarisatie en bespreking van de knelpunten die in de literatuur en in de praktijk zijn geconstateerd ten aanzien van de toepassing van de Wet politieregisters. Het gaat dan om tekortkomingen of verbeterpunten in de wettelijk verplichte en de facultatieve maatregelen die de goede uitvoering van de politietaak en de bescherming van de grondrechten van de burger waarborgen. De tweede onderzoeksvraag luidt derhalve als volgt.

OV2: *Welke knelpunten zijn er in de literatuur en de praktijk geconstateerd ten aanzien van de waarborgende werking van de Wet politieregisters?*

De in sectie 1.1 beschreven drie waarborgen vormen het uitgangspunt bij deze inventarisatie. De knelpunteninventarisatie is gebaseerd op een onderzoek naar argumenten in (1) de wet, (2) de literatuur, (3) de jurisprudentie, en (4) op ons eigen verkennend veldwerk (zie sectie 1.4, methoden van onderzoek).

1.2.4 OV3: tegemoetkoming in de Wet politiegegevens

Na de inventarisatie van de geconstateerde knelpunten via onderzoeksvraag 2 wordt aan de hand van (a) de Wet politiegegevens, (b) de relevante literatuur en (c) de ideeën opgedaan in het verkennend veldwerk (zie sectie 1.4) nagegaan op welke wijze de Wet politiegegevens tegemoet komt aan deze knelpunten. Daarom luidt onderzoeksvraag 3 als volgt.

OV3: *In hoeverre komt de Wet politiegegevens, mede in het licht van de ervaringen met de Wet bescherming persoonsgegevens, tegemoet aan de geconstateerde knelpunten?*

Bij de behandeling van de door de Wet politiegegevens geboden oplossingen zullen ook de reeds opgedane ervaringen met de uitvoering van de Wet bescherming persoonsgegevens worden betrokken. Daarbij zal eveneens aandacht zijn voor de nieuwe technologische ontwikkelingen waarop de Wet politiegegevens anticipeert (denk aan het eerder genoemde *datamining* en *machine learning*). Op die manier kunnen we ons een oordeel vormen over de vraag of de geboden oplossingen daadwerkelijk effect zullen hebben in de praktijk.

Wij denken dat de onderzoeksresultaten die afkomstig zijn van de drie genoemde onderzoeksvragen ons voldoende materiaal zullen bieden om een gefundeerd antwoord te kunnen formuleren op de probleemstelling.

1.3 DRIE BEPERKINGEN VAN HET ONDERZOEK

Het onderzoek kent drie beperkingen. De eerste beperking is ingegeven door de grote omvang van het werkingsgebied van de Wet politiegegevens. Het onderzoek wordt uitgevoerd binnen het ANITA-project, dat staat voor Administrative Normative Information Transaction Agents. Het project is een onderdeel van het ToKeN-programma, deelprogramma politie en justitie (projectnummer: 634.000.017). De doelstelling van het project is het ontwikkelen van juridisch verantwoorde regulering van de elektronische uitwisseling van politiegegevens met behulp van agenttechnologie.³¹ Dit onderzoek vormt de juridische component van het project en brengt in kaart welke veranderingen de wetgever heeft aangebracht in het normatief kader voor de politieke gegevensverwerking en welke gevolgen dat heeft voor de bescherming van de politietaken en de grondrechten van betrokkenen. Zodoende wordt een juridische basis gegeven voor de onderzoeken van de in het ANITA-project deels reeds afgeronde onderzoeken van Teepe³², Aldewereld³³, Dijkstra e.a.,³⁴ en Koelewijn³⁵. In het ANITA-project hebben wij ervoor gekozen het onderzoek te beperken tot de informatieverwerking door Criminele Inlichtingen Eenheden (CIE) op nationaal niveau. De keuze van de beperking is mede bepaald door het feit dat bij de CIE de botsing van de belangen A en B pregnant aanwezig is. De CIE is in een regio belast met de informatievoorziening over georganiseerde of zware criminaliteit.³⁶ Met andere woorden, informatieverwerking is een kerntaak van een CIE. Bovendien merken we op dat, ter ondersteuning van de researchfunctie de CIE veelal zachte, niet bevestigde, informatie verwerkt, die afkomstig is van

31 Zie voor een uitgebreide beschrijving van het project en de diverse deelonderzoeken: Koelewijn, 2009, p. 20-22.

32 Teepe, 2006.

33 Aldewereld, 2007.

34 Dijkstra e.a., 2007.

35 Koelewijn, 2009.

36 Art. 2 CIE-regeling.

informanten. Informatie van informanten is niet alleen bijzonder privacy-gevoelig, maar de taak van de CIE-en brengt volgens de wetgever ook met zich mee dat gegevens over levenswijze, gedragingen en contacten voor een langere periode dienen te worden opgeslagen dan de gewone politieregisters toelaten.³⁷ De gevoeligheid en de kwaliteit van informanteninformatie was dan ook een van de belangrijkste redenen voor de invoering van de Wet bijzondere politieregisters, waarin de regels en normen met betrekking voor gegevensverwerking door de CIE werden aangescherpt.³⁸

De tweede beperking is gelegen in het feit dat het onderzoek zich niet richt op de *vergaring* van gegevens door de politie.³⁹ Centraal staat de *verwerking* van politiegegevens die met behulp van andere bevoegdheden zijn verkregen. Deze beperking zit impliciet in de behandeling van de Wet politieregisters en Wet politiegegevens. Beide regelingen reguleren en normeren niet de vergaring van gegevens, maar alleen de registratie, respectievelijk verwerking van de gegevens die door de inzet van andere bevoegdheden zijn vergaard. De tweede beperking is dus gelegen in het feit dat niet de politieke informatievergaring, maar uitsluitend de politieke informatieverwerking wordt behandeld.

De derde beperking betreft het onder subsectie 1.1.4 besproken dynamische karakter van de Wet politiegegevens. Het dynamische karakter is geen expliciet onderwerp van onderzoek. Dat wil zeggen dat geen aparte onderzoeksvraag aan dat onderwerp is gewijd. Wel wordt aan het verschijnsel – dat vooral gestuurd wordt door de technologische ontwikkelingen – aandacht besteed bij (1) de behandeling van de bij de gegevensverwerking betrokken belangen (OV2, die in hoofdstuk 3 behandeld wordt) en (2) de analyse van de onder de Wet politieregisters geconstateerde knelpunten, alsmede in (3) de beantwoording van de probleemstelling, en (4) de formulering van toekomstig onderzoek.

Naast deze drie expliciete beperkingen aangaande het specifieke onderzoek, hebben we twee beperkingen van algemene aard. De eerste algemene beperking is dat het onderzoek zich niet bezig houdt met specifieke politieke afwegingen. De tweede algemene beperking is erin gelegen dat we geen rekening houden met de invloed van de media.

1.4 DE METHODOLOGIE VAN HET ONDERZOEK

De methodologie van het onderzoek is in beginsel analytisch van aard. Wel wordt de analyse ondersteund door enig eigen veldwerk. In subsectie 1.4.1 wordt de methodologie voor het analytisch onderzoek besproken, in subsectie 1.4.2 die voor het verkennend veldonderzoek.

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

38 Schreuders e.a., 2005, p. 33.

39 De daartoe strekkende bevoegdheden worden voor een goed begrip van de hier behandelde materie kort besproken in sectie 2.3.

1.4.1 Methoden van analytisch onderzoek

Het onderzoek is gebaseerd op vier verschillende juridische onderzoeksbronnen, te weten (1) de parlementaire geschiedenis van de wet, (2) de toepasselijke Europese richtlijnen en daarbij behorende officiële publicaties, (3) de doctrine, en (4) de rechtspraak. De inventarisatie van de knelpunten is primair gebaseerd op de doctrine die aanwezig is op het gebied van de toepassing van privacy- en het gegevensbeschermingsrecht bij de CIE-en. Deze benadering vraagt bijzondere aandacht. Het is immers goed mogelijk dat bepaalde knelpunten in verhouding met de politiepraktijk onevenredig veel aandacht hebben gekregen in de literatuur. Uiteraard kan deze situatie zich ook omgekeerd voordoen. Bepaalde knelpunten kunnen ondervertegenwoordigd zijn in de literatuur of zijn wellicht zelfs helemaal niet beschreven. Met verkennend veldwerk (zie sectie 1.4.2) in de CIE-praktijk is getracht de theoretische knelpuntenanalyse te toetsen aan de praktijk.

1.4.2 Methoden van verkennend veldwerk

Voor een goede analyse van de ons ter beschikking staande informatie hebben wij in de CIE-praktijk aanvullend veldonderzoek uitgevoerd. In deze fase van het onderzoek hebben wij (Koelewijn en Kielman) met vijftien CIE-en van regionale politiekorpsen contact gezocht. Daarvan waren zeven regio's bereid mee te werken aan het onderzoek. Bij elk van die regio's is in samenwerking met Wouter Koelewijn een interview afgenomen. Daarbij is in totaal gesproken met vijf CIE-chefs, drie groepshoofden, twee CIE-rechercheurs en één administrateur.⁴⁰ Verder is gesproken met een privacy-adviseur van de politieacademie, een CIE-officier van justitie en een informatiesysteemspecialist van het Concern Informatiemanagement Politie. Met elk van deze personen is een open vraaggesprek gehouden op basis van een onderwerpenlijst. Bij het opstellen van de onderwerpenlijst is de systematiek van de wet zoveel mogelijk gevolgd. In gespreksvorm zijn voorts de verschillende onderwerpen met de te interviewen persoon behandeld. Daarbij was het doel inzicht te verkrijgen in de wijze waarop de geïnterviewde omgaat met persoonsgegevens. Tijdens de gesprekken zijn aantekeningen gemaakt die direct na het afgenomen interview zijn uitgewerkt door Hugo Kielman. Vervolgens heeft Wouter Koelewijn deze uitwerkingen consistent gemaakt, daar waar nodig. Voorts is het onderzoeksmateriaal geanalyseerd volgens de gefundeerde-theoriebenadering. Dit betekent dat het onderzoeksmateriaal globaal de volgende vier fasen heeft doorlopen: (1) exploratie, (2) specificatie, (3) reductie, en (4) integratie.

40 Het verschil in de genoemde functies en de werkzaamheden die daarbij horen worden in hoofdstuk 2 behandeld.

In de exploratiefase is het onderzoeksmateriaal geordend aan de hand van de belangrijkste begrippen die in de praktijk naar voren zijn gekomen. Vervolgens is in de specificatiefase voor deze centrale begrippen het verschil in benadering door de verschillende geïnterviewden vastgesteld en getracht te benoemen met variabelen. In de reductiefase is daarna op basis van het materiaal getracht een aantal centrale thema's te onderscheiden. In de integratiefase is geprobeerd een verband te leggen tussen de in de voorgaande fasen onderscheiden elementen. Ten slotte is het materiaal en de uitwerking van de analyse, zoals die is opgenomen in het proefschrift, ter validatie voorgelegd aan politie-organisatiedeskundige Johan Oostveen. Hij heeft op basis van het materiaal en de tekst van het proefschrift vastgesteld dat de formuleringen van de binnen de politie geconstateerde knelpunten op juiste wijze zijn weergegeven en dat de conclusies die op basis van dit materiaal getrokken zijn op een juiste wijze zijn geformuleerd. Tot deze manier van validatie is besloten in overleg met Ruud Bik (voorheen hoofdcommissaris politieregio Zuid-Holland-Zuid, vanaf 1 januari 2008 hoofd van de KLPD) en Johan Oostveen.

1.5 PLAN VAN BEHANDELING

In hoofdstuk 1 is de aanleiding tot het onderzoek beschreven, voorts zijn de probleemstelling en onderzoeksvragen OV1 tot en met OV3 geformuleerd, alsmede de methodologie van het onderzoek.

In hoofdstuk 2 wordt een beschrijving gegeven van onderdelen en activiteiten van de CIE, te weten (1) de ontstaansgeschiedenis, (2) de taak van de CIE: informatievoorziening, (3) de bevoegdheden, en (4) de organisatie van de CIE. Na de IRT-affaire is in de oorspronkelijke formulering (door de wetgever) in de punten (2) tot en met (4) een aantal forse veranderingen doorgevoerd. Aan de hand van deze veranderingen wordt de huidige situatie besproken. Hierbij zal de nadruk liggen op de bijzondere opsporingsbevoegdheden uit de Wet BOB, die in de dagelijkse praktijk worden ingezet door een CIE. Tevens is het grensvlak tussen (a) de inzet van deze bevoegdheden en (b) de werkzaamheden, die niet als bijzondere opsporingsbevoegdheid kunnen worden aangemerkt, geduid en beschreven. Hoofdstuk 2 dient als een inleiding op de CIE. Het verschaft daarmee de benodigde basiskennis die de leesbaarheid van de overige hoofdstukken verbetert.

In hoofdstuk 3 wordt een antwoord geformuleerd op OV1. Centraal staat de verhouding tussen de goede uitvoering van de politietaak en het belang van de grondrechten van de burger. Beide belangen worden geraakt door het verwerken van politiegegevens. De inhoud van het begrip 'politietaak' wordt beschreven, waarbij de nadruk is gelegd op de wijze waarop de politietaak gediend is met het verwerken van persoonsgegevens. Voorts wordt besproken op welke wijze afbreuk wordt gedaan aan de grondrechten van de burger door politieke gegevensverwerking. Bij deze bespreking wordt aandacht besteed aan (1) de nationale wetgeving, (2) de rechtspraak

en (3) doctrine, als ook aan (4) de Europese verdragen. Met de bespreking daarvan wordt een theoretisch fundament gelegd voor de beantwoording van de probleemstelling.

Uit de formulering alleen al is duidelijk dat er een sterke samenhang bestaat tussen de OV2 en OV3. Het gaat daar immers om een inventarisatie van de wettelijke knelpunten (OV2) en de daarvoor in de Wet politiegegevens geboden oplossingen (OV3). Bij de beantwoording van OV2 is het goed om de oplossing van OV3 direct te betrekken. De in sectie 1.1.1 genoemde drie waarborgen zullen bij de behandeling leidend zijn. Aan de hand van (1) het wettelijk regime dat ziet op de verwerking van politiegegevens, (2) het kennisnemingsrecht, en (3) controle en toezicht worden in respectievelijk de hoofdstukken 4, 5 en 6 antwoorden gegeven op OV2 en OV3.

In hoofdstuk 4 wordt een antwoord gegeven op OV2 en OV3 voor zover het de wet als waarborg betreft. De knelpunten in het huidige wettelijk regime ten aanzien van de verwerking van persoonsgegevens door de CIE-en worden besproken aan de hand van de vijf verschillende activiteiten (opname, bewaren, verstrekken, koppelen, analyseren). Vervolgens wordt aan de hand van dezelfde activiteiten beschreven op welke wijze de Wet politiegegevens tegemoet komt aan deze knelpunten.

In hoofdstuk 5 wordt een antwoord gegeven op OV2 en OV3 met het kennisnemingsrecht als waarborg. Het wettelijke regime en de daarin geconstateerde knelpunten ten aanzien van het kennisnemingsrecht van de individuele burger worden besproken. De door de Wet politiegegevens geboden oplossingen komen in het tweede deel van het hoofdstuk aan bod.

In hoofdstuk 6 wordt een antwoord gegeven op OV2 en OV3 voor zover het controle en toezicht als waarborg betreft. De knelpunten in de wettelijke controle- en toezichtmaatregelen worden besproken. Het gaat dan bijvoorbeeld om de taken en bevoegdheden van het Cbp en de privacyfunctionaris. Ook wordt in dat kader aandacht besteed aan algemene controle- en toezichtmechanismen, zoals die voortvloeien uit de gezagsverhouding tussen enerzijds OM en politie (waarbij onderscheid kan worden gemaakt tussen de zaaks-ovj en de CIE-ovj) en anderzijds de controlerende functie van de rechterlijke macht. Voorts worden aan de hand van de geïnventariseerde knelpunten de daarvoor door de Wet politiegegevens geboden oplossingen besproken.

Het voorgaande leidt tot een aantal conclusies die in hoofdstuk 7 getrokken worden. Op basis van die conclusies worden aanbevelingen gedaan over de verschuivingen in het systeem van maatregelen die noodzakelijk zijn om politiegegevens effectiever te verwerken dan op dit moment gebeurt, met vanzelfsprekend de inachtneming van de omschreven waarborgen.

In hoofdstuk 1 hebben we de gegevensverwerking door Criminele Inlichtingen Eenheden (CIE-en) centraal gesteld. Derhalve is het belangrijk meer van de CIE af te weten. In dit hoofdstuk wordt een beschrijving gegeven van de werkzaamheden van de CIE. We pogen tevens inzicht te verschaffen in de achtergronden van de werkwijze en de daarbij behorende gebruiken en gewoonten. We hebben er bewust voor gekozen om een dergelijk hoofdstuk in het proefschrift op te nemen, omdat een toegankelijke en actuele beschrijving van de CIE organisatie in de literatuur ontbreekt. Later zal op verschillende plaatsen in dit proefschrift naar teksten in dit hoofdstuk worden terugverwezen.

In sectie 2.1 wordt ingegaan op de ontstaansgeschiedenis van de CIE. In sectie 2.2 behandelen we de taken van de CIE betreffende de informatievoorziening. Daarna beschrijven we in sectie 2.3 de formeel-wettelijke bevoegdheden voor het inwinnen van informatie door middel van informanten. In sectie 2.4 wordt de organisatorische samenstelling van de CIE beschreven. In sectie 2.5 geven we een samenvatting van het hoofdstuk.

2.1 ONTSTAANSGESCHIEDENIS

In 1996, na de IRT-affaire, is de CIE ingesteld als echt onderdeel (eenheid) van ieder regionaal politiekorps. Daarvoor werd het korpsonderdeel aangeduid met Criminele Inlichtingen Dienst (CID). In subsectie 2.1.1 behandelen we de opkomst en taakuitvoering van de CID. In subsectie 2.1.2 beschrijven we de overgang van CID naar CIE.

2.1.1 De Criminele Inlichtingen Dienst

De CID is ontstaan naar aanleiding van ontwikkelingen die zich in de jaren zestig (van de vorige eeuw) in de criminaliteit voordeden. Het kenmerk van die periode is dat bepaalde vormen van criminaliteit zich naar een meer georganiseerde vorm ontwikkelden; dat gebeurde bijvoorbeeld in de drugs-handel. De politie had zich tot dan toe weinig bezig gehouden met wat later pro-actieve opsporing is gaan heten. Bij pro-actieve opsporing gaat het kort-

41 Een deel van dit hoofdstuk is reeds gepubliceerd in Koelewijn en Kielman, 2006. De auteur bedankt hierbij zijn co-auteur en de uitgever voor hun toestemming om relevante gedeelten van het artikel in dit proefschrift te mogen hergebruiken.

weg om het vroegtijdig in kaart brengen van criminele activiteiten en organisaties.⁴² Pas nadat de greep op dergelijke vormen van criminaliteit onmogelijk leek te worden, ontstond het besef dat een goede informatiepositie bij de politie kon leiden tot een effectievere opsporing en tot voorkoming van misdrijven. Daarmee werd het inwinnen van informatie over criminele groeperingen en gedragingen via burgerinformanten (ook wel criminele inlichtingen genoemd) langzaam onderdeel van het politiewerk. Het inlichtingenwerk bij de politie ontstond doordat rechercheurs contact bleven houden met voormalige verdachten. Zo trachtten zij een informatiepositie te verkrijgen over het criminele circuit. Deze manier van werken leek resultaten op te leveren en nam daardoor snel een structurele vorm aan. Het inwinnen van inlichtingen bij burgers over het reilen en zeilen in de onderwereld werd aangeduid met het 'runnen' van informanten. Het inlichtingenwerk werd daarbij onder meer ondersteund door observatieteams. Deze observerende werkzaamheden werden uiteindelijk bij een aantal grotere korpsen organisatorisch ondergebracht bij de CID.

De werkwijze van de CID

De ondernomen pogingen tot het verkrijgen van inzicht in de onderwereld waren, hoewel succesvol, toch onvoldoende om een fundamenteel inzicht in de onderwereld te verkrijgen. De onderwereld bleef zich daardoor voor een groot deel nog steeds onttrekken aan het gezichtsveld van de politie. De oorzaak werd vooral gezocht in een te gefragmenteerde opzet van het politiële inlichtingenwerk. Voor de bestrijding van ernstige vormen van criminaliteit was een betere inpassing van de CID in de politieorganisatie nodig.⁴³ Hoewel een concept-regeling voor de CID in 1981 gereed was, heeft het toch nog tot 1986 geduurd voordat deze, tezamen met een privacyreglement, werd ingevoerd.⁴⁴ In 1987 kregen de CID-en een formele status in de Politiewet. Bij ieder politiekorps werd officieel een CID opgericht. Ondertussen waren er ook verschillende richtlijnen en instructies uitgevaardigd die onder meer voor de CID-en golden.⁴⁵ Er kwam met genoemde wijzigingen een striktere scheiding tussen het klassieke researchewerk en het inlichtingenwerk van de CID. Het opbouwen van een informatiepositie kwam in een ontwikkelingsfase en professionaliseerde daardoor sterk. De CID werkte daarbij echter voornamelijk regionaal. Iedere regionale CID was verantwoordelijk voor de informatiepositie in zijn regio en had daarvoor ook de beschikking over een eigen observatieteam. Een centrale rol bij het inlichtingenwerk was weggelegd voor de Centrale Recherche Informatiedienst (CRI). Zij waren verantwoordelijk voor de ondersteuning van de regionale diensten en hadden in dat kader onder meer tot taak het constateren van verbanden tussen de ver-

⁴² Zie uitgebreider subsectie 2.2.1.

⁴³ Brief van de minister van binnenlandse zaken, 12 juni 1981, kenmerk _EA80/u1496, betreffende de concept-regeling criminele inlichtingendiensten.

⁴⁴ *Stcrt.* 29 mei 1986.

⁴⁵ Regeling bijzonder opsporingsgelden, *Stcrt.* 2006, nr. 39.

schillende regionale criminele inlichtingen en het onderhouden van contacten daarover met de verschillende regio's. Niettemin liet die informatieuitwisseling te wensen over. De afstemming tussen verschillende CID-en onderling en de verschillende rechercheafdelingen verliep stroef. Een van de oorzaken daarvoor was te vinden in slecht op elkaar afgestemde informatie-huishoudingen.⁴⁶

De groei van de CID

De invulling van de taak van de CID-en verschilde per regio aanzienlijk. In een "terughoudende" regio was de taak van een CID beperkt tot de afscherming van informanten. In een "vooruitstrevende" regio gingen de taken van een CID verder en werd alle informatie opgeslagen in de registers voorzover deze zag op vormen van ernstige criminaliteit.⁴⁷ De vooruitstrevende CID-en groeiden uit tot een zelfstandig opsporingsinstituut, dat onafhankelijk van de reguliere recherche opereerde. De verregaande mogelijkheden tot afscherming bij de CID maakte deze daarmee een veilige haven voor speciale onderzoeken of voor het toepassen van speciale onderzoeksmethoden. De CID stond tot het midden van de jaren negentig binnen de politieorganisatie dan ook bekend als de "afdeling stiekem". De afstand in werkwijze tussen de CID en die van de recherche werd groter. Waar in het begin het gezamenlijke doel was de opsporing van zware criminaliteit, won bij de CID de bronbescherming aan terrein. Afscherming van de bron werd hoe langer hoe meer leidend bij de CID. Dit werd gezien als een noodzakelijke voorwaarde voor het verkrijgen van een goede informatiepositie. Het leidde echter tot een praktijk waarin onderzoeksresultaten via een U-bocht constructie werden ontdaan van procedurele vereisten.⁴⁸ In een dergelijke constructie worden "gewone" onderzoeksresultaten via de CID in het dossier gebracht zodat vragen over bijvoorbeeld de herkomst van die gegevens kunnen worden ontweken met een beroep op de bronbescherming. De rechter bood ruimte aan deze gang van zaken door het stellen van vragen over de bronbescherming te beletten, omdat:

*"bij de beantwoording van deze vragen de effectiviteit van de opsporing van dit soort zaken, welke het welzijn van de maatschappij in hoge mate bedreigen, ernstig wordt geschaad en de veiligheid van de informant en mogelijk andere bij de opsporing betrokkenen wordt bedreigd"*⁴⁹

Ook onder het Europees Verdrag voor de Rechten van de Mens (EVRM) wordt het afschermen van bronnen toegestaan. Zo stelt het Europees Hof voor de Rechten van de Mens (EHRM) in de op dit punt nog altijd actuele

⁴⁶ Koelewijn, 2009, p. 100.

⁴⁷ Onderzoek naar het functioneren van de RCID Kennemerland, rijksrecherche Fort-team, subsectie 2.1.3.

⁴⁸ Onderzoek naar het functioneren van de RCID Kennemerland, rijksrecherche Fort-team, subsectie 2.1.4.

⁴⁹ HR 5 oktober 1982, NJ 1983 / 297 m.nt. AC'tH.

zaak Kostovski zich op het standpunt dat er in de opsporingsfase gebruik kan worden gemaakt van informanten.

“The Convention does not preclude reliance, at the investigation stage of criminal proceedings, on sources such as anonymous informants.”⁵⁰

Het ontbreken van controle

Controle op de CID-praktijk van de jaren tachtig was er dan ook vrijwel niet. Zelfs het hoofd van de CID was niet altijd op de hoogte van de handel en wandel van zijn eigen medewerkers. Gegeven deze vrijheid ontwikkelde de CID zich tot een instantie die zelfstandig opsporingsonderzoeken uitvoerde. Dat heeft uiteindelijk bijgedragen aan het ontstaan van een crisis in de opsporing. De Parlementaire Enquête Commissie (PEC) constateerde een enorme wanorde die was te wijten aan (1) het ontbreken van formele wetgeving en (2) een gebrek aan toezicht en controle. Het aantal geregistreerden in de CID-registers was groeiende. Voorts was het onduidelijk welke opsporingsmethoden werden gebruikt voor de opsporing van de georganiseerde criminaliteit en wie daar controle op uitvoerden. Leden van de CID hadden binnen de politieke taakomschrijving vrij spel. Officieren van justitie gaven te kennen nauwelijks zicht te hebben op hetgeen zich bij de CID-en afspeelde. Het rapport van de PEC was aanleiding voor een reorganisatie van de CID-organisatie. Daarbij is ook ingegrepen in het regime rond de gegevensverwerking door de CID.

2.1.2 De Criminele Inlichtingen Eenheid

Na de bevindingen van de PEC in 1996 is er veel veranderd in de organisatie van de CID. Het meest opvallend is de naamswijziging; de CID werd omgedoopt tot de Criminele Inlichtingen Eenheid (CIE). Naast de naamswijziging werden de taken en bevoegdheden van de CIE expliciet wettelijk genormeerd. Dat gebeurde in navolging van de conclusies van de PEC, waarvan we er, in het kader van dit proefschrift, vijf aanstippen.

Ten eerste concludeerde de PEC dat er ten aanzien van de politieke gegevensverwerking sprake was van een gebrekkige controle en toezicht. De PEC was van oordeel dat noch de burgemeester, noch het OM beschikte over voldoende bevoegdheden om adequaat toezicht te houden op de door de CID gevoerde registers. Ten tweede was volgens de PEC (1) het aantal geregistreerden te groot en (2) het criterium op basis waarvan geregistreerd werd te vaag. Het vage criterium voor de selectie van personen van wie gegevens mochten worden geregistreerd en gebruikt, alsmede een gebrek aan controle daarop had tot een forse groei van het aantal geregistreerde personen bij de CID geleid. Ten derde was er tussen de verschillende CID-en een verschil

50 EHRM 20 november 1989, Kostovski vs. The Netherlands, 11454/85, overw. 44.

waarneembaar in de soort en hoeveelheid gegevens die over een subject (een persoon die voor registratie in aanmerking komt) werden geregistreerd. Ten vierde was de manier waarop informatie werd verstrekt ondoorzichtig en op sommige punten zelfs in strijd met de wet. Ten vijfde werd het kennisnemingsrecht door de burgers weinig gebruikt.⁵¹

De geconstateerde aandacht- en knelpunten hebben geleid tot een aantal wetswijzigingen die in de Wpolr zijn opgenomen bij de inwerkingtreding van de Wet bijzondere politieregisters (Wbpolr). Het doel van de Wbpolr was een stringenter regime in te voeren voor de verwerking van criminele inlichtingen.⁵² Als uitgangspunt werd daarbij gesteld (met kracht van wet) dat de taak van de CIE is beperkt tot de informatievoorziening over zware criminaliteit ten dienste van de recherchefunctie. Het herziene regime van de Wpolr is onderwerp van hoofdstuk 4, en wordt daar uitgebreid behandeld. In deze subsectie is volstaan met een globale beschrijving om inzicht te geven in de ontwikkelingen die zich de afgelopen jaren hebben voorgedaan. In hoofdstuk 4 zullen de hedendaagse ontwikkelingen worden behandeld (Wpolg) en op verschillende momenten parallellen worden getrokken met de hier omschreven ontwikkelingen.

Wet bijzondere politieregisters

De invoering van de Wet bijzondere politieregisters (Wbpolr) betrof – aangaande de CIE – feitelijk de toevoeging aan de Wet politieregisters van een expliciete wettelijke regeling voor het register zware criminaliteit en voor het voorlopig register. Daarmee werd voor deze registers bij de CIE aan de invoerkant een strikt criterium ingevoerd met als doel het aantal geregistreerde personen bij de CIE terug te dringen. Het criterium werd neergelegd in art. 13a Wpolr, en is in de Wpolg gehandhaafd. Of informatie voor registratie in aanmerking kwam werd bepaald door het type strafbaar feit waar de informatie betrekking op had en de mate van betrokkenheid van de genoemde persoon. Het criterium wordt aangeduid met het CIE-criterium en wordt uitgebreid in hoofdstuk 4 behandeld. Aan de uitvoerkant werd getracht het aantal geregistreerden terug te dringen door de registers van de CIE te voorzien van bewaartermijnen. Voorts werd vanwege de gevoeligheid en onbetrouwbaarheid van de informatie een meer gesloten verstrekingsregime voor de CIE-registers ingevoerd.

Naast de Wbpolr werden ook twee vormen van lagere regelingen ingevoerd. Zij beoogden de gegevensverwerking door CIE-en onder de Wet politieregisters strikter te reguleren. Het gaat om (1) de Circulaire bijzondere politieregisters en (2) de diverse modelreglementen voor de verschillende bijzondere registers. We behandelen beide hieronder.

⁵¹ *Kamerstukken II*, 1995/96, 24 072, nr. 14, sectie 8.6.

⁵² De Wet bijzondere politieregisters heeft ook gevolgen gehad voor de registers die bij de recherche afdelingen van de verschillende korpsen worden gevoerd. Gezien de beperkingen van dit onderzoek blijven deze echter buiten beschouwing.

Ad (1) De Circulaire bijzondere politieregisters⁵³ vroeg specifiek aandacht voor de noodzakelijke maatregelen naar aanleiding van de wijziging van de Wpolr. Er wordt aangegeven wat er veranderd is naar aanleiding van de wetswijziging. Dit betreft zowel de inhoud als het beheer van de verschillende registers bij de CIE. Twee elementen waren daarbij van belang. Ten eerste is dat de uitvoering van de reglementplicht. Ten tweede gaat het om uitvoering geven aan de primaire doelstelling van de Wbpolr: het terugdringen van het aantal geregistreerden.

Ad (2) Voor de registers die gevoerd worden bij de CIE (terzijde: alsmede voor een ander register) is met de Wbpolr een reglementsplicht ingevoerd. Art. 12 lid 1 van de Wpolr maakte het mogelijk, omwille van de eenduidigheid en de efficiëntie, modelreglementen vast te stellen voor een bepaald register. Dit is voor de registers bij de CIE gebeurd (zie subsectie 2.2.3). De Registratiekamer, de voorloper van het CBP, heeft hieraan zijn goedkeuring verleend in 2000.⁵⁴ Inhoudelijk zijn de modelreglementen een uitwerking van de normen uit de Wet bijzondere politieregisters en het Besluit politieregisters. Ze worden in hoofdstuk 4 uitgebreid behandeld.

Algemeen regelgevend kader

Naast de specifieke regelingen voor gegevensverwerking die van toepassing waren op de informatieverwerking zijn CIE-en vanzelfsprekend ook gehouden aan de algemene regelgevende kaders. Daarbij moet gedacht worden aan de Politiewet 1993 (Pw1993) en het Wetboek van Strafvordering (Sv). In subsectie 2.3.2 wordt de inzet van bijzondere opsporingsbevoegdheden door de CIE behandeld. In de uitwerking van de Pw1993 werd de formele instelling van de regionale CIE-en geregeld in het Besluit beheer regionale politiekorpsen (Bbrp). Art. 5 lid 1 Bbrp bepaalde dat iedere regio moest beschikken over een eenheid die belast was met de informatievoorziening omtrent de misdrijven die in aanmerking komen voor registratie in het register zware criminaliteit, ten behoeve van de recherchefunctie van die regio.

In 2000 is de Regeling criminele inlichtingen eenheden van kracht geworden.⁵⁵ De gevolgen van de commissie-Van Traa waren inmiddels verwerkt in de verschillende regelingen, zoals de Wbpolr en de hierboven behandelde regelingen. Daarmee kreeg het CIE-takenpakket en de invulling daarvan vast omlijnde vormen. Met de CIE-regeling werd een nadere invulling gegeven aan die taken en bevoegdheden. Daarmee werd bedoeld aan te sluiten bij het striktere regime rond de gegevensverwerking door de CIE. Hierdoor werd onder meer de wijze van samenwerking tussen de verschillende CIE-en en de Nationale CIE (NCIE) geregeld. De nadruk lag daarbij op de uitwisseling van informatie. Ook werd aandacht besteed aan de interne werking van de CIE, specifiek aan de wijze waarop controle en toezicht intern

53 Circulaire bijzondere politieregisters, *Stcrt.* 1999, 221.

54 Verklaring van overeenstemming inzake modelreglementen, *Stcrt.* 2000, 198.

55 *Stcrt.* 2000, 198.

vorm worden gegeven en de wijze waarop met informatie diende te worden omgegaan. Er was voor gekozen om, anders dan in de CID-regeling 1995, geen privacyregelingen in de CIE-regeling op te nemen. In de CIE-regeling was daarover slechts opgenomen dat gegevens in overeenstemming met het regime van de Wpolr, het Besluit politieregisters en de modelreglementen dienden te worden verwerkt.

In de toelichting op de CIE-regeling werd tevens de toepassing van het audit-mechanisme besproken als instrument om toezicht te houden op de bijzondere politieregisters door de korpsbeheerder.⁵⁶ Het toezicht op de verwerking van persoonsgegevens was, waar het gaat om het beheer van de politieregisters, verder uitgewerkt in de circulaire Toezicht op beheer bijzondere politieregisters.⁵⁷ Het was ontwikkeld om intern de kwaliteit en de kwantiteit van de gegevens te kunnen beoordelen en bestond uit twee onderdelen. Ten eerste was er een jaarlijkse zelfevaluatie op basis van een vragenformulier. Ten tweede zou er iedere vier jaar een onafhankelijke externe audit zijn. De zelfevaluatie had tot doel een bewustwording bij de CIE-en te creëren en zodoende een kwaliteitsverbetering te bewerkstelligen. Het instrument van auditing wordt uitgebreid behandeld in hoofdstuk 6.

2.2 DE TAAK VAN DE CIE: INFORMATIEVOORZIENING

De taak van de CIE is in de herstructurering beperkt tot de informatievoorziening van de recherchefunctie. We onderscheiden daarbij drie processen: (1) het inwinnen van informatie, (2) het veredelen van informatie, en (3) het verwerken van informatie. We behandelen deze processen in drie subsecties hieronder om inzicht te geven in de dagelijkse werkzaamheden van de CIE en de positie die de gegevensverwerking inneemt binnen die werkzaamheden.

2.2.1 Het inwinnen van informatie

De kerntaak van de hedendaagse CIE is het inwinnen van voor de opsporing relevante informatie over zware criminaliteit. Het inwinnen van informatie is het verkrijgen van informatie die voldoet aan de wettelijke verwerkingsvereisten voor de CIE (het CIE-criterium). Kenmerkend voor de CIE is dat de informatie-inwinning vooral ziet op de pro-actieve fase. Dat is de onderzoeksfase waarin informatie wordt verzameld om (1) een algemeen inzicht te verkrijgen in het fenomeen zware criminaliteit en (2) vast te kunnen stellen of er ten aanzien van een bepaalde persoon of groepering een onderzoek kan worden gestart.⁵⁸ Er kunnen dus ook gegevens worden verkregen over

56 *Stcrt.* 2000, 198, p. 15.

57 Circulaire Toezicht op beheer bijzondere politieregisters, *Stcrt.* 2002, 51.

58 *Kamerstukken II*, 1994/95, 23 945, nr. 1.

personen ten aanzien van wie nog geen verdenking bestaat in de zin van art. 27 Sv. Op het moment dat informatie een persoon betreft van wie wordt vermoed dat deze betrokken is bij zware criminaliteit, komt die informatie in aanmerking voor verwerking door de CIE. De mate van betrokkenheid van de betreffende persoon en het soort delict waarvoor een vermoeden bestaat zijn uiteindelijk bepalend voor de vraag of tot registratie mag worden overgegaan. De gronden voor opslag van informatie (het CIE-criterium) worden uitgebreid in hoofdstuk 4 behandeld. Hier wordt volstaan met een beschrijving van de verschillende wijzen waarop informatie kan worden ingewonnen door de CIE.

Er zijn voor de CIE twee typen van informatie om in te winnen: (1) *broninformatie* en (2) *informanteninformatie*. We behandelen beide typen hieronder.

Ad (1) Broninformatie

Bij het inwinnen van informatie uit reeds aanwezige informatie (politieel of niet) maken we onderscheid tussen drie soorten bronnen, (a) openbare bronnen, (b) politiebronnen die openbaar zijn voor iedere politieambtenaar, en (c) politiebronnen die niet openbaar zijn voor iedere politieambtenaar.

Ad (a) Bij de bronnen die een ieder ander ook ter beschikking staan kan gedacht worden aan openbare bronnen, zoals het telefoonboek alsmede aan het verkrijgen van een gegevensbron door de aankoop van gegevens bij een handelsinformatiebureau. Wij duiden dit aan als particuliere broninformatie.

Ad (b) Bronnen die aan iedere politieambtenaar ter beschikking staan, zowel binnen de politie als bij de overheid in bredere zin, bevatten gegevens die voor de politie direct raadpleegbaar zijn. Deze bronnen kunnen voor een politieagent als openbare bronnen worden beschouwd. Het gaat dan bijvoorbeeld om de registraties die plaatsvinden in de Gemeentelijke Basisadministratie (GBA) en het kentekenregister van de RDW. Wij duiden deze bronnen aan als openbare politieke broninformatie.

Ad (c) De CIE kan gebruik maken van bronnen die niet voor iedere politieambtenaar beschikbaar zijn, meestal ook niet voor de CIE. Zij kan op verzoek daar echter wel specifieke gegevens uit verstrekt krijgen of in sommige gevallen zelfs tijdelijke toegang tot het register verkrijgen. Bij dergelijke bronnen moet gedacht worden aan de registraties van gevoelige gegevens die binnen de politieorganisatie worden verwerkt. Dit gebeurt bijvoorbeeld door de Regionale Inlichtingen Dienst (RID), Recherche teams die een specifiek opsporingsonderzoek uitvoeren en collega CIE-en. Wij duiden dit aan als gesloten politieke broninformatie.

Uit ons veldonderzoek is gebleken dat de CIE in deze drie vormen van informatievergaring een groeiend belang ziet. Vooral het inwinnen van informatie uit afgesloten rechercheonderzoeken kan voor een CIE waardevol zijn, maar toch is ook die informatie niet optimaal. Dit is voor een belangrijk deel te wijten aan (i) een gesloten cultuur en (ii) slecht op elkaar afgestemde informatiesystemen. Daardoor kost het de CIE veel inspanning

relevantie informatie uit de verschillende registers naar boven te halen. Het wekt geen verbazing dat er meer nuttige informatie in de verschillende registers aanwezig is dan dat er capaciteit is om deze informatie te classificeren en uit de informatiesystemen te destilleren.⁵⁹ Daarnaast constateerden we een toenemende aandacht voor de private bronnen. Het 'iemand even googelen' krijgt ook bij de CIE-en voet aan de grond.

De CIE heeft geen specifieke bevoegdheden voor de inwinning van broninformatie gekregen. Zij kan derhalve alleen over de informatie beschikken, voor zover dit is toegestaan in de regeling die op de betreffende bron van toepassing is. Voor een particuliere informatiebron zal die regeling veelal de Wet bescherming persoonsgegevens (Wbp) zijn. Wat betreft de openbare en gesloten politie-informatie kan de CIE de daarin opgenomen informatie gebruiken wanneer zij tot ontvangst daarvan gerechtigd is door de Wet politiegegevens.

Ad (2) Informanteninformatie

Naast het inwinnen van informatie door het zoeken in reeds bestaande registraties heeft de CIE ook de mogelijkheid zelfstandig informatie te verkrijgen door de inzet van (opsporings)bevoegdheden. Dit gebeurt thans voornamelijk door het zogenaamd runnen van informanten. Onder het begrip 'runnen' wordt verstaan het overdragen door de informant van de bij hem beschikbare kennis van een criminele activiteit, persoon of organisatie aan een medewerker van de CIE. De persoon over wie informatie wordt verschaft, wordt aangeduid als het 'subject'. De informant beschikt dus over bepaalde informatie van een strafbaar feit dat gepleegd is, gepleegd wordt of gepleegd gaat worden. De informant heeft over het algemeen enige vorm van betrokkenheid bij het misdrijf dat in de informatie wordt genoemd. In de minst verwijtbare vorm is die betrokkenheid beperkt tot het enkel kennis hebben van het misdrijf. Het gaat dan vaak om informatie 'van horen zeggen' of om bijvoorbeeld een familielid van het subject. In de meest verwijtbare vorm strekt de betrokkenheid zich echter uit tot het in strafrechtelijke zin (mede)plegen van een misdrijf. Het aandeel criminelen loopt in sommige informantenbestanden op tot tussen de 80 en 100%.⁶⁰ Het meest recente en sprekende voorbeeld van het inwinnen van informatie door gebruikmaking van een informant zijn de 'Endstra-tapes'.⁶¹ Endstra gaf op de achterbank van een rondrijdende auto van de CIE Amsterdam informatie aan de CIE-rechercheurs over verschillende criminele activiteiten, personen en organisaties.

Over de reikwijdte van het begrip informant bestonden verschillende benaderingen. Zowel vroeger – in het modelreglement van het register zware criminaliteit – als tegenwoordig – in de regeling criminele inlichtingen

59 Koelwijn, 2009, p. 137.

60 Van der Bel e.a., 2007, p. 102.

61 Na het uitlekken zijn de Endstra tapes uitgegeven in boekvorm: Middelburg en Vugts, 2006.

eenheden – wordt een informant omschreven als een persoon die informatie verschaft aan een opsporingsambtenaar, niet zijnde een getuige of verdachte.⁶² In het modelreglement van het informantenregister is evenwel niet uitgesloten dat een informant en een verdachte eenzelfde persoon zijn.⁶³ In de CIE-praktijk is het echter een vast gebruik dat een informant niet meer gerund wordt zodra deze als verdachte wordt aangemerkt. Thans is een informant in art. 12 lid 7 Wpolg als volgt gedefinieerd:

“persoon die heimelijk aan een opsporingsambtenaar informatie verstrekt omtrent strafbare feiten of ernstige schendingen van de openbare orde, die door anderen zijn of worden gepleegd of verricht, welke verstrekking gevaar voor deze persoon of voor derden oplevert” (art. 12 lid 7 Wpolg).

De bevoegdheden tot het inwinnen van informanteninformatie komen in sectie 2.3 aan de orde.

2.2.2 Het veredelen van informatie

De ingewonnen informatie dient na binnenkomst te worden beoordeeld op haar juistheid en volledigheid. Dit proces wordt aangeduid met het ‘veredelen’ van informatie. De verplichting hiertoe vloeit voort uit art. 4 Wpolg. Pas indien de ingewonnen informatie is veredeld, is deze geschikt voor verwerking in de registratiesystemen van de CIE.

Of broninformatie op juistheid en volledigheid dient te worden gecontroleerd, hangt af van de registratie vanwaaruit de informatie afkomstig is. Indien informatie uit het GBA wordt verkregen, kan deze in beginsel als juist en volledig worden aangemerkt. Een dergelijke bron kan worden geclassificeerd als een objectieve bron. Is informatie echter afkomstig van een nieuwsgroep op het internet, dan kan van die objectiviteit niet uit worden gegaan. Informatie afkomstig van dergelijke media, waarop over het algemeen vrijelijk kan worden gepubliceerd, wordt door het medium zelf of een andere instantie niet of nauwelijks gecontroleerd op juistheid en volledigheid. Publicatie van onwaarheden of publicaties namens een andere persoon zijn dan ook mogelijk. Er is bij deze vormen van broninformatie dan ook sprake van een subjectieve bron.

Informanteninformatie is per definitie subjectief. De informatie die informanten verschaffen is namelijk altijd in bepaalde mate gekleurd door de informant zelf. Dat kan verschillende oorzaken hebben. Zo kan het bij informatie ‘van-horen-zeggen’ voorkomen dat de informant de context van het vernomene niet kent, waardoor de informatie een andere betekenis krijgt. Ook heeft een informant vaak een eigen belang bij het geven van informatie.

62 Art. 1 onder h modelreglement zwacri-register en respectievelijk art. 1 sub d CIE-regeling.

63 Art. 1 onder e modelreglement informantenregister.

Het gebeurt bijvoorbeeld dat een criminele organisatie valse informatie geeft aan een van haar leden om op die manier te toetsen of deze persoon een lek vormt binnen de organisatie. Daarnaast blijkt uit ons veldwerk dat CIE-rechercheurs vooral op hun hoede zijn voor informanten die een collega een hak willen zetten of de aandacht van hun eigen criminele activiteiten willen afleiden door informatie te geven over een andere criminele activiteit die tegelijkertijd plaatsvindt. Ten slotte is het ook niet ongebruikelijk dat informanten voor het geven van informatie een geldelijke beloning krijgen. Het gaat in het algemeen om een paar honderd euro. In de Regeling bijzondere opsporingsgelden zijn beleidsregels neergelegd over de afhandeling van de beloning.⁶⁴ Zo moet de Officier van Justitie voor iedere vergoeding zijn toestemming geven.

Wijze van veredeling

Bij het gebruik van subjectieve bronnen, zowel afkomstig van broninformatie als ook van informanteninformatie, dient de CIE zelf een oordeel te vormen over de *juistheid* en *volledigheid* van de daaruit ingewonnen informatie. De juistheid zegt iets over de correctheid van de verschaft informatie. Volledigheid⁶⁵ gaat om de hoeveelheid relevante informatie die niet verschaft is in verhouding tot de informatie die wel verschaft is. Voor beide factoren zijn geen criteria vastgesteld aan de hand waarvan dit kan worden bepaald. De wetgever heeft aangegeven de invulling hiervan ook aan de praktijk te willen overlaten.⁶⁶ Wat we vaak zien is het volgende: het

*“wordt [...] opgelost in het hoofd van de runners”.*⁶⁷

In het verkennend veldwerk (zie 1.4.2.) zijn echter wel terugkerende factoren gesignaleerd die door de CIE-rechercheurs worden gebruikt om de juistheid en volledigheid van de informatie bevestigd te krijgen. Daartoe wordt bijvoorbeeld actief informatie bij andere informanten uitgezet. Verkregen informatie wordt vergeleken met informatie uit andere raadpleegbare bronnen, zoals het GBA. In het kader van de veredeling van informatie kan dus worden overgegaan tot het opnieuw inwinnen van informatie met gebruikmaking van de in dat kader toegekende bevoegdheden.

Daarnaast speelt bij de veredeling van informatie ook de intuïtie van de betreffende CIE-er een rol. Het verloop van het gesprek is bijvoorbeeld een indicator die daarop van invloed kan zijn. De prominente rol van de intuïtie bij de beoordeling van de ingewonnen informatie is een belangrijke reden voor de gangbare praktijk bij de CIE-en om informanten uitsluitend in twee-

⁶⁴ Stcrt. 2001, 54.

⁶⁵ De wet spreekt van nauwkeurigheid, maar wij geven de voorkeur aan de term volledigheid.

⁶⁶ Staatsblad 2007, nr. 550, p. 27.

⁶⁷ Buruma, 2002, p. 91.

tallen te runnen. De gedachte is dat dit de objectiviteit bij de beoordeling van de juistheid en volledigheid vergroot.

Voorts speelt bij de beoordeling van de juistheid en volledigheid van de ingewonnen informatie de betrouwbaarheid van de informant een belangrijke rol. Het gaat dan niet om het beoordelen van de ingewonnen informatie op juistheid en volledigheid, maar om op basis van in het verleden gegeven informatie de kans in te schatten dat de informant ook dit keer juiste en volledige informatie heeft geleverd. De informant die reeds negen keer, naar achteraf bleek, kloppende informatie heeft geleverd, zal de tiende keer sneller als betrouwbaar worden aangemerkt.⁶⁸

Het moge duidelijk zijn dat met deze werkwijze geen zekerheid te geven valt omtrent de juistheid en de volledigheid van subjectieve informatie. Vanwege deze onmogelijkheid wordt deze informatie in de literatuur en de praktijk ook wel aangeduid met de term 'zachte informatie'.⁶⁹

2.2.3 Het verwerken van informatie

Met het verwerken van informatie wordt onder meer bedoeld het (1) opslaan, (2) bewaren, (3) verstrekken, (4) koppelen, en (5) analyseren van de betreffende informatie. Feitelijk wordt de verkregen informatie na veredeling in een aantal registers van de CIE geregistreerd en indien mogelijk uitgezet bij een researcheteam, een collega-CIE, of een andere verstrekkingsgerechtigde.⁷⁰ De betrokkenheid van de informant brengt met zich mee dat aan de verwerking van de ingewonnen informatie risico's zijn verbonden. In dat verband wordt gesproken van zogenaamde afbreukrisico's of herleidbaarheid van de informatie. Veruit het grootste afbreukrisico is het gevaar dat een informant of een derde loopt door het afgeven van informatie aan de CIE. Verwerking van informanteninformatie kan bij diegene die daarmee geconfronteerd wordt, voldoende reden zijn om te concluderen dat bepaalde personen niet te vertrouwen zijn. We geven een eenvoudig fictief voorbeeld. Wapenhandelaar Laurens M. vertelt alleen aan zijn doorgaans betrouwbare handlanger (Hugo K.) in welke loods hij een nieuwe lading wapens heeft opgeslagen. De volgende dag valt de politie die loods binnen, neemt de wapens in beslag en arresteert Laurens M. Deze zal onmiddellijk Hugo K. verdenken als verklikker en mogelijk maatregelen tegen hem nemen. In het ergste geval wordt daarbij gebruik gemaakt van geweld.

Het voorbeeld laat zien dat het operationeel gebruiken van de inlichtingen ernstige gevolgen kan hebben voor de informant en daarmee ook voor de toekomstige informatiepositie van een CIE. Vanzelfsprekend zullen na een dergelijk voorval informanten minder snel geneigd zijn om informatie met de

68 Buruma, 2002, p. 91.

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

70 Koelewijn, 2009, p. 107-114.

CIE te delen vanwege de angst dat daarmee onzorgvuldig wordt omgegaan. Het minimaliseren van de afbreukrisico's heeft dan ook prioriteit nummer één bij de CIE. De CIE-ers ervaren bronbescherming als hun belangrijkste taak.

Dit brengt gezien hun wettelijke taak (informatievoorziening van de recherchefunctie) met zich mee dat er bij de verwerking van politiegegevens sprake is van een voortdurende afweging tussen beschermingsbelangen en opsporingsbelangen. Illustratief voor dit 'duivelse dilemma' is een uitspraak die een CIE-chef deed in een van de interviews die wij hebben afgenomen:

"Een aantal moordzaken kunnen eenvoudig worden opgelost. Maar dan liggen een week later wel de betreffende informanten in de goot".⁷¹

Onder de Wet politieregisters waren bij de verwerking van politiegegevens drie registers van belang: (1) het informantenregister, (2) het voorlopig register, en (3) het register zware criminaliteit. Onder de Wet politiegegevens worden de toepasselijke regels en normen bepaald door het doel van de verwerking (we spreken niet langer over registers als aangrijpingspunt). De Wpolg kent voor de CIE twee typen verwerking: (1) de verwerking van informatie over informanten en (2) de zwacri-verwerking. In dit hoofdstuk zullen de bevoegdheden voor informatieverwerking niet aan de orde komen; dit is het onderwerp van hoofdstuk 4.

2.3 BEVOEGDHEID TOT INWINNEN VAN INFORMATIE

Voor de verkrijging van informatie maakt de CIE gebruik van twee bevoegdheden. Ten eerste gaat het om de bevoegdheidstoedeling in art. 2 Politiewet. Deze wordt in subsectie 2.3.1 behandeld. Ten tweede gaat het om de opsporingsbevoegdheid in art. 126sv SV, welke in subsectie 2.3.2 wordt behandeld. Hoewel de vergaring van informatie niet het kernonderwerp is van dit proefschrift (maar de verwerking van informatie, zie sectie 1.3) wordt hieronder toch kort aandacht besteed aan deze twee bevoegdheden, omdat daarmee inzicht wordt gegeven in de herkomst van de informatie, hetgeen bij de verwerking van de informatie van belang is.

2.3.1 Art. 2 Politiewet 1993

Niet iedere handeling van een politieambtenaar is neergelegd in een aparte wettelijke regeling. Eenvoudige opsporingshandelingen die een geringe grondrechtelijke inbreuk tot gevolg hebben, kunnen worden teruggevoerd op de algemene taakomschrijving van de politie in art. 2 Pw1993. Zo kennen we bijvoorbeeld geen specifieke bevoegdheidstoedeling voor het in

71 Koelewijn en Kielman, 2006, p. 231-255.

het openbaar fotograferen⁷² en observeren en schaduwen⁷³ van personen. De Hoge Raad formuleerde dit als volgt:

“de politie [is] ingevolge art. 2 Politiewet 1993 bevoegd [...] in de proactieve fase handelingen te verrichten welke de in die bepaling aan haar opgedragen taak meebrengt, en dat ook indien door zulke verrichtingen een beperkte inbreuk op de persoonlijke levenssfeer zou worden gemaakt, de globale taakomschrijving van art. 2 Politiewet 1993 daarvoor een toereikende wettelijke grondslag biedt.”⁷⁴

In beginsel worden de informanten van de CIE gerund onder de algemene bevoegdheid van art. 2 Pw1993. Zoals opgemerkt in subsectie 2.1.1, staat ook het EVRM een dergelijke grondslag niet in de weg. Wanneer het runnen van informanten echter stelselmatige vormen aanneemt, ontstaat dergelijk handelen het kader van art. 2 Politiewet en moet de uitoefening van die bevoegdheid als bijzondere opsporingsbevoegdheid worden aangemerkt. In art. 126v Sv is het stelselmatig inwinnen van informatie door middel van een burgerinformant als bijzondere opsporingsbevoegdheid geregeld.

2.3.2 Art. 126v Sv

Het stelselmatig inwinnen van informatie door gebruikmaking van een burgerinformant is een bijzondere opsporingsbevoegdheid onder de Wet bijzondere opsporingsbevoegdheden (Wbob). Het stelselmatig inwinnen van informatie, waarbij een compleet beeld wordt verkregen van het subject, werd geacht niet zonder specifieke wettelijke grondslag te kunnen worden ingezet door de politie. De stelselmatigheid brengt met zich mee dat de inbreuk op de persoonlijke levenssfeer daarvoor te groot is. De grens tussen het runnen van informanten onder de bevoegdheid van art. 2 Politiewet enerzijds en onder de bevoegdheid van art. 126v Sv anderzijds wordt dus gevormd door de stelselmatigheid van het inwinnen. Er zijn echter geen uniforme criteria die bepalen wanneer het runnen van een informant de bevoegdheid van art. 2 Politiewet ontstaat en stelselmatige vormen aanneemt. Ook in de rechtspraak zijn geen uniforme criteria ontwikkeld die bepalen wanneer er sprake is van het stelselmatig inwinnen van informatie. De zaken waarin deze kwestie met betrekking tot de informatieverwerking door CIE-en speelde zijn er enkele.

In de literatuur wordt wel aansluiting gezocht bij het leerstuk van de stelselmatige observatie, dat in de memorie van toelichting op de Wbob en rechtspraak wel verder is ingevuld. Deze aansluiting stuit echter op de nodige kritiek, omdat blijkens de memorie de wetgever bij het inwinnen van informatie een striktere vorm van stelselmatigheid voor ogen had dan bij de

⁷² HR 13 oktober 1992, NJ 1993, 223.

⁷³ HR 14 oktober 1986, NJ 1987, 564 en HR 14 oktober 1986, NJ 1988, 511.

⁷⁴ HR 19 december 1995, NJ 1996, 249 (Zwolsman-arrest).

observatie.⁷⁵ De minister van Justitie stelt echter dat (1) het verzoek dat gericht is aan een informant en (2) de verwachting dat met de terugkoppeling een min of meer volledig beeld van het subject kan worden verkregen leidend zouden moeten zijn in de bepaling van de stelselmatigheid.⁷⁶

De mening van praktijkdeskundigen

Ook zijn er praktijkdeskundigen die stellen dat er sprake is van stelselmatigheid zodra de ingewonnen informatie te veel het privé-leven van de betrokken persoon betreedt. De vraag is dan echter wanneer 'te veel' van het privé-leven wordt blootgelegd. We beschouwen hieronder de mening van twee praktijkdeskundigen, te weten Van Straelen en Corstens. In de weinige literatuur die hierover beschikbaar is, stelt Van Straelen dat daarbij rekening moet worden gehouden met (1) de aard van de ingewonnen informatie, (2) de verwachtingen die de betrokkene mag hebben rond de bescherming van zijn persoonlijke levenssfeer, en (3) de indringendheid van het inlichtingenproces.⁷⁷ Zo kan iemand die betrokken is bij georganiseerde drugshandel verwachten dat hij zal worden geobserveerd en dat er informatie over hem wordt ingewonnen. Zolang het inwinnen van die informatie voornamelijk ziet op het 'professionele' leven van die persoon zou dat niet als stelselmatig dienen te worden aangemerkt. Van Straelen is daarnaast van mening dat een informant die op eigen initiatief contact heeft gezocht met de politie, nooit stelselmatig in de zin van art. 126v Sv kan worden gerund.⁷⁸ Pas als de politie de informant zelf heeft verzocht om op een stelselmatische wijze aanvullende informatie te vergaren zou er sprake zijn van het gebruik van de art. 126v-informant. Corstens stelt evenwel dat indien permanent en langdurig gebruik wordt gemaakt van een bepaalde informant de contacten dusdanig indringend zijn dat dit leidt tot het stelselmatig inwinnen van informatie. Dat het initiatief van dat contact enkel bij de informant ligt, doet daar volgens hem niet altijd aan af.⁷⁹ Ook lijkt er sprake te kunnen zijn van stelselmatische inwinning indien een volledig beeld van het privéleven kan worden verkregen met gebruikmaking van meerdere informanten.⁸⁰

De praktijk

In de praktijk worden twee benaderingen gehanteerd: (1) in hoeverre de politie sturend is geweest bij het handelen van de informant en (2) de mate waarin het optreden van een informant inbreuk heeft gemaakt op het privé-leven van het subject.⁸¹ Deze twee benaderingen zijn echter door de CIE-en zelf bedacht. De twee in de praktijk ontwikkelde criteria komen in hoge mate

75 Beijer e.a., 2004, p. 93-94.

76 Minister van Justitie, Brief aan de TK, 22 mei 2001, kenmerk 5095838/01/6.

77 Van Straelen, 2002, p. 34-35.

78 Van Straelen, 2002, p. 36.

79 Corstens, 2008, p. 460.

80 *Kamerstukken II*, 2001/02, 26 269, nr. 41.

81 Beijer e.a., 2004, p. 90.

overeen met het uitgangspunt uit het handboek voor de opsporingspraktijk, dat in dit geval op 1 januari 2008 in werking is getreden.

Volgens het handboek voor de opsporingspraktijk zijn twee factoren van belang bij de bepaling of de inwinning van informatie van een burgerinformant stelselmatig is. Ten eerste, de vraag of er actieve bemoeienis is van de politie in de informatievergaring. Ten tweede, of de burgerinformant zich begeeft in de omgeving waar degene over wie wordt geïnformeerd mag verwachten onbevange zichzelf te kunnen zijn. Pas als van beide omstandigheden sprake is, dient er volgens het handboek in beginsel een bevel ex. art. 126v Sv te worden afgegeven. Bijzondere omstandigheden kunnen ertoe leiden dat ook in een geval waar niet direct aan de twee voorwaarden is voldaan, toch een bevel dient te worden afgegeven.⁸² Dit zou betekenen dat het veredelen van informatie via informanten die zich in de persoonlijke sfeer van een subject begeven (bijvoorbeeld de vrouw of vriendin van een subject) een vorm van stelselmatig inwinnen is. Ook is in het handboek voor de opsporingspraktijk opgenomen dat het begrip stelselmatigheid in het geval van art. 126v niet met de stelselmatische observatie vergeleken kan worden.⁸³

Strafvorderlijke waarborgen

De consequentie van het stelselmatig inwinnen van informatie is dat de inzet ervan de toepasselijkheid van een reeks strafvorderlijke waarborgen met zich meebrengt. Elke bijzondere opsporingsbevoegdheid wordt daarmee omkleed. De wijze van bewijsverzameling moet namelijk achteraf voor de rechter inzichtelijk kunnen worden gemaakt. De strafvorderlijke waarborgen worden bepaald door een stelsel van maatregelen die de openbaarheid en de controleerbaarheid van de inzet van deze middelen garanderen (let op, dit zijn strafvorderlijke waarborgen, geen waarborgen uit de Wet politiegegevens). Bij de inzet van het stelselmatig inwinnen van informatie dient bijvoorbeeld een proces-verbaal van bevindingen te worden opgemaakt.⁸⁴ Tevens dient, ten behoeve van de transparantie van de inzet van de opsporingsbevoegdheid, een contract te worden opgesteld waarin de rechten en plichten van de informant worden uiteengezet. Het mag duidelijk zijn dat een dergelijke openbaarheid en controleerbaarheid op gespannen voet staat met de afbreukrisico's die verbonden zijn aan de informatie afkomstig van de informant, zoals beschreven is in subsectie 2.2.1.⁸⁵

De taak van de CIE brengt in de praktijk met zich mee dat in beginsel geen gebruik wordt gemaakt van bijzondere opsporingsbevoegdheden. De CIE plaatst geen telefoontaps en doet geen huiszoekingen. Het verzamelen en verspreiden van inlichtingen door de CIE is dan ook uitdrukkelijk niet

82 Handboek voor de opsporingspraktijk, 13^e aanvulling op de Aanwijzing opsporingsbevoegdheden, *Stcrt*, 13 december 2007, nr. 239, p.11.

83 Handboek voor de opsporingspraktijk, 13^e aanvulling op de Aanwijzing opsporingsbevoegdheden, *Stcrt*, 13 december 2007, nr. 239, p.11.

84 Zie de artt. 152 en 153 Sv.

85 Van der Bel e.a., 2007, p. 102-108.

bedoeld om te fungeren als bewijs in een individuele strafzaak. Van Straelen stelt om die reden dat de CIE geen gebruik zou moeten maken van het stelselmatig inwinnen van informatie. De openheid die verbonden is aan het verkrijgen van bewijs, past niet bij de werkwijze van de CIE, waar geheimhouding van de identiteit van de informant centraal staat.⁸⁶ In het evaluatierapport Wet bijzondere opsporingsbevoegdheden is dit aangemerkt als de reden voor het niet gebruiken van de 126v-bevoegdheid in de praktijk. Er wordt eerder gekozen voor een terughoudend optreden door de CIE zodat de grens van de art. 2-informant niet wordt overschreden. De definitie van stelselmatigheid wordt daarbij ontleend aan de jurisprudentie rond de stelselmatische observatie, ondanks het feit dat die vergelijking volgens sommigen, zoals hierboven is beschreven, niet correct is.

Het voorgaande maakt in ieder geval duidelijk dat het inwinnen van informatie door middel van informanten de grenzen van de bevoegdheid uit art. 2 politiewet raakt en wellicht zelfs overschrijdt. De mate waarin dat gebeurt blijft onduidelijk⁸⁷ en is vooral afhankelijk van de wijze waarop men 'stelselmatig' pleegt te formuleren. Aangezien er in de CIE-praktijk geen gebruik wordt gemaakt van de 126v-informant, is er ook geen ruimte voor een jurisprudentie-ontwikkeling van dat begrip. De in de praktijk bestaande uitleg van 'stelselmatigheid' kan om die reden niet op rechtmatigheid worden getoetst. Het achterblijven van het gebruik van de art. 126v-informant doet vermoeden dat een deel van de art. 126v-informanten onterecht als art. 2-informanten wordt aangemerkt. Het is in ieder geval op z'n minst in strijd met de ratio van art. 126v Sv wanneer een aantal CIE chefs stellen dat een:

*"[...] art. 2 Politiewet 1993 [...] informant [...] in de praktijk even bruikbare informatie [blijkt] op te leveren als de stelselmatische informant en [...] bovendien beter afgeschermd [kan] worden."*⁸⁸

2.4 ORGANISATORISCHE SAMENSTELLING VAN DE CIE

In deze sectie behandelen we de organisatorische samenstelling van de CIE. Daarbij maken we onderscheid tussen de nationale samenstelling, die in subsectie 2.4.1 wordt behandeld, en de regionale samenstelling, die in subsectie 2.4.2 wordt beschreven. Met de nationale samenstelling bedoelen we de wijze waarop de verschillende CIE-en over de verschillende politiekorpsen en andere opsporingseenheden zijn verspreid. Met de regionale samenstelling doelen we op de organisatiestructuur binnen de CIE als eenheid. Voorts merken we op dat Koelewijn in zijn proefschrift een uitgebreide analyse van de CIE-structuur heeft gegeven.⁸⁹

86 Van Straelen, 2002, p. 32. Beijer e.a., 2004, p. 89.

87 Beijer e.a., 2004, p. 41.

88 Tak, 2002, p. 13.

89 Koelewijn, 2009, p. 131-153.

2.4.1 De CIE nationaal bezien

Hoewel de CIE van origine een regionale instelling is, bezien wij de CIE-en tegenwoordig als een nationaal opererende eenheid. De CIE is ontstaan vanuit de recherchefunctie waar behoefte was aan een geprofessionaliseerde manier van het inwinnen van inlichtingen. Deze ontwikkeling heeft na een formaliseringsslag uiteindelijk geleid tot 25 regionale CIE-en, één CIE bij het Korps Landelijke Politie Diensten (KLPD), één bij de Koninklijke Marechaussee (KMAR), en één bij de bijzondere ambtenaren van politie (de rijksrecherche).⁹⁰ Daarnaast is er één Nationale CIE (NCIE) die is gestationeerd bij de Dienst Nationale Recherche Informatie (DNRI). In totaal komen we zo op 29 CIE-en. De DNRI heeft een belangrijke centrale rol bij het verwerken van informatie die van groot gewicht is voor de bestrijding van zware criminaliteit. De NCIE verwerkt CIE-gegevens op nationaal niveau.⁹¹ Zij faciliteert onder meer het VROS-systeem⁹² dat de regionale verzamelingen van CIE-gegevens koppelt. Regionale CIE-en worden hoe langer hoe meer in dienst gesteld van de NCIE. De veranderingen die zijn doorgevoerd met de invoering van de Wet politiegegevens en de gecentraliseerde organisatie van de Nederlandse politie zijn daarbij drijvende krachten. Naast de 29 CIE-en bij de politie werd het ook wenselijk geacht een CIE bij iedere bijzondere opsporingsdienst in te stellen. In 2003 zijn in totaal vier extra CIE-en ingesteld bij de belastingdienst/FIOD-ECD, VROM/IOD, SIOD en bij de AID.⁹³ Derhalve bedraagt het aantal CIE-en 33.

2.4.2 De CIE regionaal bezien

Bij de meeste CIE-en is intern eenzelfde structuur doorgevoerd. Omdat deze interne structuur voor de CIE niet bindend is voorgeschreven is zij enigszins organisch. Om die reden kent deze subsectie een wat andere benadering dan de voorgaande. Hieronder wordt kort ingegaan op de verschillende functies die in een CIE kunnen worden onderscheiden.⁹⁴

De CIE is binnen de politie een afgeschermd eenheid en ook intern wordt informatie voor elkaar bewust afgeschermd. Het principe *'need to know, nice to know'* is een belangrijke factor. De chef van de CIE heeft daarbij een sturende, begeleidende, en controlerende rol over de andere CIE-ers en is meestal de enige persoon die kan beschikken over alle binnen de CIE aanwezige informatie. Tussen de CIE-chef en de CIE-runners bevinden zich een of meerdere groepschefs die de runners op dagelijks niveau aansturen.

90 Art. 1 onder a CIE-regeling.

91 Art. 8 CIE-regeling.

92 Zie voor een uitgebreide beschrijving van de vormen van verstrekking en het VROS-systeem: Koelewijn, 2009, p. 111.

93 Staatsblad 2002, 484.

94 Koelewijn, 2009, p 142-143.

Zij bepalen welke CIE-ers met elkaar runnen en op welke informanten zij runnen. Ook bepaalt de groepschef (of de CIE-chef) samen met de runners de juistheid en volledigheid van de informatie. Deze procedure heeft ten doel de objectiviteit van die vaststelling zoveel mogelijk te waarborgen. De CIE-ers die informanten runnen vormen vanzelfsprekend het hart van de CIE. Zij onderhouden de contacten met de informanten, brengen de informatie binnen, en zijn betrokken bij de bepaling van de juistheid en volledigheid van de informatie en het afbreukrisico dat aan de informatie moet worden toegekend. De invoering van de informatie in de systemen gebeurt vervolgens door de administratieve afdeling van de CIE. Deze administratieve afdeling bestaat meestal uit enkele fte's, die in sommige gevallen ook een gedeelte van hun tijd besteden als CIE-rechercheur. Zij halen uit de brutoverslagen de nettoblokken die in het register zware criminaliteit worden opgeslagen en worden voorzien van een afhandelingscode.⁹⁵ Bij de CIE zijn voorts ook rechercheurs aanwezig die tot taak hebben analyses te maken op basis van de aanwezige informatie. Dat kunnen verschillende soorten analyses zijn: zowel beleidsmatige analyses voor de managementlaag van het politiekorps, als tactische analyses die de informatie bij een tactisch team (opnieuw) onder de aandacht brengen.

Een persoon die niet direct onderdeel uitmaakt van de politieorganisatie, maar wel nauw bij inlichtingenproces is betrokken is de CIE-officier van justitie. Hij is vanuit het openbaar ministerie de persoon die het gezag voert over de CIE. Dit gebeurt thans in de praktijk op intensieve wijze. Zo houdt hij toezicht op de verschillende informanten, de binnengekomen informatie, de registraties in de verschillende systemen en uitgaande informatie. Zijn taken en bevoegdheden worden in hoofdstuk 6 behandeld.

2.5 HOOFDSTUKCONCLUSIE

In dit hoofdstuk is een beschrijving gegeven van de CIE-organisatie. Allereerst is de ontwikkeling van de CID naar de CIE beschreven. Daarbij is aandacht besteed aan de wijzigingen in de taken en bevoegdheden van de CID. De informatievoorziening van de recherchefunctie kwam centraal te staan bij de opsporing en bij het voorkomen van zware criminaliteit. Deze ontwikkeling heeft geleid tot een flinke hoeveelheid regelgeving die ziet op (1) de verwerking van politiegegevens door de CIE en (2) de wijze waarop de CIE haar informatie verkrijgt.

Uitgebreid is stilgestaan bij de informatie-inwinning en -veredeling door de CIE. Het inwinnen van informatie gebeurt voornamelijk door het gebruik van informanten die in anonimiteit informatie overdragen aan de CIE over criminele activiteiten waar zij kennis van hebben. Deze informatie wordt

⁹⁵ Zie voor een uitgebreide weergave en beschrijving van de afhandelingscodes Van der Bel e.a., 2007, p. 128-131.

door de CIE na het inwinnen beoordeeld op juistheid en volledigheid en vervolgens verwerkt. Het beoordelen op juistheid en volledigheid is het veredelen van informatie en gebeurt door het toetsen van informatie aan andere bronnen en informanten. Andere bronnen kunnen bestaan uit bijvoorbeeld het GBA. Ook speelt de betrouwbaarheid van de informant zelf een rol bij de veredeling van de informatie. Na de beoordeling vindt er een afweging plaats om te bepalen welk afbreukrisico aan de ingewonnen en veredelde informatie moet worden toegekend. De inhoud van de informatie kan immers exclusieve kennis van de informant zijn en dus bij openbaring tot ontmaskering van de tot dan toe anonieme informant leiden, met alle gevolgen van dien. Het gaat dan om de herleidbaarheid van de informant. De bronbescherming is het belangrijkste uitgangspunt van de CIE bij zijn taakuitvoering. Zonder informanten verkrijgen we immers geen inlichtingen.

Het inwinnen van informanteninformatie kan ten slotte worden teruggevoerd op twee verschillende bevoegdheden: (1) de algemene politietaakbepaling uit art. 2 Pw1993 en (2) de bijzondere opsporingsbevoegdheid voor het stelselmatig inwinnen van informatie bij informanten, neergelegd in art. 126v Sv. De mate van stelselmatigheid is van belang voor de bepaling of er sprake is van een art. 2-informant of een art. 126v-informant. Uniforme duidelijke criteria voor de vaststelling van die stelselmatigheid zijn echter niet gegeven, althans niet door de rechter getoetst. De CIE-praktijk heeft aangegeven de art. 126-informant niet te zullen gebruiken vanwege de risico's die dit met zich meebrengt voor de herleidbaarheid van die informant. Deze herleidbaarheid tot de informant verhoudt zich immers niet met de tal van strafvorderlijke waarborgen waarmee het stelselmatig inwinnen van informatie is omgeven en waarbij openbaarheid en controleerbaarheid een belangrijk rol spelen.

Uit het voorgaande mogen we concluderen dat het weinige gebruik van de art. 126v-informant ertoe leidt dat er ook in de rechtspraak nog geen criteria zijn ontwikkeld voor de vaststelling of er sprake is van het stelselmatig inwinnen van informatie. Er lijkt hiermee een patstelling te zijn ontstaan die vooralsnog vooral ten nadele van het subject lijkt uit te vallen.

3 | Betrokken belangen⁹⁶

In dit hoofdstuk bespreken we de betrokken belangen bij het verwerken van persoonsgegevens door CIE-en. Het hoofdstuk maakt duidelijk dat het recht op bescherming van persoonsgegevens de privacymantel van zich afschudt en dat dit recht zich de status van een zelfstandig grondrecht lijkt te gaan verwerven. De opvatting dat het gebruik van persoonsgegevens uitsluitend gevolgen voor de privacy met zich meebrengt, is geen gemeengoed meer.⁹⁷ De beschrijving van deze ontwikkeling (de ontwikkeling van onderdeel van privacybescherming naar een zelfstandig grondrecht) stelt ons in staat een antwoord te geven op OV1: op welke wijze zijn de politietaak en de grondrechten van de burger betrokken bij het gebruik van politiegegevens?

Bij het gebruik van persoonsgegevens door de politie worden over het algemeen twee belangen onderscheiden: het belang van de goede uitvoering van de politietaak enerzijds en gegevensbescherming anderzijds (belang A tegenover belang B). De eerste taak omschrijven we als de instrumentele functie van de Wpolg. De tweede taak omschrijven we als de beschermende functie van de Wpolg. Deze twee 'standaarden' nemen we als uitgangspunt bij het bespreken van de betrokken belangen bij de politieke informatieverwerking. In sectie 3.1 worden de betrokken belangen in hun algemeenheid besproken aan de hand van de strafrechtelijke doctrine. De instrumentele functie van de Wpolg wordt voorts in sectie 3.2 behandeld. De beschermende functie van de Wpolg komt in sectie 3.3 aan bod. In sectie 3.4 worden de verschillende internationale regelingen behandeld die van invloed zijn op de politieke gegevensverwerking. In sectie 3.5 wordt de sturende rol van technologische ontwikkelingen behandeld en daar zien we ook duidelijk de ontwikkeling naar een zelfstandig grondrecht. Uiteindelijk wordt in sectie 3.6 een antwoord geformuleerd op OV1.

3.1 INSTRUMENTALISME EN RECHTSBESCHERMING

In een instrumentalistische benadering wordt regelgeving gezien als middel om uitvoering te geven aan de (strafrechtelijk) handhaving van de rechtsorde. Deze benadering staat tegenover de beschermingsbenadering, waarin privacybescherming voorop staat. De benadering van de normen uit de Wet

⁹⁶ Een deel van dit hoofdstuk is reeds gepubliceerd: Kielman en Koelewijn, 2005. De auteur bedankt hierbij zijn co-auteur en de uitgever van het tijdschrift *Privacy en Informatie* voor hun toestemming om relevante gedeelten van het artikel in dit proefschrift te mogen hergebruiken.

⁹⁷ *Kamerstukken II*, 1985/86, 19 589, nr. 3, p. 1-2.

politieregisters als privacy-beschermende normen was in 1991 algemeen aanvaard en weinig verrassend.⁹⁸ Dit is niet meer zo vanzelfsprekend. Het gaat daarom in de navolgende drie subsecties steeds om een korte theoretische verhandeling met als doel de ontwikkelingen en de doelstellingen van de Wpolg te verduidelijken. In subsectie 3.1.1 behandelen we de theorie van het instrumentalisme. In subsectie 3.1.2 bespreken we de theoretische achtergrond van de beschermingsbenadering. In subsectie 3.1.3 bespreken we het spanningsveld tussen deze twee verschillende karaktertyperingen van het strafrecht.

3.1.1 Theorie van het instrumentalisme

In het strafrecht zijn er talloze dwangmiddelen die een verdachte moet dulden. Deze dwangmiddelen dwingen een verdachte in een ondergeschikte houding. De verdachte ondergaat tijdens dat proces bijvoorbeeld een voorlopige hechtenis, een ophouding voor verhoor, en een verwerking van persoonsgegevens. De bevoegdheid voor het opleggen van deze dwangmiddelen ligt (in laatste instantie) bij de rechterlijke macht. Een positieve bijdrage aan de uitvoering van de politietaak is het uiteindelijke doel van de inzet van dergelijke instrumenten. In dat doel wordt ook een rechtvaardiging gevonden voor de inbreuk die genoemde inzet van instrumenten maakt op de burgerlijke vrijheid.

Bevoegdheid als instrument

Steenhuis⁹⁹ benaderde de bevoegdheidstoedeling vrijwel uitsluitend instrumenteel. Hij vergeleek in twee artikelen de strafrechtswetenschap met een bedrijf. Het bedrijf heeft als missie de strafrechtelijke handhaving van de rechtsorde. Die kan worden bereikt door de inzet van de bevoegdheden uit het strafrecht. Door middel van straffen, strafdreiging en normbevestigingen wordt de burger gedwongen zich conform de wet te gedragen. Een dergelijke visie op de functie van strafrechtelijke bevoegdheden wordt veelal aangeduid met instrumentalisme. Het gaat dan om een vorm van beleid, dat er in essentie op neer komt dat criminaliteit wordt bestreden door het handhaven van normen. Criminaliteitsbestrijding is dus het primaire doel. Op die manier worden de goede burgers tegen de kwade beschermd.

Het strafrecht als sturingsmiddel

Op grond van de effectiviteit van bovengenoemde instrumenten is er een stroming ontstaan die *instrumentalisme* heet. Dit is een visie waarin het straf-

98 De titel van de Wet politieregister laat daar geen onduidelijkheid over bestaan: Wet van 21 juni 1991, houdende regels ter bescherming van de persoonlijke levenssfeer in verband met politieregisters.

99 Steenhuis, 1984, p. 497-512.

recht wordt gezien als sturingsmiddel van de maatschappij en wordt aangemerkt als beleidsinstrument. In het verlengde daarvan ligt *instrumentaliteit*, dat ziet op de middelen die de politie tot haar beschikking heeft om norm-conform gedrag af te dwingen, waarbij de normen het resultaat zijn van het beleid. Dergelijke inzichten hebben geleid tot een meer economische benadering van de strafrechtspleging.¹⁰⁰ Daarbij ligt de focus vooral op criminaliteitsbestrijding. Het huidige veiligheidsdenken is daarvan een uitwerking. Het leidt ertoe dat thans talrijke instrumenten worden ingezet in de opsporing die geen specifieke wettelijke basis meer hebben in het wetboek van strafvordering. De M-lijn (Meld Misdaad anoniem) is daarvan een voorbeeld. Als het gaat om politieke gegevensverwerkingen kan het informantenregister worden genoemd. Ook daarvoor ontbreekt een wettelijke basis.¹⁰¹ Daarnaast worden de instrumenten die wel zijn voorzien van een wettelijke basis in een steeds vroeger stadium ingezet als gevolg van een verschuiving in de grenzen die de toepassing van dergelijke middelen afbakent. Zo constateert Moerings in 2006 dat het strafrecht ook ingezet wordt om risico's zoveel mogelijk te elimineren.¹⁰² Bij politieke gegevensverwerking is die ontwikkeling eveneens waarneembaar. Onder de Wpolg is een speciaal verwerkingsregime ingesteld voor de verwerking van gegevens rond bijvoorbeeld terrorisme en mensenhandel, zodat al in een zeer vroeg stadium daarover gegevens mogen worden verwerkt.¹⁰³ Dergelijke ontwikkelingen brengen het gevaar met zich mee dat er een tendens kan ontstaan waarin het (beleids) doel de opsporingsmiddelen heiligt.

3.1.2 Theorie van de rechtsbescherming

De visie op de functie van strafwetgeving die uitgaat van de beschermingsfunctie wordt ook wel aangeduid met de machtskritische benadering.¹⁰⁴ Deze benadering ziet als primaire functie van wetgeving de beteugeling van overheidsmacht. Door het stellen van voorwaarden voor de toepassing van bijvoorbeeld dwangmiddelen wordt de burger beschermd tegen een wijdverbreide toepassing ervan. Het verwerken van politiegegevens behoeft eenzelfde normering om redenen die in sectie 3.3 aan de orde komen.

Aan de hand van de positie van verdachten in het strafproces heeft Peters¹⁰⁵ betoogd dat ook de rechtsbescherming zelf bescherming behoeft. Hij gaat daarbij uit van een vrijheidsgedachte, die zijn juridische uitwerking kent in onder meer de Nederlandse grondwet en de mensenrechtenverdragen. Specifiek voor het gegevensbeschermingsrecht wordt dit uitgebreid

100 Steenhuis, 1988.

101 Zie uitgebreid subsectie 4.5.2.

102 Moerings, 2006, p. 161 – 174.

103 Zie subsectie 4.5.3.

104 Foqué en 't Hart, 1990, p. 102. Foqué en 't Hart, 1990a.

105 Peters, 1993, p. 80.

besproken in sectie 3.3. Het uitgangspunt is dat de burgerlijke vrijheid bescherming nodig heeft tegen onder meer de invloed van strafwetgeving. Kenmerkend voor de bevoegdheden die in de strafwetgeving zijn neergelegd is de eigenschap om de vrijheid van diegenen die verdacht worden van misdrijven in te perken. Daarbij geldt dat hoe ruimer en omvangrijker de bevoegdheden van de politie zijn, des te meer van de burgerlijke vrijheid zal worden ingeperkt. Peters stelt dat het niveau van bescherming van de individuele vrijheid van verdachten onder meer dient te worden bepaald op basis van de empirie. Bescherming moet immers geboden worden tegen de daadwerkelijke vrijheidbeperkende handelingen van de politie. Daarbij mag niet worden uitgegaan van de veronderstelling dat de politie zich aan haar wettelijke bevoegdheden houdt.

“Ook wetshandhaving en opsporing van misdaad (zijn) onderworpen [...] aan eigen noden en dwangmatigheden”,

aldus Peters.¹⁰⁶ Peters wordt over het algemeen aangemerkt als de belangrijkste machts criticus wanneer het gaat om strafwetgeving. De tekst van zijn oratie is daarvoor exemplarisch. Als de drie belangrijkste karakteristieken van het strafrecht worden daarin aangemerkt (1) de legaliteits eis, (2) ‘zonder schuld geen straf’, en (3) seculiere vergelding.¹⁰⁷

Om die vrijheid te realiseren in een strafrechtelijke procedure maakt hij een analytisch onderscheid tussen ‘proces’ en ‘procedure’. ‘Proces’ weerspiegelt alle elementen die de onvrijheid van verdachten met zich meebrengen. ‘Procedure’ ziet daarentegen op alle elementen die de vrijheid van de verdachte realiseren en beschermen. Kenmerkend voor deze elementen is dat daar waar het ‘proces’ zich vrijwel geheel vanzelf ontwikkelt, ‘procedure’ tegen-natuurlijk is. ‘Procedure’ is ontwikkeld om vorm te geven aan het hogere maatschappelijke doel van individuele vrijheid. Het verschaft de verdachte een zoveel mogelijk gelijkwaardige positie als zijn wederpartij. Eén van dergelijke maatregelen is bijvoorbeeld het creëren en in stand houden van beginselen die zien op openbaarheid van het politieoptreden. In deze uitwerking van ‘proces’ en ‘procedure’ stelt Peters dat vanuit rechtsvergelijkend perspectief het belang van deze vrijheid in Nederland wordt onderschat. Dientengevolge is er te weinig aandacht voor deze beginselen en de rechtsbescherming in de strafprocedure.¹⁰⁸

106 Peters, 1993, p. 87.

107 Peters, 1972.

108 Peters, 1972, p. 105.

3.1.3 Het spanningsveld tussen instrumentalisme en rechtsbescherming

Logischerwijs leed de rechtsbeschermende functie van de strafrechtspleging onder de ontwikkeling van het instrumentalisme. Het realiseren van een adequaat niveau van rechtsbescherming vergt immers inspanning en is, zoals Peters het noemt, 'tegennatuurlijk'. De rechtsbeschermende functie verdraagt zich nu eenmaal slecht met de benadering van het strafrecht als maatschappelijk sturingsinstrument. Of in termen van Peters: het 'proces' voltrekt zich als vanzelf en dreigt eenvoudig de tegennatuurlijke 'procedure' te overstemmen. Het gebrek aan beteugeling van de overheidsmacht wordt dan ook over het algemeen aangemerkt als één van de grote tekortkomingen van de instrumentalistische benadering.

Zo betogen Foqué en 't Hart dat een instrumentalistische benadering van het strafrecht uitsluitend is gericht op het behalen van een maatschappelijk gewenst resultaat door middel van generale en speciale preventie. Het maatschappelijk resultaat wordt daarbij door de politiek bepaald.¹⁰⁹ Het recht wordt door beleidsmakers gemaakt, zonder dat deze zich laten beïnvloeden door andere factoren dan 'maatschappelijke winst'. Foqué en 't Hart nemen om die reden stevig stelling tegen de instrumentalistische benadering van het strafrechtssysteem. Ze verwijten de aanhangers ervan te weinig oog te hebben voor de belangen die gediend worden door de machtskritische benadering. Het verwijt is gebaseerd op een analyse van de historische ontwikkeling van het strafproces. Gesteld wordt dat, gezien de gezagsverhouding die er bestaat tussen de overheid en de burger, de burger middelen moet hebben om tegen dat gezag *en* zijn medeburgers in verweer te komen. Die middelen worden gevonden in het contradictoire strafproces.¹¹⁰ Dit kan ook thans op brede steun rekenen binnen de strafrechtdoctrine.¹¹¹

Foqué en 't Hart wijzen de instrumentele benadering van strafwetgeving niet af. Zij kunnen zich tot op zekere hoogte vinden in de argumenten en doelstelling die eraan ten grondslag liggen. Het is de eenzijdigheid van de benadering waar hun kritiek zich op richt. Er zit namelijk een bovengrens aan de inzet van die instrumenten; die bovengrens wordt volgens hen bepaald door de machtskritische benadering. Daar waar de inzet van instrumenten een gevaar dreigt te worden voor de burgerlijke vrijheid dient deze inzet terughoudend te worden toegepast. De grenzen van het instrumentele beleid worden bepaald door de grenzen die de *rule of law* daaraan stelt. Daarbij speelt dus onder meer de legaliteitseis een belangrijke rol.

In deze benadering zijn duidelijke overeenkomsten te ontwaren met de door Peters onderscheiden begrippen 'proces' en 'procedure', ondanks dat dezelfde Peters door Foqué en 't Hart als een machts criticus wordt aangemerkt. Ook bij het onderscheid tussen 'proces' en 'procedure' gaat het even-

109 Foqué en 't Hart, 1990, p. 102.

110 Foqué en 't Hart, 1990, p. 323-324.

111 Groenhuijsen, 2008.

wel om beperkingen van de individuele vrijheid door de inzet van strafrechtelijke instrumenten (het 'proces'), waartegen een vorm van bescherming moet worden geboden (middels 'procedure'). Foqué en 't Hart duiden dit spanningsveld aan als het relationele karakter van het strafrecht.

Dit zogenoemde relationele karakter van het strafrecht is een theoretische benadering die handelt over de functies van het strafrechtelijk systeem binnen de maatschappij. Het vertoont daarmee grote overeenkomsten met de afweging die ten grondslag ligt aan de regulering van het verwerken van politieke gegevens. De wetgeving op dat gebied is immers het resultaat van een afweging tussen de goede uitvoering van de politietaken (instrumenteel enerzijds en de bescherming van de persoonlijke levenssfeer (rechtsbescherming) anderzijds.

3.2 DE WPOLG EN INSTRUMENTALISME

Het instrumentalistisch karakter van de Wpolg hangt sterk samen met de politietaken. Politieke gegevens mogen onder de Wpolg alleen verwerkt worden indien dit in het kader van de politietaken gebeurt. In subsectie 3.2.1 beschrijven we de politietaken. In subsectie 3.2.2 behandelen we het formele gebruik van politiegegevens voor buiten de politietaken gelegen doelen. Met formeel bedoelen we gebruiksdoeleinden die in de Wpolg zijn vastgelegd. In subsectie 3.2.3 gaan we kort in op het informele gebruik van politiegegevens buiten de politietaken. Met informeel bedoelen we dat gebruik van politiegegevens dat buiten de regeling in de Wpolg om plaatsvindt en dat formeel gezien dus als onrechtmatig kan worden aangemerkt. Uiteindelijk behandelen we in subsectie 3.2.4 het gebruik van politiegegevens in het licht van hetgeen is beschreven in sectie 3.1.

3.2.1 De politietaken

In een instrumentalistische benadering worden de bevoegdheden uit de Wpolg benaderd als instrumenten ter ondersteuning van de politie in de uitvoering van haar taken. Die taken zijn in art. 2 van de Politiewet 1993 (Pw1993) als volgt omschreven:

“De politie heeft tot taak in ondergeschiktheid aan het bevoegde gezag en in overeenstemming met de geldende rechtsregels te zorgen voor de daadwerkelijke handhaving van de rechtsorde en het verlenen van hulp aan hen die deze behoeven”

De taakstelling van de politie valt blijkens art. 2 Pw1993 uiteen in (a) de daadwerkelijke handhaving van de rechtsorde en (b) het verlenen van hulp aan hen die deze behoeven. Deze taken mogen zij uitsluitend uitvoeren in ondergeschiktheid van het bevoegde gezag. Dit is uitgewerkt in de artt. 12

en 13 Pw1993. We behandelen de twee elementen van de politietaak hieronder afzonderlijk: (1) de daadwerkelijke handhaving van de rechtsorde en (2) het verlenen van hulp aan hen die deze behoeven.

De daadwerkelijke handhaving van de rechtsorde

Het onderdeel van de politietaak dat wordt omschreven als 'de daadwerkelijke handhaving van de rechtsorde' valt opnieuw uiteen in twee componenten. Ten eerste de strafrechtelijke handhaving van de rechtsorde. Ten tweede de handhaving van de openbare orde.

Onder de strafrechtelijke handhaving wordt verstaan: "de voorkoming, de opsporing, de beëindiging, de vervolging en de berechting van strafbare feiten, alsmede de tenuitvoerlegging van beslissingen van de rechter of het openbaar ministerie".¹¹² Het moge duidelijk zijn dat de rol van de politie vooral vorm krijgt bij de voorkoming, opsporing en beëindiging. Vervolging, berechting en de tenuitvoerlegging van de straf is met name een taak van het OM en de rechterlijke macht. De politie speelt bij die taken een ondergeschikte rol. In het kader van de strafrechtelijke handhaving verwerkt de politie een groot aantal persoonsgegevens. In hoofdstuk 2 is uitgebreid stilgestaan bij de rol die de CIE vervult in deze taakuitvoering.

De handhaving van de openbare orde geschiedt onder de verantwoordelijkheid van de burgemeester van de gemeente waar de ordehandhaving plaatsvindt. In tegenstelling tot de strafrechtelijke handhaving is de politie niet de enige instantie die zich bezighoudt met de handhaving van de openbare orde. Andere instanties zijn bijvoorbeeld de brandweer, stadswachten, particuliere toezichthouders, instellingen en bedrijven, zoals de RDW en de ANWB. Zij hebben elk hun eigen gegevensverwerking die onderhevig is aan het regime van de Wbp of een specifieke wettelijke regeling, zoals geldt voor de Gemeentelijke basisadministratie (GBA). Als het gaat om de politieke informatieverwerking in het kader van de openbare orde kan allereerst gewezen worden op de basisregisters van de politie. Denk daarbij bijvoorbeeld aan het registratiesysteem dat vanuit de surveillance-auto raadpleegbaar is. Daarnaast kent de politie een register dat specifiek ziet op de handhaving van de openbare orde.¹¹³ Het register wordt beheerd door de regionale inlichtingendienst (RID) en ziet op de voorkoming van zwaardere en regelmatig terugkerende vormen van verstoringen van de openbare orde. De RID is belast met de informatievoorziening binnen de politieorganisatie op dit gebied. Daarbij kan worden gedacht aan informatie omtrent supportersgeweld rond voetbalwedstrijden. Tevens fungeert de RID als regionaal gestationeerde post van de Algemene Inlichtingen en Veiligheids Dienst (AIVD). De RID kan, indien dit nodig is voor de uitvoering van haar politietaak, gebruik maken van CIE-informatie. In sommige politieregio's heeft de RID rechtstreekse toegang tot de registers van de CIE. Op deze wijze kan

¹¹² *Kamerstukken II*, 1985/1986, 19 535, nr. 3, p. 6.

¹¹³ Modelreglement Openbare orde Informatie (Code-nr.02/238.OOI.1).

CIE-informatie bijdragen aan de handhaving van de openbare orde. Ook de burgermeester kan bij de handhaving van de openbare orde gebruik maken van CIE-informatie. De CIE heeft bij de handhaving van de openbare orde echter geen zelfstandige rol.

Het verlenen van hulp aan hen die deze behoeven

De wettelijke hulpverleningstaak van de politie krijgt vooral in de praktijk gestalte. Het gaat daarbij bijvoorbeeld om het geven van richtingsaanwijzingen aan toeristen en het verlenen van assistentie bij een verkeersongeval. Ook kan gedacht worden aan het optreden tegen openbare dronkenschap, wildplassen, en psychische noodhulpverlening. Logischerwijs is bij dit gedeelte van de politieke taakuitvoering de belangrijkste rol weggelegd voor de agenten op straat. Het gebruik van politiegegevens speelt daarbij een marginale rol. De informatievoorziening rond deze taken van de politie behoort, zoals beschreven in hoofdstuk 2, ook niet tot de taken van de CIE-en. Zij verwerkt informatie ten behoeve van de opsporing en ter voorkoming van zware criminaliteit.

Daarnaast is er een tendens waarneembaar waarin de hulpverleningstaak wordt terug-gedrongen. Zo wordt in het rapport *'Naar een veiliger samenleving'* opgemerkt dat de hulpverleningstaak van de politie in verhouding te veel tijd kost.¹¹⁴ Dit wordt onder meer geweten aan de 24-uurs bereikbaarheid, die veel andere instellingen niet hebben. Er zouden meer hulpverleningstaken bij die andere organisaties weggezet kunnen worden, bijvoorbeeld psychische opvang door crisisdiensten of hulp bij ongevallen door de ANWB. In het rapport wordt ervoor gepleit om de hulpverleningstaak van de politie te beperken tot acute hulsituaties. Die ontwikkeling lijkt uitgevoerd te worden. Middels de prestatiecontracten wordt de politie gedwongen minder tijd aan de hulpverleningstaak te besteden.¹¹⁵

De hulpverleningstaak van de politie zal gezien de gegeven beperkingen in dit onderzoek verder niet aan bod komen.

3.2.2 Formele verstrekkingen van politiegegevens

Het wettelijk kader voorziet in de mogelijkheid politiegegevens ook buiten de sfeer van de politietaken te gebruiken. In de Wpolr is daarvoor een zogenaamd gesloten verstrekkingssysteem opgenomen. Dit wil zeggen dat informatie alleen aan die personen en/of instanties verstrekt mag worden die genoemd staan in de Wet politieregisters of het Besluit politieregisters. Dit zijn de zogenaamde formele verstrekkingen. We behandelen hier een aantal van deze verstrekkingsgerechtigden die gebruik kunnen maken van CIE-

114 Veiligheidsprogramma (2002), *Naar een veiliger samenleving*. Den Haag: Ministeries van Justitie en van Binnenlandse Zaken en Koninkrijksrelaties, p. 79.

115 Stol, 2004, p. 12.

informatie, maar die geen onderdeel uitmaken van de politieorganisatie. We noemen met name de AIVD/MIVD, de burgemeesters, de medewerkers van het bureau BIBOB, en de minister van Justitie. Het betreft hier geen limitatieve opsomming, maar de duiding van een aantal ontvangstgerechtigden, die exemplarisch zijn voor de breedte waarin politie-informatie buiten de politieorganisatie kan worden verwerkt. Gezien ons onderwerp (het verwerken van politiegegevens) behandelen we hieronder de vier genoemde instanties expliciet, vooral om enig inzicht te geven in de informatiestromen.

Het belang van de behandeling van de verstrekkingsgerechtigden is dat politiegegevens via deze weg gebruikt kunnen en mogen worden voor een taak, anders dan de politietaak. Dat is direct van invloed op het belang dat moet worden toegekend aan het instrumentele karakter van de Wpolr. Bij de bepaling daarvan is dus niet alleen de politietaak van belang, maar ook de taken van andere ontvangstgerechtigden. De politie fungeert bij dergelijke verstrekkingen feitelijk alleen als verzamelaar en doorgever van gegevens. Daardoor zijn de gevolgen van het verwerken van gegevens door de politie ook merkbaar buiten de werkingssfeer van de politietaak.

AIVD

Volgens art. 17 lid 1 Wpolg kunnen politiegegevens aan de inlichtingen- en veiligheidsdiensten verstrekt worden voor zover dat voortvloeit uit de WIV2002. CIE-informatie kan dus aan de AIVD worden verstrekt. Uit het veldwerk van Kielman en Koelewijn bleek dit in de praktijk veelvuldig te gebeuren.¹¹⁶ Toch is het goed op te merken dat er tussen de CIE en de AIVD in beginsel een aanzienlijk verschil is in taakopdracht. De AIVD heeft kort gezegd tot taak de bescherming van de democratische rechtsorde, de staatsveiligheid en ander gewichtige belangen van de staat. Strafrechtelijke opsporing behoort niet tot haar taken. In de uitvoering van haar taak heeft de AIVD evenwel de beschikking over een breed scala aan bevoegdheden. Inherent aan de taken van een inlichtingen- en veiligheidsdienst is er derhalve een bepaalde mate van onduidelijkheid omtrent de werkzaamheden van dergelijke diensten.

Burgemeester

De burgemeester is formeel het bevoegde gezag over de politie gezamenlijk met de officier van justitie. In deze rol heeft hij ook een bepaalde mate van zeggenschap over de politie. Met name als het gaat om de handhaving van de openbare orde beschikt hij ook over een redelijk groot aantal zelfstandige bevoegdheden. Het instellen van een noodverordening of de beslissing over het al dan niet afgeven van een horecaverunning zijn specifieke bevoegdheden voor een burgemeester. Bij dergelijke beslissingen, die wel bijdragen aan de handhaving van de openbare orde, maar niet tot de politietaak beho-

116 Zie subsectie 1.4.2.

ren, kan de burgemeester gebruik maken van de informatie die aanwezig is bij de politie.¹¹⁷ Derhalve kan hij ook van CIE-informatie gebruik maken.

BIBOB

Het bureau Bevordering Integriteitsbeoordelingen door het Openbaar Bestuur (BIBOB) is ingesteld om integriteitsonderzoeken uit te voeren in opdracht van verschillende bestuursorganen. Op verzoek voert het bureau onderzoek uit naar personen om het betreffende bestuursorgaan te kunnen voorzien van een advies over de integriteit van een persoon. Dat kan bijvoorbeeld een aanvrager zijn van een horecaverunning. Doel hiervan is te voorkomen dat door het afgeven van subsidies of vergunningen de overheid bijdraagt aan de instandhouding of opbouw van criminele activiteiten. In de Wet BIBOB is neergelegd in welke gevallen een bestuursorgaan gebruik kan maken van de BIBOB-diensten. Het moet gaan om een beschikking die ziet op de verkrijging van enige vorm van subsidie of een specifiek aantal genoemde vergunningen en ontheffingen.¹¹⁸ Dat zijn onder meer een horecaverunning, een beroepsvervoervergunning, een personenvervoervergunning en een bouwvergunning. Bij de afhandeling van dergelijke integriteitsonderzoeken kan door het bureau BIBOB gebruik worden gemaakt van gegevens uit politieregisters, waaronder dus ook CIE-informatie. Doel van deze informatieverwerking is de ondersteuning van bestuurlijke besluitvorming rond subsidie- en vergunningverlening.

Minister van Justitie

De minister van Justitie is bevoegd om voor verschillende doelen kennis te nemen van de inhoud van politieregisters. Het gaat dan bijvoorbeeld om de verstrekking van antecedenten¹¹⁹ en, voor zover hij deze behoeft, voor de uitvoering van de Wet documentatie vennootschappen¹²⁰. Voor individuele burgers is vooral van belang dat de minister ook informatie uit politieregisters verstrekt kan krijgen voor de bepaling of een verklaring van goed gedrag wordt afgegeven.¹²¹ Deze verklaring van goed gedrag moet voor tal van (overheids) functies worden aangevraagd. Het doel van een dergelijke informatieverwerking is de toekomstige werkgever van de individuele burger te voorzien van informatie omtrent het gedrag van deze persoon.

3.2.3 Informele verstrekkingen van politiegegevens

Naast de formele stromen van politiegegevens onderscheiden we informele informatiestromen. Deze stromen hebben geen wettelijke basis en zouden

¹¹⁷ Art. 15 lid 1, b onder 2 Wpolr.

¹¹⁸ Art. 1 lid 1 onder c Wet BIBOB.

¹¹⁹ Art. 16 lid 1 onder a Wpolr.

¹²⁰ Art. 15 lid 1 onder e Wpolr.

¹²¹ Art. 15 lid 1 onder f Wpolr.

dus in beginsel niet mogen plaatsvinden. Bij informele informatiestromen wordt vaak gesproken van een 'old-boys netwerk'.¹²² Dit zijn kennissen uit het vak die informatie uit de systemen halen en aan bevriende personen geven. Veel informatiebureaus maken gebruik van deze manier van opereren om aan hun informatie te komen.¹²³

Het oude onderzoek van Van Kralingen en Prins heeft duidelijk gemaakt dat buiten de politieorganisatie behoefte is aan de verwerking van politiegegevens. Zij noemden onder andere bedrijfsverenigingen en uitkeringsinstanties, hulpverleningsinstanties, openbaar bestuur, particulieren, woningbouwcorporaties, bedrijven, deurwaarders, recherchebureaus, verzekeraars en financiële instellingen.¹²⁴ De uitwisseling van gegevens tussen de politie en dergelijke instanties bleek op verschillende wijzen plaats te vinden en was sterk afhankelijk van de bevraagde regio en de afhandelende ambtenaar.¹²⁵ Elk van de instanties die een bepaalde behoefte heeft aan politiegegevens kon deze in meer of mindere mate verkrijgen. Zo bleek ook uit het onderzoek van Van Ruth en Gunther Moor. Zij concludeerden dat informatiestromen in de praktijk voornamelijk gestalte kregen door sociale structuren. Familie, 'old-boys' netwerken, etniciteit en organisatorische verbanden waren de belangrijkste drijfveren achter informele informatieverstrekkingen. De regelgeving speelde daarbij logischerwijs een ondergeschikte rol. Indien een bepaalde verstrekking door de politie als nodig of nuttig werd bestempeld dan werd daarvoor een oplossing gevonden. Tot 1 januari 2008 werd art. 30 Wpolr aangevoerd als formele basis voor dergelijke uitzonderingsverstrekkingen. Er werd gebruik gemaakt van de vage bewoordingen in die bepaling en van het verschil van mening dat bestond over de reikwijdte ervan.¹²⁶ Thans is in de Wpolg de mogelijkheid opgenomen om in een uitzonderingssituatie politiegegevens te verstrekken aan derden die niet direct als ontvangstgerechtigd zijn aangemerkt.¹²⁷

3.2.4 De Wpolg als instrument

De regels en normen uit de Wpolg worden hoofdzakelijk vanuit privacyperspectief benaderd. Wij constateren in die benadering een fundamenteel verschil met de discussie tussen strafrechtsspecialisten, zoals we die beschreven in sectie 3.1. Waar in het strafrechtelijk debat te weinig aandacht is voor de constitutionele grondslagen, lijkt dit in de discussie rond het gebruik van politieke gegevensverwerking tegenovergesteld. In de verhandelingen over politieke gegevensverwerking wordt namelijk veel nadruk gelegd op de

122 Van Kralingen en Prins, 1996, p. 29.

123 Van Ruth en Gunther Moor, 1997, p. 127.

124 Van Kralingen en Prins, 1996, p. 15-17.

125 Van Kralingen en Prins, 1996, p. 32.

126 Van Ruth en Gunther Moor, 1997, p. 12.

127 Zie subsectie 4.7.3.

beschermingsfunctie en juist weinig op het instrumentele karakter ervan. Buruma wees er in 1997 al op dat er met betrekking tot de gevolgen van het gebruik van politiegegevens sprake was van een “onterechte reductie tot privacy-problemen”.¹²⁸

We hebben gezien dat tegenover de wettelijke beschermingsfunctie de instrumentele functie staat. In subsectie 2.3.1 hebben we beschreven dat destijds niet-ingrijpende instrumenten geen specifieke wettelijke grondslag behoeften maar hun grondslag vonden in art. 2 Politiewet 1993 (Pw), waarin de politietaak was neergelegd. Voor de verwerking van persoonsgegevens werd ook toen al specifieke wetgeving wel noodzakelijk geacht.¹²⁹ De Wpolg neemt als uitgangspunt dat de bevoegdheden die in de wet staan omschreven alleen mogen worden aangewend ten behoeve van de politietaak. Het gaat dan om het opslaan, bewaren, verstrekken, koppelen, en analyseren van informatie waardoor het opbouwen en in stand houden van een informatiepositie mogelijk is. Daarmee zijn die bevoegdheden een instrument dat bijdraagt aan een behoorlijke taakuitoefening. Het belang van die bijdrage is algemeen geaccepteerd.¹³⁰ Een duidelijk voorbeeld van een bevoegdheid die de administratieve en ondersteunende functie ontstijgt is *gerichte datamining*.¹³¹ Deze vorm van datamining wordt ingezet naar aanleiding van een concrete verdenking of een aanwijzing en richt zich op een specifieke groep of persoon.¹³² Een gericht dataminingsonderzoek op een aantal radicale internetforums in combinatie met politiegegevens kan bijvoorbeeld nieuwe informatie over een terroristische groepering opleveren en zodoende een bijdrage leveren aan de opsporing van moslimterrorisme. Ook kan gewezen worden op de CT infobox (Contra Terrorisme).¹³³ Daarin worden politiegegevens geautomatiseerd verwerkt in combinatie met gegevens van de veiligheidsdiensten, het openbaar ministerie en de vreemdelingendienst. Door toepassing van datamining worden uit de aanwezige databestanden de relevante gegevens gefilterd.

Informationele opsporingsmethoden

Uit het voorgaande volgt dat het niet zozeer de kunst is om informatie te verzamelen, maar om daaruit de voor de opsporing relevante informatie te selecteren. De bevoegdheden die dat laatste mogelijk maken duiden wij aan met *informationele opsporingsmethoden*. Wij constateren een opvallende overeenkomst tussen de aard van deze ‘informationele opsporingsmethoden’ en strafvorderlijke opsporingsmethoden. Enerzijds wordt bescherming geboden tegen verregaande inbreuken op de grondrechten van burgers door de politie; het zijn evenwel dezelfde inbreuken die anderzijds belangrijke

128 Buruma, 1997, p. 306-307.

129 HR 19 december 1995, NJ 1996, nr. 249.

130 Corstens, 2008, p. 299.

131 Sietsma, 2006, p. 82.

132 Sietsma, Verbeek en Van den Herik, 2002, p. 59.

133 *Kamerstukken II*, 2004/05, 30 070, nr. 6.

instrumenten zijn voor de opsporing. Het doel van de toepassing van dergelijke 'informatieele opsporingsmethoden' is daarmee hetzelfde als een strafvorderlijke opsporingsmethode, namelijk: nieuwe kennis verkrijgen. Die kennis kan bijvoorbeeld meewerken aan het construeren van een strafrechtelijke verdenking of gebruikt worden als bewijs in een individuele strafzaak.

Het verkrijgen van die nieuwe kennis is noodzakelijkerwijs gebonden aan een aantal voorwaarden. Ook materieel zijn er dus overeenkomsten. Zo is gerichte datamining een zwaar middel. Toch mag dit middel onder de Wpolg, evenals de toepassing van een bijzondere opsporingsbevoegdheid, onder de verantwoordelijkheid en in opdracht van een officier van justitie worden toegepast.¹³⁴ Uit art. 1 Sv vloeit voort dat de basis voor dergelijke opsporingsmethoden moet zijn neergelegd in een formele wet. Als het gaat om de toepassing van technieken als gerichte datamining voorziet de Wpolg daarin. De Wpolg heeft daarmee een sterke legitimerende instrumentele werking. Op deze wijze zijn deze 'informatieele opsporingsmethoden', net zoals strafvorderlijke opsporingsmethoden, terug te voeren op het wetboek van strafvordering. Een duidelijker strafvorderlijk belang van de verdachte kan er niet zijn, dunkt ons. Een soortgelijke conclusie trekken ook Buruma en anderen.¹³⁵

Meer bevoegdheden nodig

Ten aanzien van dit legitimerende effect van de Wpolg stelt het kabinet in de Memorie van Toelichting van de Wpolg dat meer bevoegdheden nodig zijn om politiegegevens beter te kunnen gebruiken ter uitvoering van de politietask. De mogelijkheden daartoe zijn ofwel te beperkt ofwel anticiperen onvoldoende op de huidige technologische ontwikkelingen. Daarbij verwijst het kabinet weliswaar naar het spanningsveld met de privacy, maar de noodzaak tot een uitbreiding van de bevoegdheden is de hoofdaanleiding voor de voorgestelde regimewijziging, zo constateren Kielman en Koelewijn.¹³⁶ Onder de Wpolg is het mogelijk "zeer geavanceerde zoekmethoden" bij een opsporingsonderzoek in te zetten op "alle beschikbare politiegegevens".¹³⁷ Als we bij *alle* politiegegevens de gegevens uit openbare en commerciële bronnen betrekken is het mogelijk om bijvoorbeeld gedetailleerde profielen en beelden van personen te verkrijgen. Ook in de hoeveelheid informatie waarvan gebruik kan worden gemaakt is een groei waarneembaar. De digitale sporen die je als burger achterlaat, nemen in omvang toe en staan in honderden databases geregistreerd. Al die gegevens worden door de overheid zoveel mogelijk beschikbaar gemaakt voor de inzet van 'informatieele opsporingsmethoden'. De voorgenomen opslag van verkeersgegevens is

134 Art. 11 lid 4 Wpolg.

135 Buruma, Goos en Michels, 2003, p. 54. Zie ook: Sietsma, Verbeek en Van den Herik, 2002, p. 144.

136 Kielman en Koelewijn, 2005a, p. 451.

137 *Kamerstukken II*, 2005/06, 30 327, nr. 3, p. 11.

daarvan een goed voorbeeld.¹³⁸ Alleen al op basis van deze verkeersgegevens is af te leiden wat de interesses van een persoon zijn, welke vakantieplannen hij heeft, welke activiteiten hij in zijn dagelijks leven ontplooit en met wie deze persoon contacten onderhoudt. De 'informatieele opsporingsmethoden' zijn dan ook, zoals het kabinet het noemt, "bijzonder verstrekkend".¹³⁹

Het relationele karakter

Al deze ontwikkelingen tezamen brengen ons tot de conclusie dat de regelingen rond de verwerking van politiegegevens een sterk instrumentalistisch karakter hebben. Het in subsectie 3.1.3 besproken relationele karakter van het strafrecht is op eenzelfde wijze toepasbaar op de regelingen rond de verwerking van persoonsgegevens. Het verwerken van persoonsgegevens is namelijk een instrument voor de politie en de grenzen van dat gebruik worden aangegeven door de rechtsbeschermende werking van diezelfde wetgeving. De beschermende werking van de Wpolg (en vroeger de Wpolr) krijgt in de literatuur wat ons betreft evenwel relatief veel aandacht. De materie die we in deze subsectie hebben beschreven, maakt duidelijk dat de Wet politiegegevens de privacyjas van zich afschudt, in die zin dat haar instrumentele functie aan belang toeneemt. Wat betreft die instrumentele functie hebben we duidelijk gemaakt dat de verwerking van politiegegevens meer is dan een ondersteunende functie voor de uitvoering van de politietaak, en zich daardoor langzaam de status van een zelfstandig opsporingsmiddel verwerft. Deze constatering heeft onder meer gevolgen voor de consequenties die in het strafproces aan een normschending van de Wpolg worden verbonden.¹⁴⁰ In subsecties 4.8.3 en 4.9.3 is uitgewerkt welke regelingen de Wpolg bevat ten aanzien van deze bevoegdheden en in sectie 6.7 is beschreven welke consequenties worden verbonden aan de schendingen hiervan in het strafproces. Ook daar zal blijken dat de Wet politiegegevens thans nog te veel vanuit zijn privacy-achtergrond wordt benaderd.

3.3 DE WPOLG EN RECHTSBESCHERMING

Het ontstaan van juridische vraagstukken rond het gebruik van persoonsgegevens wordt over het algemeen toegekend aan de technologische ontwikkelingen die begonnen in de jaren zeventig van de vorige eeuw. De discussie speelde toen voornamelijk in het domein van de privacy. Dit had oprekking van het privacybegrip tot gevolg. Dit werd tot dan toe namelijk restrictief geïnterpreteerd en beperkt tot de klassieke elementen.

138 Schmidt en Zwenne, 2005, p. 292-302.

139 *Kamerstukken II*, 2005/06, 30 327, nr. 3, p. 11.

140 Zie subsectie 6.7.4.

In subsectie 3.3.1 worden de klassieke elementen van het privacyrecht besproken. Voorts wordt in subsectie 3.3.2 de opkomst van het informatieve privacyrecht behandeld. Subsectie 3.3.3 handelt vervolgens over de laatste ontwikkelingen rond de bescherming van politiegegevens.

3.3.1 De klassieke elementen van het grondrechtelijk privacyrecht

Als de klassieke elementen van het privacyrecht worden de volgende onderdelen onderscheiden: (1) 'ruimtelijke privacy', (2) 'relationele privacy', en (3) 'lichamelijke privacy'. Deze drie elementen zullen we achtereenvolgens kort in deze subsectie behandelen.

Ad (1) Ruimtelijke privacy

Privacy als rechtsconcept is aan het einde van de negentiende eeuw geïntroduceerd door Warren en Brandeis. Als eersten benaderden zij de privacy als zelfstandig rechtsbegrip. Dit concept bood bescherming aan gedachten, sentimenten en emoties.¹⁴¹ Aanleiding voor het schrijven van dit standaardwerk was de roddelpers die door toepassing van moderne technieken tot de huiskamer van de Amerikaanse burger wist door te dringen. Het privacyrecht werd aanvankelijk dus beperkt tot 'de huiskamer' van het private leven. Een soortgelijke beperkte uitleg werd in de eerste helft van de twintigste eeuw in Nederland gehanteerd. De werking van het privacyrecht werd toen namelijk beperkt tot hetgeen zich binnenshuis afspeelt, de zogenaamde ruimtelijke privacy. De ruimtelijke privacy biedt een persoon de vrijheid om zich binnen de eigen vier muren vrijelijk te bewegen en te ontplooien. De bescherming van de huiselijke sfeer wordt voornamelijk fysiek bepaald. Dit wil zeggen dat het beschermt tegen het binnentreden van de woning. Daarentegen wordt het enkel kennisnemen van hetgeen zich binnenshuis afspeelt, dus zonder een fysiek binnentreden, niet beschermd door het grondwettelijk huisrecht.¹⁴²

Ad (2) Relationele privacy

Het beschermingsbereik van de privacy werd in eerste instantie gelijk gesteld met de ruimte waar de persoonlijke levenssfeer het meest tot uiting komt. Het toekennen van een bredere werkingssfeer aan de persoonlijke levenssfeer zou onbepaalbare grenzen tot gevolg hebben en om die reden leiden tot rechtsonzekerheid.¹⁴³ Niettemin werd uitbreiding van de werkingssfeer in de tweede helft van de twintigste eeuw toch betoogd. Het argument van de dreigende rechtsonzekerheid moest het afleggen tegen de behoefte om ook bescherming te bieden aan de persoonlijke levenssfeer bui-

141 Warren en Brandeis, 1890, p. 193-220.

142 De Graaf, 1977, p. 112.

143 De Brauw, 1965.

ten de huiskamer. Inmiddels wordt breed aanvaard dat de werkingssfeer van de privacy ook buiten het eigen huis haar invloed kan doen gelden. Zo behoren thans ook bepaalde vormen van persoonlijke communicatie tot de vaste kern van de privacy. Het beschermt de vertrouwelijkheid, zodat gedachten en emoties die bijvoorbeeld via een brief vertrouwelijk worden uitgewisseld ook vertrouwelijk blijven. Omdat de bepaling techniekafhankelijk is geformuleerd is de werking ervan beperkt tot de genoemde communicatiemiddelen, te weten brief, telefoon en telegraaf. Andere manieren van communiceren, zoals bijvoorbeeld e-mail of chat, worden hierdoor niet beschermd. Dit onderscheid komt wellicht wat vreemd over. Een e-mail heeft thans immers de functie van de papieren brief grotendeels vervangen. Eenzelfde grondwettelijk beschermingsniveau voor e-mail als voor een brief zou dan ook in de rede liggen. Deze ontwikkeling en de gevolgen daarvan worden in sectie 3.4 nader beschreven.

Ad (3) Lichamelijke privacy

Gedurende de jaren zeventig van de vorige eeuw werd men zich in toenemende mate bewust van de noodzaak van privacybescherming. Een volgende uitbreiding ziet op de privacyaspecten van de integriteit van het lichaam.¹⁴⁴ Het is dan wederom de technologie die zorgt voor het ontstaan van die discussie. De opkomst van de bloedproef ter vaststelling van het alcoholpromillage is daarvoor een van de aanleidingen.¹⁴⁵ Ook moet echter gedacht worden aan de toepassing van bepaalde opsporingsmethoden (onderzoek aan en in het lichaam in verband met drugszaken). Sinds de jaren zeventig is er een voortdurende aanwas van nieuwe technologieën die dergelijke privacyvraagstukken met zich mee brengen. De opkomst van het DNA-onderzoek is daarvan een goed voorbeeld.¹⁴⁶ In 2005 domineerden het biometrisch paspoort en Radio Frequency Identification (RFID) de discussie.

Tezamen worden de bovengenoemde drie elementen van de privacy aangeduid als de klassieke elementen van de privacy. Daarmee worden zij ook wel beschouwd als de harde kern van het privacyrecht. Het privacyrecht omvat dus in ieder geval deze elementen. Met de grondwetsherziening van 1983 zijn deze elementen afzonderlijk in een artikel opgetekend, te weten respectievelijk de artt. 11, 12 en 13 Gw. Deze bepalingen worden dan ook beschouwd als een uitwerking van het algemeen geformuleerde privacyrecht dat is neergelegd in art. 10 lid 1 Gw. Deze laatste bepaling geldt als een soort vangnet voor de schendingen van de persoonlijke levenssfeer die niet onder de werking van de klassieke elementen vallen. Er kan bijvoorbeeld

¹⁴⁴ Zie een uitgebreider: Blok en Vedder, 2002, p. 5-31, en de daar aangehaalde literatuur.

¹⁴⁵ HR 26 juni 1962, NJ 1962, nr. 470 (Bloedproef II-arrest).

¹⁴⁶ Nota n.a.v. het nader verslag van de regeling van het DNA-onderzoek in strafzaken, 26 mei 2000, *Kamerstukken II*, 1999/2000, 26 271, nr. 9.

gedacht worden aan het opnemen van gesprekken binnenshuis met een richtmicrofoon. Hoewel dit op het eerste gezicht een schending van het huisrecht lijkt op te leveren is dit, zoals is beschreven onder ad (1), niet het geval. De afbakening van het huisrecht wordt immers gekenmerkt door fysieke criteria. In zo'n geval kan dus aansluiting worden gezocht bij de algemene bepaling van art. 10 lid 1 Gw. Een ander voorbeeld van deze vangnetfunctie is de bescherming van (versleutelde) e-mail. Deze wordt niet beschermd door art. 12 Gw. Bij een onrechtmatige kennisneming van de inhoud van een e-mailbericht zal dan ook sprake zijn van een schending van de algemene privacybeschermingsbepaling. De reikwijdte van de grondwettelijke privacybescherming bestaat dus in ieder geval uit de klassieke elementen, maar is daar nadrukkelijk niet toe beperkt. Zij kunnen worden aangemerkt als de *specialis* van de *generalis* uit art. 10 lid 1 Gw. De algemene formulering van de algemene privacybepaling uit art. 10 lid 1 Gw brengt met zich mee dat de reikwijdte van de privacybescherming vrijwel voortdurend in beweging is. Een nadelig effect van de vangnetfunctie is dat de ruime en open formulering open en vage grenzen tot gevolg heeft. Blok duidde deze bepaling dan ook aan als "de allervraagste uit de grondrechtencatalogus".¹⁴⁷

3.3.2 Informationele privacy

Met de opkomst van de automatisering in het gebruik van persoonsgegevens in de jaren zeventig van de vorige eeuw werd het privacybegrip uitgebreid met wat later de informationele privacy is genoemd.¹⁴⁸ In Nederland kreeg dit besef op dat moment zijn weerslag. Het landelijke verzet tegen de veertiende volkstelling van 1970 in combinatie met de invoering van een Centrale personenadministratie (Cpa) wordt daarvoor in het algemeen als omslagpunt aangemerkt. De bewustwording omtrent de gevaren van het gebruik van persoonsgegevens was daarmee in de jaren zeventig een feit. In 1972 verwoordde Van Agt het als volgt:

*"Dat ook de computer een bedreiging kan vormen voor ons persoonlijke leven en onze persoonlijke vrijheid, daarvan is men zich in brede kringen nog slechts kort geleden bewust geworden."*¹⁴⁹

Men realiseerde zich echter ook dat de aard en inhoud van persoonsgegevens niet altijd met zich meebrachten dat het gebruik ervan afbreuk deed aan de in de vorige paragraaf omschreven klassieke elementen van de persoonlijke levenssfeer.

¹⁴⁷ Blok, 2002, p. 39.

¹⁴⁸ Westin, 1967.

¹⁴⁹ Instellingsrede van de Commissie Koopmans door minister-president Van Agt, behorend bij: Staatscommissie Koopmans, 'Eindrapport van de Staatscommissie bescherming persoonlijke levenssfeer in verband met persoonsregistratie', Den Haag, 1976.

Vier nieuwe accenten van privacy

De commissie Koopmans, die werd ingesteld om de gevolgen van deze ontwikkeling in kaart te brengen, sprak van “nieuwe accenten” aan de bescherming van de persoonlijke levenssfeer. Deze zou zich voortaan ook buiten de strikte privésfeer laten gelden.¹⁵⁰ Tijdens de voorbereiding van de grondswetswijziging in 1983 bracht de commissie Koopmans haar rapport uit over de wenselijkheid van opnemings van een apart artikel dat de persoonlijke levenssfeer beschermt in verband met de registratie van persoonsgegevens. Het ging daarbij vooral om de verhouding tussen de overheid en de burger die door de opkomst van technologische registratiemogelijkheden sterker onder druk was komen te staan. De commissie Koopmans vond evenwel geen directe aanleiding om een regeling te treffen omtrent de persoonsregistraties. Er hadden zich bijvoorbeeld geen incidenten voorgedaan die voortkwamen uit de toenemende registraties van persoonsgegevens. Feitelijk was er alleen een vorm van onrust. De commissie schetst daarbij vier categorieën waarop die maatschappelijke onrust kan worden teruggevoerd.

Ten eerste was dit de ‘autonomie’. De burger heeft de behoefte om ‘zich zelf te zijn’. Men moet de vrijheid hebben om te kunnen beslissen om bepaalde zaken voor zichzelf te houden zodat deze geen invloed hebben op de eigen reputatie of anderszins invloed uitoefenen op het eigen leven. De commissie stelde dat het gebruik van persoonsgegevens een nieuwe dimensie zou toevoegen aan dit beschermingsdoel van de privacybescherming. Ten tweede ging het om de ‘regie’. Er heerste een gevoel dat de burger zijn grip op zijn persoonsgegevens dreigde kwijt te raken. Met de komst van de automatisering werd misbruik van persoonsgegevens, gebruik buiten het doel waarvoor ze waren verkregen, sterk vereenvoudigd. Er werd gevreesd voor dergelijk misbruik en voor het ontstaan van ‘monster-databanken’, waarin alles over iedereen kon worden teruggevonden. Ten derde noemen we de ‘afhankelijkheid’. Er heerste een gevoel onder de bevolking dat de betrokkenheid van de burger bij besluitvormingsprocessen afnam. Er werd gevreesd dat besluiten buiten het zicht zouden worden genomen op basis van een aantal registraties. Daarbij zou de burger in een afwachtende en lijdelijke houding worden gedwongen en zodoende teveel afhankelijk worden van de juistheid en volledigheid van zijn registraties. Ten vierde was er de ‘spam’. Er werd gevreesd voor een verdere commercialisering van persoonsgegevens. Het gebruik van dergelijke databanken voor marketingdoeleinden zou ongetwijfeld een verergering van de ‘brievenbusvervuiling’ tot gevolg hebben.

De commissie stelde om bovenstaande redenen voor om onder het begrip persoonsgegeven elke registratie te verstaan die herleidbaar was tot een natuurlijk persoon. Daarmee dreigde een vergaande regulatie van het gebruik van persoonsgegevens. De commissie stelde evenwel dat niet elk gebruik van persoonsgegevens een schending van de persoonlijke levens-

150 *Idem*, p. 20.

sfeer oplevert. Bij het gebruik van persoonsregistraties moet volgens de commissie een afweging worden gemaakt tussen de belangen van degene die de gegevens verwerkt en de belangen van diegenen wiens gegevens worden verwerkt.¹⁵¹ De burger heeft een zekere beeldvorming te dulden. Anders zou bijvoorbeeld belastinginning kunnen worden voorkomen door simpelweg te weigeren persoonsgegevens te verschaffen. Een maximale controle over de eigen persoonsgegevens is dus niet haalbaar. Bij deze afweging ging de commissie uit van een directe relatie tussen de registratie van persoonsgegevens en privacy. Die keuze is voornamelijk maatschappelijk bepaald en kon rekenen op een breed draagvlak. De benadering van de commissie Koopmans paste ook in de benadering van het verwerken van persoonsgegevens in de toenmalige literatuur.¹⁵²

Het registreren

Op basis van deze overwegingen formuleerde de commissie Koopmans drie algemene uitgangspunten waaraan het registreren van persoonsgegevens zou moeten voldoen.¹⁵³ Ten eerste moest de registratie van persoonsgegevens transparanter worden. De belangrijkste vragen daarbij waren: wie?, wat? en voor welk doel? Ten tweede verdiende de burger, wiens persoonsgegevens geregistreerd worden, een sterkere positie te verkrijgen. Op die manier zou het voor hem mogelijk zijn om gebruik te maken van de voordelen van de transparantie en kon hij zonodig tegen een foutieve of onjuiste registratie in het geweer komen. Ten derde nam de commissie als uitgangspunt dat het versterken van die positie niet afdoende zou zijn om naleving van het wettelijke regime af te dwingen. Er zou een overheidsinstantie moeten komen die ook controle en toezicht zou houden op het gebruik van persoonsgegevens.

Met deze zaken als uitgangspunt deed de commissie een uitgebreid voorstel voor wetgeving, dat grotendeels overeenkwam met de later ingevoerde Wet persoonsregistraties.

Het gebruik

De Graaf was een van de eersten die de gevolgen van het gebruik van persoonsregistraties uitgebreid heeft behandeld. Hij gaf voor de koppeling tussen het gebruik van persoonsgegevens en de privacy twee redenen: (1) beïnvloeding van het leven van een individu en (2) een directe inbreuk op de persoonlijke levenssfeer.¹⁵⁴ We behandelen deze twee redenen achtereenvolgens.

151 *Idem*, p. 22.

152 De Graaf, 1977, p. 169.

153 Staatscommissie Koopmans, 'Eindrapport van de Staatscommissie bescherming persoonlijke levenssfeer in verband met persoonsregistratie', Den Haag, 1976, p. 28.

154 De Graaf, 1977, p. 159-161.

Ad 1) Beïnvloeding van levens

Iedere registratie van een persoonsgegeven heeft de potentie om het leven van die persoon te beïnvloeden. Hieraan ligt ten grondslag dat de interpretatie van persoonsgegevens, geplaatst in een bepaalde context, kennis wordt. Die kennis biedt de mogelijkheid het leven van de betreffende persoon (nadelig) te beïnvloeden, hetgeen vaak wordt aangeduid met het adagium 'kennis is macht'.¹⁵⁵ De beïnvloeding kan indirect een inbreuk op de privacy opleveren. Overkleeft-Verburg formuleerde het privacygevaar van het gebruik van persoonsgegevens als de vrijwaring van de burger van een '(inadequate) administratieve beeldvorming'.¹⁵⁶ Een van de vele illustratieve voorbeelden hiervan is het verzoek in Kort Geding van de stichting Brein aan vijf internetproviders.¹⁵⁷ Zij vorderde bekendmaking van de persoonlijke gegevens van klanten die ongeautoriseerde muziekbestanden via het internet aanboden. Met die persoonsgegevens had de stichting Brein de betreffende gebruikers dit willen verbieden en een schadevergoedingsclaim bij hen willen indienen. Echter, de voorzieningenrechter achtte de verwerking van persoonsgegevens door Brein allereerst in strijd met de privacyreggeving. Daarnaast zou Brein deels foutieve informatie hebben verstrekt waardoor het niet viel uit te sluiten dat de persoonsgegevens van niet-betrokken personen zouden worden verstrekt. Het verzoek werd derhalve afgewezen op privacygronden. De verstrekking van foutieve informatie had anders geleid tot een (onjuiste) beeldvorming over de geregistreerde personen. Bovendien zou dat 'beeld' dan bij de provider onvoldoende beschermd geweest zijn.

In beginsel wordt iedere natuurlijke persoon tegen bepaalde beeldvorming beschermd. Het behoeft dan ook niet altijd te gaan om een gevormd beeld dat onderdeel uitmaakt van de klassieke elementen van het privacyrecht. Indien een gegevensverwerking geen elementen bevat die beschermd worden door het klassieke privacyrecht, dan spreken wij van een indirect gevaar voor de persoonlijke levenssfeer. De ernst van een dergelijke beeldvorming wordt bepaald door (1) de aard van de persoonsgegevens, (2) het doel waarvoor deze gebruikt worden, en (3) de context waarin ze gebruikt worden. Juist bij de registratie van persoonsgegevens door de politie is die context een gegeven. Het enkele feit dat de persoonlijke gegevens van een persoon door de politie worden geregistreerd duidt namelijk op een al dan niet negatieve vorm van betrokkenheid bij criminele activiteiten. Het is dan ook niet verwonderlijk dat in de Wbp, in navolging van de Wpr, strafrechtelijke gegevens als bijzondere gegevens worden aangemerkt en dus ook worden gereguleerd en genormeerd door een stringenter regime. Het gevaar dat aan het gebruik van die gegevens kleef is voor de persoonlijke levenssfeer

155 Bacon, 1645, p. 32. "nam et ipsa scientia potestas est" wat vertaald wordt met o.a. 'Human knowledge and human power meet in one' of 'knowledge is power'.

156 Overkleeft-Verburg, 1995, p. 23.

157 Voorzieningenrechter rechtbank Utrecht 12 juli 2005, *LJN* AT9073.

nu eenmaal groter dan dat van 'gewone' persoonsgegevens. De wetgever stelt in dit verband dat het bij het gebruik van politiegegevens dan ook meestal om nogal gevoelige gegevens gaat. Daarnaast, zo vermeldt de memorie van toelichting, zijn dergelijke politiegegevens over het algemeen niet vrijwillig afgestaan.

Ad 2) Directe afbreuk aan privacy

Het gebruik van persoonsgegevens kan wel degelijk direct afbreuk doen aan de persoonlijke levenssfeer. Een deel van de persoonsgegevens heeft namelijk betrekking op zaken die tot het privéleven behoren. In de bevolkingsregisters zijn bijvoorbeeld gegevens opgenomen over burgerlijke staat en ras. Ook kan gedacht worden aan gegevens die zijn opgenomen in de registers van ziekenhuizen, zorgverzekeraars, en kredietverstrekkers. De inhoud van die gegevens is informatie die valt onder het beschermingsbereik van de klassieke elementen van de privacy. Wij spreken dan van een direct gevaar voor de persoonlijke levenssfeer. Dat verandert vanuit de informationele privacy in beginsel niets aan het toepasselijke regelgevend kader, maar is wel van invloed op de mate waarin de beeldvorming afbreuk doet aan de persoonlijke levenssfeer.

3.3.3 De Wpolg als gegevensbeschermmer

In de Wpolg wordt als uitgangspunt voor het reguleren van het verwerken van politiegegevens aansluiting gezocht bij de privacy. Dat past in de ontwikkeling van deze regelingen. Ook bij de Wpolr bleek uit de officiële titel van de wet onmiskenbaar de beschermingsfunctie van die wet: "Wet (...) houdende regels ter bescherming van de persoonlijke levenssfeer in verband met politieregisters". Bij de invoering van de Wet bijzondere politieregisters in 2000 is deze grondslag ongewijzigd gehandhaafd.¹⁵⁸ De persoonlijke levenssfeer als beschermingsobject is volgens sommigen echter te beperkt. Dit is in belangrijke mate ingegeven door de vaagheid van het privacybegrip¹⁵⁹, die volgens Blok heeft geleid tot begripsverwarring. Er zou onderscheid moeten worden gemaakt tussen de bescherming van de klassieke elementen van de persoonlijke levenssfeer enerzijds en zorgvuldig gegevensbeheer anderzijds. Blok geeft voor zijn tweedeling twee redenen.¹⁶⁰

158 "Het bevat met het oog op de bescherming van de persoonlijke levenssfeer nadere voorwaarden voor de opslag en het gebruik van persoonsgegevens." *Kamerstukken II*, 1996/97, 25 398, nr. 3, p. 1.

159 Vedder, 1996, p. 17-30.

160 Blok, 2001, p. 435-439.

Ten eerste is er een aanzienlijk verschil in uitgangspunt van beide leerstukken. Bij het klassieke privacyrecht gaat het om de onschendbaarheid van de persoonlijke levenssfeer; het afweerrecht. Inbreuken op de persoonlijke levenssfeer zijn slechts toegelaten indien is voldaan aan een aantal criteria, zoals die neergelegd zijn in het tweede lid van art. 8 EVRM. Bij de informatieve privacy is juist de schendbaarheid het uitgangspunt. Zorgvuldig gegevensbeheer strekt er in beginsel dan ook niet toe inbreuken af te weren, maar weerspiegelt een afweging tussen conflicterende belangen. Inbreuken op de persoonlijke levenssfeer zijn in beginsel *wel* toegelaten, mits deze vorm krijgen in overeenstemming met het wettelijke regime.

Ten tweede is het beschermingsobject van zorgvuldig gegevensbeheer breder dan dat van de klassieke elementen van de persoonlijke levenssfeer. Zoals we eerder hebben gesteld, hebben persoonsgegevens niet altijd betrekking op de klassieke elementen van de persoonlijke levenssfeer. Het begrip persoonsgegevens omvat namelijk voor een groot deel gegevens die onderdeel zijn van het openbare leven en daardoor in feite zijn onttrokken aan de persoonlijke levenssfeer. De verwerking van een telefoonnummer uit de telefoongids valt bijvoorbeeld onder het verwerkingsregime van de Wpolg, terwijl dit gegeven niet direct een aspect vertegenwoordigt dat behoort tot de persoonlijke levenssfeer. Openbaarheid van informatie en inmenging met de persoonlijke levenssfeer lijken elkaar dan ook uit te sluiten. De Hert en Gutwirth maken een soortgelijk onderscheid.¹⁶¹ Om deze reden wordt ook wel betoogd dat niet de informatie zelf object van bescherming zou moeten zijn, maar het beeld dat daardoor kan ontstaan. De verwerking van informatie is immers niet bezwaarlijk omdat de informatie herleidbaar is tot een persoon. De gevolgen van het gebruik van die informatie kunnen evenwel afbreuk doen aan de persoonlijke levenssfeer. Die beeldvorming zou object van bescherming moeten zijn in plaats van de informatie zelf.¹⁶² Die gedachte is vanuit de privacybenadering gezien zuiver. Gezien vanuit de problematiek die aan het gebruik van persoonsgegevens verbonden is, is dit echter niet het geval. De beeldvorming als gevolg van het gebruik van informatie kan namelijk niet alleen afbreuk doen aan de persoonlijke levenssfeer, maar aan veel meer zaken. Immers, het gevaar dat aan de '(inadequate) administratieve beeldvorming' is verbonden, raakt in beginsel alle grondrechten. Dit kan de privacy zijn, maar evengoed een ander grondrecht. We geven daarvan een voorbeeld (zie figuur 3.1). We gebruiken een fictieve casus waarbij de fouten zich opstapelen en waaruit dus een overduidelijke privacyschending zou moeten blijken.

161 De Hert en Gutwirth, 2003, p. 111-162.

162 Nabben en Van de Luytgaarden, 1996, p. 58-59.

In strijd met de normen uit de Wpolg wordt de heer Mommers geregistreerd in het register zware criminaliteit als vooraanstaand lid van een drugskartel. Als de heer Mommers van zijn wellicht toekomstige werkgever een verklaring omtrent het gedrag moet overleggen, vraagt hij deze aan bij de burgemeester van de gemeente Rotterdam. Afgifte wordt vervolgens geweigerd op grond van het enkele feit dat over de heer Mommers politiegegevens zijn verwerkt. Weigering van de afgifte om deze reden is echter in strijd is met art. 35 van de Wet justitiële gegevens. Levert deze flagrante schending van beide informatiele privacyregelingen nu een schending van de persoonlijke levenssfeer op? Indirect wordt het privéleven van de heer Mommers door deze onrechtmatige handeling wel getroffen. Maar de heer Mommers wordt ook ongelijk behandeld in vergelijking met andere sollicitanten; een schending van het non-discriminatieverbod van art. 1 Gw. Logischer is het evenwel te betogen dat de heer Mommers hierdoor onrechtmatig beperkt wordt in zijn grondrecht van vrije keus van arbeid, neergelegd in art. 19 lid 3 Gw. Solliciteerde Mommers op een openbare functie, dan komt daarnaast ook nog eens art. 3 Gw in het geding.

Figuur 3.1: Privacy en grondrecht.

Grotere gevaren onder de Wpolg

Onder het regime van de huidige Wpolg zijn de gevaren op privacyschending groter dan onder de oude wetgeving. Een van de belangrijkste redenen om tot instelling van de huidige wet over te gaan was namelijk het gesloten verstrektingsregime in die oude wetgeving. De politiepraktijk had behoefte aan meer informatie-uitwisseling met derden, zoals woningbouwcorporaties. Door dit bredere verstrektingsregime wordt het risico dat een burger te maken krijgt met de onwenselijke gevolgen groter. Derden kunnen in de toekomst gemakkelijker kennis nemen van de veronderstelde betrokkenheid bij criminele activiteiten van een persoon. Daarmee groeit de kans dat die persoon met dat (onjuiste) beeld geconfronteerd wordt. Het betekent in ieder geval dat de nieuwe wetgeving en de kans op het verspreiden van een onjuist beeld onlosmakelijk met elkaar verbonden zijn. Welke gevolgen dit heeft hangt af van het doel waarvoor een organisatie de informatie gebruikt. Het gevaar schuilt dan voornamelijk in het verschijnsel van discriminatoire gevolgen. Uitsluiting van aanbestedingen, verlies van een huurcontract, en weigering van een horecavergunning zijn daarvan enkele voorbeelden.

3.3.4 Meer dan privacy

Het beschermingsobject van de verschillende informatiele-privacy-regelingen is dus breder dan de persoonlijke levenssfeer alleen. De beeldvorming als gevolg van het gebruik van persoonsgegevens kan het leven van de betreffende persoon nadelig beïnvloeden. Deze invloed is evenwel niet beperkt tot het privéleven. Het voorgaande laat namelijk zien dat bij deze beeldvorming meer grondrechten in het geding zijn. Welke grondrechten dit zijn wordt voornamelijk bepaald door de aard van de informatie en de context waarin deze wordt verwerkt. Dit kan de persoonlijke levenssfeer zijn, maar evengoed een ander grondrecht.

Deze reductie tot privacy is wat ons betreft onterecht. Privacy is een belangrijk deel van het gegevensbeschermingsrecht, maar omvat meer dan dat. De privacyjas is te knellend. De consequenties van die keuze van de wetgever laat zich bij iedere discussie over het gegevensbeschermingsrecht voelen. Door de reductie tot privacy kan die discussie namelijk niet zuiver gevoerd worden. Dat brengt met zich mee dat bij iedere keuze die in de praktijk gemaakt wordt in de verwerking van politiegegevens gebaseerd is op een onjuist uitgangspunt. Daarbij moet immers een afweging worden gemaakt tussen de uitvoering van de politietaak enerzijds en de gevolgen van die gegevensverwerking voor de betreffende persoon anderzijds. Deze laatste gevolgen worden echter vanuit privacyperspectief benaderd, waardoor deze afweging niet volledig is. Zoals gezien laten deze gevolgen zich immers niet in de privacyhoek voelen, maar juist op een ander vlak en onder de werking van een ander grondrecht. Het duidelijkste voorbeeld dat wij hiervan kunnen geven is de wijze waarop de strafrechter omgaat met een schending van de normen uit de Wpolr door de politie. Kort gezegd dient de Wpolr volgens de strafrechter geen strafvorderlijk belang, omdat het een privacyregeling is. We behandelen deze problematiek uitgebreid in sectie 6.7. Het maakt duidelijk dat de positionering van de Wpolr en de Wpolg als privacywet tot een onzuivere discussie leidt met alle gevolgen van dien.

De benadering van de Wpolr en de Wpolg vanuit privacyperspectief kent haar oorsprong in internationale verdragen en de daaruit voortgekomen grondwettelijke bepalingen die het gebruik van persoonsgegevens reguleert. We behandelen deze regelingen in de navolgende sectie.

3.4 INTERNATIONALE EN NATIONALE POLITIËLE GEGEVENSVERWERKING

De verschillende betrokken belangen bij politieke gegevensverwerkingen zijn niet alleen onderwerp in nationale regelingen. Ook op Europees en mondiaal niveau zijn verschillende verdragen tot stand gekomen die iets bepalen over het gebruik van persoonsgegevens en de inbreuken die daarbij gemaakt worden op grondrechten, waarbij het privacyrecht als belangrijkste wordt aangemerkt. Deze internationale regelingen en verdragen vormen veelal een basis of uitgangspunt voor de regelingen die op nationaal niveau worden vastgesteld. In sommige gevallen is een lidstaat ook niet vrij om van het in het verdrag bepaalde af te wijken. De bescherming van persoonsgegevens in Nederland heeft sinds de jaren zestig en zeventig van de vorige eeuw gestalte gekregen, zij het voornamelijk op praktisch niveau. Wettelijke regelingen op grondwettelijk en formeel-wettelijk niveau kregen pas in de jaren tachtig gestalte. Op internationaal niveau zijn deze ontwikkelingen sneller gegaan. In subsectie 3.4.1 behandelen we de belangrijkste verdragen als het gaat om politieke gegevensverwerking. Voorts komt in subsectie 3.4.2 het nationale kader voor gegevensbescherming aan bod. In subsectie 3.4.3 behandelen we ten slotte de toekomstige verdrags- en wetsontwikkelingen op internationaal en nationaal gebied.

3.4.1 Internationale gegevensverwerking

In deze subsectie behandelen we de internationale verdragen die van invloed zijn op het nationale gegevensbeschermingsrecht. De internationalisering van het gegevensbeschermingsrecht zal naar onze verwachting in de toekomst alleen maar groeien. De eenwording van Europa en de daarmee gepaard gaande groei van het grensoverschrijdend gegevensverkeer vragen om een gelijkwaardig beschermingsniveau. Ook voor het gegevensverkeer van de politie is een dergelijke tendens waarneembaar.¹⁶³ We behandelen hieronder: (a) EVRM, (b) EHRM, (c) IVBPR, (d) het Databeschermingsverdrag, en (e) Aanbeveling (85)R15 van de Raad van Europa en (f) regelgeving Europese Unie.

Ad (a) EVRM

Art. 8 Europees Verdrag voor de Rechten van de Mens (EVRM) voorziet in een algemene beschermingsbepaling voor de persoonlijke levenssfeer. Het artikel ziet dus niet specifiek op de bescherming van persoonsgegevens, maar geeft een ieder het 'recht op respect voor zijn privé-leven, zijn familie- en gezinsleven, zijn woning, en zijn correspondentie'.¹⁶⁴ Een inmenging in de uitoefening van dit recht is slechts toegestaan wanneer daarin is voorzien bij wet en als deze inmenging noodzakelijk is in een democratische samenleving als het gaat om "de nationale veiligheid, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen".¹⁶⁵

Ad (b) EHRM

Onder het beschermingsbereik van art. 8 EVRM moet inmiddels ook het gebruik van persoonsgegevens gerekend worden. De reikwijdte van dat beschermingsbereik wordt thans nog steeds in sterke mate beïnvloed door twee arresten van het Europees Hof voor de Rechten van de Mens (EHRM) uit de jaren tachtig. In het Leander-arrest bepaalde het EHRM dat het registreren en verstrekken van bepaalde informatie over de heer Leander uit een geheim veiligheidsregister een schending van art. 8 lid 1 EVRM opleverde. Daarbij nam het Hof in overweging dat hem de mogelijkheid tot weerlegging van die gegevens werd onthouden. Het EHRM oordeelde uiteindelijk dat de inmenging werd gerechtvaardigd doordat een dergelijke handeling noodzakelijk was ter bescherming van de nationale veiligheid.¹⁶⁶

Het tweede, in dit verband veel besproken, arrest van het EHRM is de zaak Gaskin. Hierin werd door het EHRM een schending van art. 8 aangenomen, omdat voor het verkrijgen van toegang tot de persoonsgegevens van de heer Gaskin niet was voorzien in een procedure. Daardoor kon Gaskin geen kennis nemen van de informatie die hem zijn jeugd en ontwikkeling

¹⁶³ Verbeek, 2004. De Vlieger en Verstuyft, 2007.

¹⁶⁴ Art. 8 lid 1 EVRM

¹⁶⁵ Art. 8 lid 2 EVRM

¹⁶⁶ EHRM, 26 maart 1987, Serie A, Vol. 116.

zou kunnen helpen te leren kennen en begrijpen. Dat raakte volgens het EHRM een 'vital interest'.¹⁶⁷

Aangezien het tweede lid een inbreuk op de persoonlijke levenssfeer in geval van 'het voorkomen van [...] strafbare feiten' toelaat, lijkt het verwerken van politiegegevens een dergelijke rechtvaardiging te zijn. Het bestaan van een dergelijke uitzonderingsmogelijkheid betekent uiteraard niet direct dat iedere verwerking van persoonsgegevens daarmee kan worden gerechtvaardigd. De verwerking moet noodzakelijk zijn met het oog op het doel van de verwerking. Daarbij gaat het volgens het EHRM om de eisen van proportionaliteit en subsidiariteit. Daarnaast moet er sprake zijn van een 'pressing social need'. Een dergelijke toets van het EHRM wordt gekenmerkt door de omstandigheid dat de betreffende staat een '*margin of appreciation*' heeft. Dat brengt met zich mee dat de noodzakelijkheid van een gegevensverwerking een belangrijke rol speelt bij de vraag of er een ongerechtvaardigde schending van art. 8 plaatsvindt. Met het opnemen van verschillende noodzakelijkheidstoetsen in de Wpolr vroeger, evenals in de Wpolg nu, heeft de wetgever ervoor gekozen die noodzakelijkheidstoets in de praktijk bij uitvoerders van de wetgeving te leggen. Art. 10 Wpolg bepaalt bijvoorbeeld dat gegevens uit het register zware criminaliteit in ieder geval dienen te worden verwijderd indien deze niet meer noodzakelijk zijn voor het doel waarvoor het register wordt gehouden.

Het voorgaande betekent echter niet dat de wetgever daarmee aan zijn verdragsrechtelijke verplichting heeft voldaan. Naast de noodzakelijkheidstoets stelt het EHRM bepaalde kwaliteitseisen aan de wetgeving. Zo moet de inbreuk op de persoonlijke levenssfeer door het gebruik van persoonsgegevens toegankelijk en voorzienbaar zijn. Dit betekent dat de burger kennis moet kunnen nemen van de regelingen over het gebruik van persoonsgegevens en dat hij daaruit moet kunnen afleiden welke persoonsgegevens onder welke omstandigheden mogen worden verwerkt. Daarnaast moet wetgeving van een dusdanige kwaliteit zijn dat vooraf duidelijk is voor welke doeleinden en onder welke voorwaarden gegevens mogen worden verwerkt. Voor zover het gaat om de verwerking van politiegegevens heeft de wetgever daarin in de Wpolg voorzien.

Het EHRM stelt tevens dat het bij de kwaliteit van wetgeving niet alleen gaat om de voorwaarden waaronder informatie mag worden verzameld en verwerkt. Ook worden eisen gesteld aan de maatregelen die moeten waarborgen dat geen misbruik gemaakt wordt van de in de wet neergelegde bevoegdheden. Een goed voorbeeld in deze is de zaak Rotaru waarin het Hof stelt:

"[...] interference by the executive authorities with an individual's rights should be subject to effective supervision, which should normally be carried out by the judiciary, at least in the last resort, since judicial control affords the best guarantees of independence, impartiality and a proper procedure[...]".¹⁶⁸

167 EHRM, 7 juli 1989, Series A, Vol. 160.

168 EHRM, 4 mei 2000, reports 2000, r.o. 59.

Het EHRM geeft daarmee aan dat het treffen van een wettelijke regeling alleen niet afdoende is. Er moet sprake zijn van *'adequate and effective safeguards'* die in de wet zijn vastgelegd. Zij stelt zelfs dat als daarin niet wordt voorzien het gevaar dreigt dat met dergelijke veiligheidsmaatregelen de democratie geweld wordt gedaan in plaats van te worden verstevigd.¹⁶⁹ Of een specifiek systeem van maatregelen adequaat en effectief is moet volgens het EHRM worden beoordeeld aan de hand van de omstandigheden van het geval.¹⁷⁰

Hoewel het in de betreffende zaken een vorm van *'secret surveillance'* betrof, acht de wetgever dit ook van toepassing op de reguliere verwerking van persoonsgegevens.¹⁷¹ Wat precies onder *'surveillance'* moet worden verstaan is niet duidelijk. Het lijkt dan te gaan om een vorm van toezicht of observatie door de overheid op burgers. Schermer heeft dit onderwerp uitgebreid behandeld.¹⁷² Wat hier ook van zij, het verwerken van persoonsgegevens door inlichtingendiensten, zoals de CIE-en, wordt genormeerd door art. 8 EVRM. Onder dat beschermingsbereik valt ook het vereiste van de aanwezigheid van effectieve waarborgen die het gebruik van persoonsgegevens reguleren en normeren.

Ad (c) IVBPR

Een verdrag dat grote gelijkenis vertoont met het EVRM is het Internationaal Verdrag inzake Burgerlijke en Politieke Rechten. In dit verdrag is dan ook een soortgelijke bepaling als art. 8 EVRM opgenomen. Art. 17 IVBPR bepaalt:

- “1. Niemand mag worden onderworpen aan willekeurige of onwettige inmenging in zijn privéleven, zijn gezinsleven, zijn huis en zijn briefwisseling, noch aan onwettige aantasting van zijn eer en goede naam.
2. Een ieder heeft recht op bescherming door de wet tegen zodanige inmenging of aantasting.”

Er zijn twee belangrijke factoren die eraan bijdragen dat aan art. 17 IVBPR in de praktijk minder betekenis toekomt dan zijn grote broer uit het EVRM. Ten eerste komt dat door de vage bewoordingen van deze bepaling. Daardoor zijn het beschermingsbereik en de vereisten waaronder inmenging met dat recht is toegelaten, onduidelijk. In het verlengde daarvan ligt de tweede oorzaak. Door het ontbreken van een rechtsprekend orgaan, zoals het EHRM, is er geen uniforme uitleg van art. 17 IVBPR.

169 EHRM, 4 mei 2000, reports 2000, r.o. 59.

170 EHRM, 6 september 1978, Series A, vol. 28, r.o. 50.

171 Bij de verhandeling van de regering over de gevolgen van het gebruik van persoonsgegevens in het licht van art. 8 EVRM.

172 Schermer, 2007, p. 35-47.

Ad (d) Het databeschermingsverdrag

Het Verdrag van Straatsburg (databeschermingsverdrag) is de eerste regeling die specifiek ziet op het reguleren van het gebruik van persoonsgegevens in geautomatiseerde gegevensbestanden.¹⁷³ Het is al in 1993 in Nederland in werking getreden. De reden voor de opstelling van het verdrag is de opkomst van het computergebruik in administratieve procedures. Meer gegevens worden daardoor opgeslagen en de gebruiksmogelijkheden daarvan nemen toe. Dit brengt met zich mee dat steeds meer beslissingen op die gegevensbestanden zullen worden gebaseerd. In het *'explanatory report'* bij het databeschermingsverdrag wordt dit *'information power'* genoemd. Deze *'kennis is macht'* brengt verantwoordelijkheden met zich mee voor degenen die persoonsgegevens verwerkt. Deze zijn neergelegd in het databeschermingsverdrag.

Het verdrag heeft geen directe werking. Een burger kan in een gerechtelijke procedure dus geen direct beroep doen op een schending van een verdragsbepaling. De normale verdragsrechtelijke werking van het databeschermingsverdrag verplicht Nederland wel haar nationale regelgeving met het verdrag in overeenstemming te brengen en daarmee ook de regelingen rond het gebruik van politiegegevens.¹⁷⁴

Het databeschermingsverdrag gaat uit van een aantal basisbeginselen waaraan in ieder geval tegemoet zou moeten worden gekomen door de staten die het verdrag hebben ondertekend. Deze zijn neergelegd in de artt. 4 t/m 11. We behandelen deze artikelen hieronder in het kort. Art. 4 legt de verplichting aan iedere staat op om in zijn nationale wetgeving uitvoering te geven aan deze basisbeginselen. Art. 5 ziet op de kwaliteit van de gegevens. Dit artikel bepaalt onder meer dat (1) de gegevens eerlijk en rechtmatig moeten worden verkregen en verwerkt en dat (2) deze gegevens alleen voor een specifiek en legitiem doel mogen worden opgeslagen. Art. 6 definieert een aantal gegevens als gevoelige gegevens. Deze mogen niet automatisch worden verwerkt zonder dat daarbij is voorzien in passende waarborgen. Dat geldt ook voor informatie die gerelateerd is aan strafrechtelijke veroordelingen. Art. 7 vereist dat passende beveiligingsmaatregelen worden genomen zodat de gegevens en de gerelateerde informatie beschermd zijn tegen onder meer ongeautoriseerde toegang of verandering van gegevens en informatie. Art. 8 stelt dat de persoon wiens persoonsgegevens worden verwerkt een aantal rechten moet krijgen die het mogelijk maken dat hij tot op zekere hoogte invloed kan uitoefenen op de geautomatiseerde verwerking van persoonsgegevens. Een in dit verband belangrijke uitzondering is opgenomen in art. 9 lid 2 onder a. Daarin staat namelijk dat van de artt. 5, 6, en 8 mag worden afgeweken indien dit bij wet is voorgeschreven en dit noodzakelijk

173 Verdrag tot bescherming van personen met betrekking tot de 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.

174 Art. 3 lid 1 Databeschermingsverdrag.

is in een democratische samenleving ter onderdrukking van criminele misdrijven. Niet onder deze afwijkingsbepaling valt de verplichting voortvloeiend uit art. 10. Hierin wordt de staat verplicht om zorg te dragen voor passende sancties en maatregelen die moeten waarborgen dat de regelingen, die uitvoering geven aan de genoemde basisbeginselen, worden nageleefd.

Art. 10 van het verdrag raakt daarmee aan het hart van de doelstellingen die de lidstaten van de Raad van Europa voor ogen hadden bij de opstelling ervan. Het doel van de optekening van deze basisbeginselen was meer waarborgen te creëren voor ieders rechten en vrijheden, vooral het recht op privacy, in de bescherming tegen geautomatiseerde gegevensverwerkingen.

Ad (e) Aanbeveling (85)R15 van de Raad van Europa

Binnen de Raad van Europa is na vaststelling van het databeschermingsverdrag door de raad van ministers een aanbeveling opgesteld voor de verwerking van persoonsgegevens door de politie. Anders dan het databeschermingsverdrag bindt deze aanbeveling de staten niet aan de inhoud ervan. Er is voor de betrokken staten slechts een morele verplichting om zich conform het in de aanbeveling bepaalde te gedragen. In het opstellen van nationale regelingen dienen ze daar dan ook zoveel mogelijk rekening mee te houden.

Het doel van de aanbeveling ligt erin een grotere eenheid te scheppen in de verwerking van politiegegevens tussen de verschillende lidstaten. Daarbij is het volgens de Raad van Europa noodzakelijk om een evenwicht te zoeken tussen enerzijds het gebruik van geautomatiseerde gegevensbestanden door de politie en anderzijds de bescherming van de privacy van de individuele burger. De bedreiging voor de privacy zit hem daarbij voornamelijk in het misbruik van de geautomatiseerde methoden van gegevensverwerking.

De aanbeveling werkt de basisbeginselen van het databeschermingsverdrag uit. Lidstaten worden geacht rekening te houden met de in de aanbeveling gegeven richtsnoeren. Daarbij gaat het om controle en notificatie, het verzamelen van informatie, het opslaan, het gebruik, de verspreiding, de bewaartermijnen, en de beveiliging. In het kader van dit onderzoek is met name het element 'controle en notificatie' interessant. De aanbeveling stelt dat iedere lidstaat een onafhankelijke organisatie dient te hebben die buiten de politieorganisatie staat en verantwoordelijkheid draagt voor de naleving van het bepaalde in de aanbeveling. In Nederland is dat het CBP.

Ad (f) Regelgeving Europese Unie

Op basis van het EG-verdrag zijn een aantal richtlijnen opgesteld waarin regels en normen worden gegeven voor de verwerking van persoonsgegevens.¹⁷⁵ Omdat deze regels en normen gebaseerd zijn op het EG-verdrag,

¹⁷⁵ Richtlijn 94/46/EG van het Europees Parlement en de Raad van de Europese Unie van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (PbEG 1995, L 281) en Richtlijn 97/66/EG van het Europees Parlement en de Raad van de Europese Unie van 24 oktober 1995 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de telecommunicatiesector (PbEG 1998, L 24).

strekken ze niet tot de verwerking van politiegegevens. De richtlijnen zullen hier dan ook niet verder behandeld worden. Als het gaat om de verwerking van politiegegevens zijn er in EU-verband afspraken gemaakt over de internationale samenwerking.¹⁷⁶ De laatste ontwikkeling op dat gebied is het zogenaamd Zweeds Kaderbesluit. Dit kaderbesluit tracht kort gezegd de uitwisseling van politiegegevens op Europees niveau te vereenvoudigen, onder meer door de verstrekking van politiegegevens zonder tussenkomst van een officier van justitie of rechter mogelijk te maken.¹⁷⁷ Het verstrekken van CIE-informatie naar het buitenland blijft in beginsel echter alleen mogelijk met toestemming van de CIE-officier van justitie en geschiedt uitsluitend via NCIE.¹⁷⁸ Het kaderbesluit bevat geen normen over de wijze waarop politiegegevens op nationaal niveau verwerkt dienen te worden. Aangezien ons onderzoek niet tot doel heeft de internationale uitwisseling van politiegegevens te bespreken (zie sectie 1.3) volstaan we hier met deze bespreking van het kaderbesluit. Wel merken we nog op dat de verplichtingen die uit het Zweeds kaderbesluit voortvloeien in de Wpolg en de daarbij behorende regelingen zijn doorgevoerd, zodat met het vervullen van de verplichtingen uit de Wpolg, tevens aan de verplichtingen uit het kaderbesluit is voldaan.

3.4.2 Nationale regelgeving

De hierboven beschreven ontwikkelingen hebben ertoe geleid dat met de grondwetsherziening de informatieve privacy in de grondwet is neergelegd. Art. 10 lid 2 en 3 bepalen:

- "2. De wet stelt regels ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens.*
- 3. De wet stelt regels inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van zodanige gegevens."*

Daarmee werd het treffen van regelingen die het gebruik van persoonsgegevens reguleren en normeren niet alleen politiek wenselijk, maar ook grondwettelijk verplicht. Op aanzet van de commissie Koopmans was de Wet persoonsregistraties (Wpr) in die tijd dan ook onderwerp van discussie. Deze is uiteindelijk in 1989 in werking getreden. De werkingssfeer van de Wpr strekte echter niet tot het gebruik van persoonsgegevens door de politie.¹⁷⁹

¹⁷⁶ Kranenborg, 2007, p. 104 e.v.

¹⁷⁷ Het Kaderbesluit van de Raad betreffende de vereenvoudiging van de uitwisseling van informatie en inlichtingen tussen de rechtshandhavingsautoriteiten van de lidstaten van de EU van 18 december 2006, 2006/960/JBZ, PbEG L 386/89.

¹⁷⁸ Art. 5:1lid 6 Bpolr.

¹⁷⁹ Art. 2 lid 3 onder B Wpr.

Datzelfde geldt voor de vervanger van de Wpr, de Wbp.¹⁸⁰ De wetgever achtte het toen noodzakelijk de verwerking van persoonsgegevens in een apart wettelijk kader onder te brengen. Dat is uiteindelijk 2 jaar na de inwerkingtreding van de Wpr gebeurd. In de Wpolr zijn domeinspecifieke regels en normen opgenomen die het gebruik van persoonsgegevens door de politie reguleren. Deze hebben een tweeledige waarborgfunctie.¹⁸¹ Ten eerste is er een afweerrecht, dat wil zeggen dat een afweging tussen de betrokken belangen dient te worden gemaakt alvorens persoonsgegevens mogen worden gebruikt. Ten tweede, en belangrijker, heeft de wetgeving een beschermingsfunctie geïntroduceerd die wordt verwezenlijkt door het stellen van zorgvuldigheidseisen aan de politieke gegevensverwerkingen. De Wpolg heeft, ondanks een andere afweging tussen belang A en belang B, nog steeds dezelfde uitgangspunten.

Zes redenen voor een aparte wet

De wetgever noemde destijds zes redenen om een apart regime voor de verwerking van politiegegevens in te stellen.¹⁸² Ten eerste gaat het bij de verwerking van politiegegevens om heel andersoortige gegevens dan in andere gegevensverzamelingen worden verwerkt. Het gaat namelijk om gegevens die veelal niet van de persoon zelf afkomstig zijn en er is in de meeste gevallen geen toestemming verleend voor de verwerking van deze gegevens. Dit laatste is een van de vereisten voor een rechtmatige gegevensverwerking onder de Wbp.¹⁸³ Ten tweede gaat het bij het gebruik van persoonsgegevens vrijwel uitsluitend om de verwerking van gevoelige gegevens. Zij duiden namelijk op een vorm van betrokkenheid bij criminaliteit. Dergelijke gegevens worden zowel door nationale als internationale regelingen als gevoelig aangeduid.¹⁸⁴ Dat rechtvaardigt volgens de wetgever de instelling van een apart regime voor de verwerking van persoonsgegevens. Ten derde is de verhouding tussen de politie en de burger als bijzonder aan te merken. In de verhouding tussen de overheid en de burger is er de voortdurende dreiging dat de belangen van de burger ondermijnd worden. Er is sprake van een gezagsverhouding die beteugeling behoeft, vooral als het gaat om politieoptreden. De politie treedt namelijk juist op die momenten op, wanneer die verhouding onder druk komt te staan. Ten vierde was er een toename van technieken die het koppelen van gegevensbestanden vereenvoudigde. De wetgever achtte het noodzakelijk voor zover dit het koppelen van politiegegevens betreft, dat er speciale waarborgen voor opgenomen zouden worden. Ten vijfde brengen politiegegevens met zich mee dat, anders dan bij normale persoonsgegevens, de inzage ervan door de burger beperkt dient te worden.

180 Art. 2 lid 2 onder C Wbp.

181 Overkleef-Verburg, 1995, p. 23.

182 *Kamerstukken II*, 1985/86, 19 589, nr. 3, p. 2-4.

183 Art. 8 onder a Wbp.

184 Art. 16 Wbp, art. 6 Databeschermingsverdrag.

Ten zesde brengt de gevoeligheid van de inhoud van politieregisters met zich mee dat het wenselijk is om in de wet vast te leggen wie voor de verwerking van die gegevens verantwoordelijk is.

Op basis van deze overwegingen is besloten een aparte wet in te voeren voor de verwerking van politiegegevens, naast de Wbp. Daarmee werd volgens de wetgever uitvoering gegeven aan art. 10 van de GW en het Databeschermingsverdrag.¹⁸⁵ In hoofdstuk 4 wordt een gedetailleerde analyse gegeven van de oude Wpolr, alsmede van de nieuwe Wpolg.

3.4.3 Naar een zelfstandig grondrecht?

De internationale en nationale regelingen lijken op het eerste gezicht de verwerking van persoonsgegevens te benaderen vanuit privacyperspectief. Toch signaleren wij ook op dat gebied ontwikkelingen die passen in de door ons in subsectie 3.3.4 opgeworpen vraag of de beperking tot privacy volstaat. Zo is in een handvest van de EU¹⁸⁶, evenals in de 'Europese Grondwet'¹⁸⁷, het gegevensbeschermingsrecht in een apart artikel opgenomen. Daar lijkt het besef dat gegevensbescherming meer omvat dan alleen privacy voet aan de grond te krijgen. Het werd bovendien zodanig belangrijk geacht dat het een zelfstandig positie binnen de regeling verdient. Met andere woorden, het gegevensbeschermingsrecht wordt zo belangrijk geacht dat de beschermende werking van de reeds bestaande fundamentele rechten (waaronder, maar niet beperkt tot het recht op privacy) kennelijk niet voldoende wordt geacht. Gegevensbescherming wordt zodoende steeds meer als zelfstandig grondrecht benaderd en wordt dus gescheiden van de privacy. Als belangrijkste argument daarvoor geldt dat de privacybenadering niet volstaat. Zo concluderen De Hert en Gutwirth, op grond van deze Europese ontwikkelingen en de grondslagen van het gegevensbeschermingsrecht in andere Europese landen, dat: "there are several grounds for data protection, which does not allow the use of one general privacy label".¹⁸⁸

Het voorgaande maakt duidelijk dat de beschermende functie van de Wet politiegegevens op internationaal niveau niet langer tot privacy beperkt kan worden. Op nationaal niveau is een dergelijke grondwettelijke ontwikkeling niet waarneembaar. Wel zijn ook daar vanuit de literatuur al langer geluiden die voor een scheiding van privacy en gegevensbeschermingsrecht pleiten. Het feit dat het gegevensbeschermingsrecht de privacyjas van zich afschudt heeft kort gezegd consequenties voor de plaatsing van het recht in de grondwet. Zoals beschreven is deze regeling thans nog onderdeel van de bescherming van de persoonlijke levenssfeer, neergelegd in art. 10 van de

185 *Kamerstukken II*, 1985/86, 19 589, nr. 3, p. 4.

186 Art. 8 The Charter of Fundamental Rights. Het handvest is te downloaden op: http://europa.eu.int/comm/justice_home/unit/charte/en/charter02.html.

187 Art. II-68 verdrag ter vaststelling van een Europese Grondwet.

188 De Hert en Gutwirth, 2003, p. 126.

grondwet. Blok heeft reeds in 2002 betoogd dat de leden 2 en 3 van art. 10 van de grondwet geschrapt zouden moeten worden.¹⁸⁹

Dit leidt tot de vraag of het gegevensbeschermingsrecht een zelfstandige positie in de grondrechtencatalogus verdient of dat de beschermende werking van de reeds bestaande grondrechten volstaat. Als werkhypothese gebruiken we hier *het recht op vrijheid van gegevens*, als mogelijke grondwettelijke basis van het gegevensbeschermingsrecht. De vraag of de ontwikkeling van het gegevensbeschermingsrecht daartoe noopt is echter omvangrijk, zowel staats- en verdragsrechtelijk als op praktisch niveau. Het gaat dan onder meer om de inhoud en reikwijdte van het recht op de vrijheid van gegevens en de vraag of hierdoor een aparte positie tussen de bestaande grondrechten gerechtvaardigd wordt. Het laatste punt is door de commissie grondrechten in het digitale tijdperk aan de orde gesteld. Zij hebben onderzocht of het recht op privacy, zoals dat is neergelegd in art. 10 Gw, gewijzigd zou moeten worden naar aanleiding van de technologische ontwikkelingen die zich tot 2000, het jaar van het rapport van de commissie, hebben voorgedaan. De commissie noemt onder andere een recht op anonimiteit en informatieve zelfbeschikking, zoals dat in Duitsland voet aan de grond heeft gekregen door het Bundesverfassungsgericht.¹⁹⁰ De commissie acht een dergelijke wijziging in de grondwettelijke regulering van de verwerking van persoonsgegevens niet noodzakelijk. Het gaat in de verhandeling van de commissie echter vooral over de wijze van regulering binnen het privacykader.¹⁹¹ De meer fundamentele vraag of de technologische ontwikkeling maakt dat de verwerking van persoonsgegevens meer omvat dan privacy alleen en zo ja, hoever dit strekt, is geen onderwerp van onderzoek geweest. Ook na het rapport van de commissie grondrechten in het digitale tijdperk is de discussie over de inhoud van een recht op vrijheid van gegevens niet op gang gekomen. De door ons geschetste ontwikkeling op internationaal niveau lijkt zich voor wat Nederland betreft in stilte te voltrekken. Die ontwikkeling maakt een fundamentele discussie over de positionering van het gegevensbeschermingsrecht in de grondrechtencatalogus echter wel noodzakelijk. Het voeren van die discussie gaat het bestek van deze dissertatie te buiten. We komen hier in onze aanbevelingen in hoofdstuk 7 op terug.

3.5 GEGEVENSVERWERKING EN TECHNOLOGIE

De technologische ontwikkelingen aan het einde van de twintigste eeuw waren voor de regering aanleiding om de commissie Franken in te stellen. De commissie werd gevraagd te onderzoeken in hoeverre de Grondwet aanpassing behoefde aan de opkomst van de informatiemaatschappij. In haar

189 Blok, 2002, p. 72.

190 Franken e.a., 2000, p. 125-126.

191 Franken e.a., 2000, p. 125-127.

rapport typeerde de commissie Grondrechten in het Digitale Tijdperk het grondwettelijke systeem als volgt:

“Bij het sobere karakter van de Grondwet past dat een informatierecht alleen dan als grondrecht behoort te worden opgenomen als dit recht waarlijk essentieel is voor het persoonlijk en maatschappelijk functioneren van burgers. Het open systeem van de Grondwet brengt met zich mee dat ook niet alle grondrechten in de Grondwet behoeven te worden opgenomen.”

De commissie oordeelde dat de verwerkingen van persoonsgegevens dusdanig in vorm en omvang waren toegenomen dat enkele wijzigingen in de tekst van art. 10 van de Grondwet nodig waren. De commissie stelde voor om in lid 2 te spreken van de ‘verwerking van persoonsgegevens’ in plaats van het enkel ‘vastleggen en verstrekken van persoonsgegevens’. Daarmee werd aansluiting gezocht bij de ontwikkelingen rond de Wbp op dat moment. Hetzelfde gold voor de voorgestelde wijziging van het derde lid van art. 10 Gw, waarin onder meer de rechten van de geregistreerde waren opgenomen. Deze zijn echter in het licht van de veranderingen in het gebruik van persoonsgegevens nu niet meer afdoende.

De grondwettelijke regelingsopdracht voor het gebruik van persoonsgegevens was reeds techniekonafhankelijk geformuleerd. Die techniekonafhankelijke formulering komt voort uit het feit dat de daadwerkelijke privacybescherming niet door de Grondwet wordt geboden. Zij legt de formele wetgever immers ‘slechts’ de plicht op om het gebruik van persoonsgegevens te reguleren. Door de regulering en normering daarvan in lagere regelgeving wordt daadwerkelijke bescherming geboden aan de informatiele privacy.

Hoewel de technologische ontwikkelingen aanleiding waren voor het onderzoek van de commissie Franken kan die ontwikkeling niet op zichzelf worden gezien. Al in de jaren zeventig, bij de opkomst van de discussie rond het gebruik van persoonsgegevens, stelde de commissie Koopmans het volgende.

“De mate, waarin de persoonlijke levenssfeer zou kunnen worden bedreigd door de registratie van persoonsgegevens, wordt vooral door technische factoren bepaald. Waar thans reeds kan worden vastgesteld, dat mogelijkheden tot aantasting aanwezig zijn, moet worden aangenomen, dat bij een voortschrijdende technische ontwikkeling die mogelijkheden naar aard en omvang zullen toenemen.”¹⁹²

Met andere woorden; de technologische ontwikkelingen zijn van het begin af aan de drijvende kracht geweest achter de ontwikkeling van de informatiele privacy. Het is dus niet zozeer een ontwikkeling van de laatste jaren. Deze stelling kunnen we overigens ook op de andere privacyvarianten toepassen. In de historische ontwikkeling van het privacyrecht blijken voornamelijk technologische ontwikkelingen reden te zijn voor uitbreiding ervan.

192 Staatscommissie Koopmans, ‘Eindrapport van de Staatscommissie bescherming persoonlijke levenssfeer in verband met persoonsregistratie’, Den Haag, 1976, p. 15.

Ook bij de eerste voorvechters van het privacyrecht, Warren en Brandeis, waren technologische ontwikkelingen een belangrijk argument om de privacy object van rechtsbescherming te maken. Dit is niet anders geweest bij de opkomst van de relationele en lichamelijke privacy. Het briefgeheim is op zichzelf bezien het gevolg geweest van de drukkunst als technologische ontwikkeling. Ook de opkomst van telegraaf- en telefoonverkeer, en met name de technische mogelijkheden om dit verkeer te onderscheppen, zijn belangrijke factoren in de discussie rond de relationele privacy. De ontwikkelingen rond de bescherming van de lichamelijke integriteit werden daarnaast in grote mate beïnvloed door de opkomst van forensische onderzoeksmethoden. Bloedproef-onderzoeken ter vaststelling van het alcoholpromillage en DNA-technieken zijn daarvan goede voorbeelden.

De technologiegestuurde ontwikkeling van het gegevensbeschermingsrecht past dus in de ontwikkeling van het privacyrecht in het algemeen. Laatstgenoemde ontwikkeling wordt gekenmerkt door een sterke afhankelijkheid van technologische ontwikkelingen. Daarbij is het van belang op te merken dat in een digitaliserende samenleving normen en waarden veranderen als gevolg van de inburgering van technologieën. Het gaat dan om een geleidelijke verschuiving in ons normbesef, die (deels) het resultaat is van deze nieuwe technologieën. Waar in de jaren zeventig de Nederlandse bevolking in opstand kwam tegen de toenemende registraties vinden we het vandaag de dag kennelijk niet verontrustend dat we in honderden registratiebestanden zijn opgenomen.¹⁹³ Er is kennelijk een bepaalde mate van acceptatie van de noodzaak tot registratie tot stand gekomen. Sterker nog, technologische ontwikkelingen scheppen vanzelfsprekend ook bepaalde verwachtingen bij burgers dat dergelijke technieken worden ingezet. In de strijd tegen het terrorisme is de overheid in zoverre ook gehouden gebruik te maken van de technologische mogelijkheden die er zijn op het gebied van bijvoorbeeld datamining, machine learning, en surveillance.¹⁹⁴ Aan deze verwachtingen is de acceptatie van dergelijke middelen onlosmakelijk verbonden. Het gaat dan om uitbreidingen (zie 3.5.1) of verschuivingen (zie 3.5.2) in bereik van het gegevensbeschermingsrecht. In onze opvatting is het daardoor gepast te onderzoeken in welke mate de technologie onze redenering steunt (zie 3.5.3).

3.5.1 Uitbreiding van het gegevensbeschermingsrecht

Wij constateren dat de opkomst alsmede elke uitbreiding van het privacyrecht voornamelijk worden toegerekend aan technologische ontwikkelingen die op dat moment onvoorziene en soms onwenselijke gevolgen met zich

193 Dit leiden we af uit de hoeveelheid inzageverzoeken die in de particuliere en publieke sector gedaan worden afgezet tegen de hoeveelheid aanwezige registraties. Zwenne e.a., 2007, p. 170-171.

194 Schreuders, 2001, Sietsma, 2006 en Schermer, 2007.

mee brachten. Juist het gegeven dat het rechtsgebied in belangrijke mate door de technologie gestuurd wordt, maakt dat de ontwikkelingsrichting van het rechtsgebied onzeker is. Net zoals in de jaren zeventig de opkomst van de computer in ieder geval de juristen verraste, zal een nieuwe techniek de privacyjuristen in de toekomst wederom verrassen en aanleiding vormen voor een nieuwe discussie over de reikwijdte van het privacyrecht. Als voorbeeld van onze opvatting geven we hier een korte beschrijving van de discussie rond de opkomst van RFID-technieken. RFID staat voor Radio Frequency Identification en maakt door middel van de uitzending van radiosignalen de identificatie van objecten of personen mogelijk. Het gaat bijvoorbeeld om een bij een huisdier ingeplante chip, zodat deze aan de door de chip uitgezonden identificatiecode kan worden herkend. Een andersoortige toepassing is de verwerking van dergelijke chips in supermarktopproducten ter vervanging van de streepjescode of de verwerking ervan in een paspoort of identificatiebewijs. Deze technologie laat zich niet goed rijmen met de huidige benadering van het gegevensbeschermingsrecht, die gebruik maakt van begrippen als ‘persoonsgegevens’, ‘doelbinding’ en ‘verantwoordelijke’. Als gevolg hiervan constateert Terstegge het volgende.

“RFID-technologie luidt naar mijn mening [...] het einde in van bestaande regelgeving zoals de Europese dataproductie richtlijn [...] en onze Wet bescherming persoonsgegevens.”¹⁹⁵

De technologische ontwikkelingen rond RFID leiden om deze reden tot een heroverweging van het beschermingsbereik van het gegevensbeschermingsrecht. Terstegge merkt daarbij op dat de nadruk van het gegevensbeschermingsrecht meer op het voorkomen van nadeel en misbruik zal komen te liggen en minder op een voorafgaande regulering van iedere verwerking van persoonsgegevens, zoals nu het geval is.¹⁹⁶ Dat lijkt ons niet de enige mogelijk reactie. De gegevens die technieken als RFID gebruiken en genereren zijn volgens ons in eerste instantie niet als persoonsgegevens aan te merken. Wat ons betreft brengt deze ontwikkeling twee vragen met zich mee: (1) is een heroverweging van het huidige normatief kader nodig? en (2) is er sprake van een nieuw element van het gegevensbeschermingsrecht dat naast de bestaande regulering van persoonsgegevens wordt opgesteld? Hierbij kan bijvoorbeeld gedacht worden aan een vangnetbepaling in de Wbp die het nadeel en misbruik van gegevens regelt en normeert.

3.5.2 Verschuivingen in het gegevensbeschermingsrecht

Nieuwe technologische ontwikkelingen nopen evenwel niet alleen tot een voortdurende heroverweging of *uitbreiding* van het beschermingsbereik. Ook

¹⁹⁵ Terstegge, 2005, p. 29-39.

¹⁹⁶ Terstegge, 2005, p. 39.

kunnen ze leiden tot gewenste en ongewenste *verschuivingen* in het beschermingsbereik. We doelen op technologische ontwikkelingen die tot gevolg hebben dat de Wpolg of de Wbp aan een dergelijke verwerking van persoonsgegevens (andere) eisen gaat stellen. Een goed voorbeeld is de opkomst van digitale videotechnieken. Deze worden bijvoorbeeld gebruikt voor het digitaal surveilleren. Ter uitvoering daarvan worden in openbare ruimtes camera's opgehangen en op het politiebureau worden vanuit de surveillancekamer deze beelden bekeken. Doordat live video niet in een bestand wordt opgenomen is de Wpolg op deze gegevensverwerking niet van toepassing. Art. 2 Wpolg bepaalt immers dat de wet van toepassing is op de verwerking van politiegegevens die in een bestand zijn opgenomen of die bestemd zijn daarin te worden opgenomen. Een bestand is elk gestructureerd geheel van politiegegevens, ongeacht of dit geheel van gegevens gecentraliseerd of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen.¹⁹⁷ Aangezien live-videobeelden, anders dan videobeelden die op een tape worden opgenomen, geen geheel van gegevens vormen, valt deze vorm van gegevensverwerking niet onder het bereik van de Wet politiegegevens.

Voor de komst van deze surveillancekamers kon toezicht door middel van camera's alleen worden uitgevoerd indien de beelden werden opgenomen op een band, een bestand, zodat het gegevensbeschermingsrecht daarop van toepassing was. Nu digitale technieken het mogelijk maken dat live-videobeelden op de surveillancekamer worden uitgelezen zonder dat daarvan een bestand behoeft te worden gemaakt, heeft dit tot gevolg dat deze vorm van surveillance niet meer onder het bereik van de Wpolg valt. Daarmee heeft de technologische ontwikkeling op het gebied van videoapparatuur tot gevolg dat het cameratoezicht dat thans bij verschillende politie-regio's wordt uitgevoerd niet onder het bereik van het gegevensbeschermingsrecht valt. Het voorbeeld maakt duidelijk dat de techniek er niet alleen voor kan zorgen dat het gegevensbeschermingsrecht uitgebreid dient te worden, maar ook dat er verschuivingen kunnen plaatsvinden.

3.5.3 Technologie stuurt

De wetgever tracht zowel de uitbreidingen van het beschermingsbereik als de verschuivingen binnen het beschermingsbereik van te voren te ondervangen door de wetgeving techniekonafhankelijk te formuleren. Die ambitie is naar onze overtuiging maar tot op zekere hoogte haalbaar. Een techniekonafhankelijke formulering is namelijk altijd tot op zekere hoogte afhankelijk van de stand van de techniek op het moment van de formulering. Bij de bepaling of een wetsartikel onafhankelijk van de techniek wordt geformuleerd, is immers de op dat moment geldige stand van de techniek bepalend.

197 Art. 2 onder c Wpolg.

Zowel juristen als de wetgever zijn niet (of slechts deels) in staat te anticiperen op technologieën die nog niet ontwikkeld zijn. De richting waarin de techniek zich ontwikkelt, is immers voor een groot deel onbekend. Dat op die technieken niet kan worden geanticipeerd laat zich vooral voelen wanneer technologische doorbraken een verschuiving met zich meebrengen in de manier waarop persoonsgegevens worden verwerkt. Als voorbeeld noemen we agenttechnologie.¹⁹⁸ De ontwikkeling van agenttechnologie heeft, wat de omgang met persoonsgegevens betreft, als grote doorbraak dat gegevensverwerkingen (opslaan, bewaren, verstrekken, koppelen, en analyseren) niet meer uitsluitend door natuurlijke personen kunnen worden uitgevoerd. Met de toepassing van agenttechnologie wordt het mogelijk dat – eenvoudig gezegd – computers afwegingen maken die tot voor kort aan politieagenten waren voorbehouden. Daarbij kan gedacht worden aan de vraag of weigering van een persoonsgegeven aan een lid van het tactische researchteam in overeenstemming is met de goede uitvoering van de politietaak. We noemen dit *computergestuurd* handelen. Een dergelijke technologische mogelijkheid was bij de totstandkoming van de Wpolg nog niet voorzien, die gaat namelijk uit van persoonlijk geautoriseerde politieambtenaren voor het verwerken van gegevens. We noemen dat *mensgestuurd* handelen. De vraag in hoeverre het een geautoriseerde ambtenaar is toegestaan die bevoegdheid te mandateren of delegeren aan een computer is door de wetgever onbeantwoord gelaten. De huidige gegevensbeschermingsregelingen gaan uit van gecentraliseerde gegevensverwerkingen en zijn niet of slecht berekend op de opkomende gedistribueerde systemen, zoals het internet en bijvoorbeeld agenttechnologie. Inzet van dergelijke nieuwe ICT-technieken roept dan ook een veelheid aan juridische vragen op.¹⁹⁹ Het voorbeeld van agenttechnologie maakt duidelijk dat grote onvoorziene en dus meer rigoureuze technologische wijzigingen altijd afbreuk zullen doen aan de mate waarin de op dat moment geldende wetgeving als technologieonafhankelijk kan worden bestempeld. Techniekonafhankelijkheid is naar onze overtuiging vergankelijk. Nieuwe technologieën kunnen er wel degelijk voor zorgen dat de techniekonafhankelijkheid van de wetgeving afneemt of zelfs verdwijnt. Zo concludeert Terstegge naar aanleiding van de opkomst van RFID het volgende:

*“Onze huidige zogenoemd ‘technologieneutrale’ privacyprincipes die dateren van de hoogtijdagen van de mainframe computer en het begin van het internettijdperk naderen het einde van hun houdbaarheid.”*²⁰⁰

Illustratief is verder de aanzet die Schermer geeft in zijn dissertatie:

198 Schermer, 2007, p. 143-144.

199 Schermer, 2007, 168-169 en Koelewijn, 2009, p. 207.

200 Terstegge, 2005, p. 39.

*"In the area of the law, additional study into [...] the changes of a legal-technical nature that are necessary to deal with the qualitative effects of agent technology [on the legal framework] should be examined further."*²⁰¹

Met betrekking tot politieke gegevensverwerking concluderen Koelewijn en Kielman dat de toepassing van nieuwe technieken, specifiek agenttechnologie, in het domein van politieke gegevensverwerking tot toepassingsproblemen leiden.²⁰² De techniekonafhankelijke formulering van wetgeving is dan ook slechts gedeeltelijk realiseerbaar en is slechts toepasbaar op marginale wijzigingen in de techniek, waarbij de technologische uitgangspunten voor regulering hetzelfde blijven.

Wetgeving die ziet op de regulering en normering van gegevensverwerkingen waarbij technologische ontwikkelingen een bepalende factor zijn, kan daarom niet techniekonafhankelijk zijn. De formulering van de wetgeving is dit echter wel, zij het in tijd beperkt. Op het moment dat de technologische ontwikkelingen een wijziging met zich meebrengen die afbreuk doet aan de basisstructuur van het gegevensbeschermingsrecht – we zagen reeds een verschuiving van mensgestuurd handelen naar computergestuurd handelen – zal wetgeving daarop moeten worden aangepast. Dit betekent dat de richting van de wetgeving voor een belangrijk deel bepaald wordt door de technologische ontwikkelingen.

Naast de wetstechnische wijzigingen die de technologische ontwikkelingen afdwingen, zagen we in sectie 3.5. dat ook vanuit de maatschappij van de politie verwacht wordt dat zij van nieuwe technologische mogelijkheden gebruik maken bij hun taakvervulling. Aanpassing van wetgeving als gevolg van technologische ontwikkelingen is dan vanuit zowel juridisch-technisch oogpunt als vanuit sociaal-politiek oogpunt noodzakelijk. Techniek heeft daarom een belangrijke sturende werking op de ontwikkeling van het regelgevend kader. De beide belangen die het regelgevend kader beoogt te beschermen worden immers in aanzienlijke mate gestuurd door deze technologische ontwikkelingen.

3.6 BEANTWOORDING OV1

We beantwoorden in deze sectie OV1: *op welke wijze zijn de politietaak en de grondrechten van de burger betrokken bij het verwerken van politiegegevens?* De twee belangen, die bij de politieke gegevensverwerking zijn betrokken, zijn in dit hoofdstuk uitvoerig aan de orde gekomen. Het gaat om (a) de goede uitvoering van de politietaak en (b) het beschermingsbelang. Daarnaast is er uitgebreid stilgestaan bij de ontwikkelingen die in de onderscheiden belangen waarneembaar zijn.

201 Schermer, 2007, p. 216.

202 Koelewijn en Kielman, 2006.

Het eerste betrokken belang is belang A, de goede uitvoering van de politietask (zie sectie 3.1). Daarbij is een toenemende instrumentalistische benadering gesignaleerd. We hebben gezien dat de politieke gegevensverwerking bij een goede uitvoering van de politietask de administratieve en ondersteunende functie inmiddels is ontstegen en als zelfstandig opsporingsmiddel dient te worden aangemerkt. Bevoegdheden die gegevensverwerking in het kader van de uitvoering van de politietask mogelijk maken, hebben we daarbij aangeduid met de term 'informatieele opsporingsmethoden' (zie sectie 3.2). Hiermee ontdoet de Wpolg zich van zijn privacyas en krijgt de politieke gegevensverwerking een grotere strafvorderlijke betekenis. Dit brengt met zich mee dat het tegenwicht dat het tweede betrokken belang, belang B, tegen de instrumentele functie van de Wpolg moet leveren om een adequaat niveau van rechtsbescherming te bieden ook groter dient te zijn dan onder de oude Wpolr.

We zien echter ook dat belang B (het beschermingsbelang) ten tijde van de Wpolr vrijwel uitsluitend vanuit het privacyperspectief werd benaderd. Daarin hebben we een verschuiving gesignaleerd die met de opkomst van de digitale technieken is begonnen. Zoals beschreven is in sectie 3.3 verwierf en verwerft het gegevensbeschermingsrecht zich steeds meer de status van een zelfstandig grondrecht. De belangen die op het spel staan bij de verwerking van persoonsgegevens zijn immers niet alleen privacybelangen, maar beslaan een breder scala aan grondrechten. Op basis van die ontwikkeling hebben we mogen concluderen dat belang B vanuit beschermingsoogpunt een zorgvuldige gegevensverwerking vereist. Mede om die reden is de privacyas van het gegevensbeschermingsrecht te klemmend. Het roept, gelet op de internationale ontwikkelingen, de vraag op of het gegevensbeschermingsrecht als zelfstandig grondrecht geduid zou moeten worden en we toe moeten naar een recht op *vrijheid van gegevens*.

Zowel voor belang A als voor belang B is het onderkennen van de technologiegestuurde ontwikkeling noodzakelijk. Technologische ontwikkelingen geven meer instrumentele mogelijkheden voor belang A en stellen om die reden tegelijkertijd hogere eisen aan belang B. Hoewel technologie niet als een zelfstandig belang kan worden aangemerkt bij de opstelling van regelingen van het gegevensbeschermingsrecht, blijkt zij dus wel een belangrijke sturende factor te zijn in het denken over de betrokken belangen bij de inzet van gegevensverwerkingen. Bij het denken over de rol die gegevensverwerking bij de uitvoering van de politietask kan spelen (sectie 3.2) en bij het denken over de vrijheid van gegevens (sectie 3.3) hebben we laten zien dat de stand van de techniek daarin bepalend is. Dit brengt ons tot de conclusie dat we vooral vanuit die achtergrond moeten kijken naar de maatregelen die de task hebben dat belangen A en B voldoende beschermd worden. Alleen dan kunnen we bepalen of in het huidige tijdsgewricht met de drie bestaande waarborgen (de wet, het kennisnemingsrecht, en controle en toezicht) kan worden volstaan of dat het tempo van de technologische ontwikkelingen verschuiving of uitbreiding van die waarborgen noodzakelijk maakt. We komen hierop terug in hoofdstuk 7, conclusies en aanbevelingen.

In dit hoofdstuk behandelen we OV2 en OV3 aangaande de wet. Ov2 luidt: *“Welke knelpunten zijn er in de literatuur en de praktijk geconstateerd ten aanzien van de waarborgende werking van de Wet politieregisters?”* en Ov3 luidt: *“In hoeverre komt de Wet politiegegevens, mede in het licht van de ervaringen met de Wet bescherming persoonsgegevens, tegemoet aan deze knelpunten?”* Deze twee onderzoeksvragen bepalen de inhoud van de hoofdstukken 4, 5 en 6. Het gaat daarbij over de wet (hoofdstuk 4), het kennisnemingsrecht (hoofdstuk 5) en controle en toezicht (hoofdstuk 6). Voor onze bespreking en analyse onderzoeken we drie wettelijke regelingen: de Wbp, de Wpolr, en de Wpolg. Wij onderzoeken vijf verschillende activiteiten met politiegegevens: (1) opslaan, (2) bewaren, (3) verstrekken, (4) koppelen en (5) analyseren. We identificeren eerst de knelpunten van de verschillende handelingen die ten aanzien van de Wpolr zijn geconstateerd, vervolgens beschouwen en analyseren we de oplossingen die de Wpolg voor deze knelpunten biedt. Dit doen we in het licht van de ervaringen die met de Wbp zijn opgedaan. Op dit punt herhalen we dat we in hoofdstuk 4 de genoemde procedure beschouwen met betrekking tot de wet.

In ons onderzoek houden wij op een wetenschappelijk verantwoorde wijze rekening met de verschillende doelstellingen en de wijze van regulering in de drie wettelijke regelingen (zie sectie 4.1). De daarin bestaande verschillen zijn niet alleen van belang voor de beantwoording van OV2 en OV3, maar vormen ook de aanleiding voor de fundamentele discussie die thans wordt gevoerd over de wijze waarop het gegevensbeschermingsrecht vorm dient te worden gegeven (sectie 4.2). In sectie 4.3 behandelen we vervolgens kort de belangrijkste verschillen in doelstellingen en in de wijze waarop het politieel gegevensbeschermingsrecht onder de Wpolr en de Wpolg vorm heeft gekregen. In sectie 4.4 beschrijven we de wijze waarop we de knelpunten, die onder het regime van de Wpolr zijn geconstateerd, vergelijken met het regime van de Wpolg (we noemen dit de driestappenbehandeling). In de secties 4.5 tot en met 4.9 voeren we voor ieder van de vijf onderdelen (opslaan, bewaren, verstrekken, koppelen en analyseren) een driestappenbehandeling uit. In sectie 4.10 behandelen we de onder de Wbp geconstateerde knelpunten en vervolgens beantwoorden we in sectie 4.11 de tweede en derde onderzoeksvraag aangaande de wet en geven we een hoofdstukconclusie op drie relevante punten.

4.1 DRIE WETTELIJKE REGELINGEN EN HUN DOELSTELLINGEN

In dit hoofdstuk staan de Wpolr en de Wpolg centraal. We zullen evenwel zien dat de Wbp een belangrijke onderliggende rol speelt. Met betrekking

tot de Wpolr en Wpolg zijn de belangen van beide wetten voor de gemeenschap uitgebreid besproken in hoofdstuk 3. De twee regelingen representeren elk een gevonden evenwicht tussen enerzijds het noodzakelijk karakter van gegevensverwerkingen ten dienste van de politietaak en anderzijds de bescherming van de grondrechten van de burger (belang A tegenover belang B). We hebben dat in hoofdstuk 3 geduid als instrumentalisme versus rechtsbescherming.

De Wbp

Aan de Wbp ligt een soortgelijke afweging ten grondslag. Vanzelfsprekend is er bij de Wbp geen sprake van een uitvoering van de politietaak. Gegevensverwerkingen (inclusief verwerkingen van persoonsgegevens) in het kader van de politietaak vallen zelfs niet onder de werking van de Wbp.²⁰³ Behoudens de uitzonderingen uit art. 2 Wbp (waaronder dus de politieke gegevensverwerking) is de Wbp van toepassing op iedere verwerking van persoonsgegevens. De Wbp heeft daarmee het karakter van een omnibuswet. De Wbp is één wet, die in beginsel alle gegevensverwerkingen in Nederland reguleert en normeert. Het instrumentele belang dat de Wbp beschermt is als gevolg daarvan niet zo strak omlijnd als het geval is onder de Wpolr en de Wpolg. Daar waar de Wpolr en de Wpolg de goede uitvoering van de politietaak als enige verwerkingsgrond hebben, wordt er in de Wbp alleen gesproken over doelbinding. Het betekent dat gegevens onder de Wbp alleen in overeenstemming met welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden mogen worden verzameld.²⁰⁴ Deze vage doelbindingsbepaling is open geformuleerd omdat de werking van de Wbp een breed bereik heeft. Ziekenhuizen, financiële instellingen, handelsinformatiebureaus en particulieren zijn enkele voorbeelden van de rechtssubjecten van de Wbp.

Twee doelstellingen

De Wbp is sinds 2001 de opvolger van de Wet persoonsregistraties, die in hoofdstuk 3 is besproken. De privacyrichtlijn 95/46/EG van de Europese Gemeenschap (EG) is met de invoering van de Wbp geïmplementeerd. Tezamen met de doelstellingen van de richtlijn zijn voor een belangrijk deel ook de doelstellingen van de Wbp gegeven. De invoering van de Wbp diende immers om te voldoen aan de implementeringsverplichting van de privacyrichtlijn. Daarbij ging het samenvattend om (1) het realiseren van een beschermingsniveau dat voldoet aan de Europese standaard en (2) het realiseren van een hoogwaardig beschermingsniveau. We behandelen deze beide doelstellingen kort hieronder.

Ad (1) Uit de preambule bij de privacy-richtlijn blijkt dat het vaststellen en handhaven van een hoogwaardig beschermingsniveau één van de doel-

203 Art. 2 onder c Wbp.

204 Art. 7 Wbp.

stellingen is.²⁰⁵ Hoewel er geen directe grondslag is voor deze doelstelling²⁰⁶ wordt zij wel als zodanig geaccepteerd.²⁰⁷ Het belang van een hoog beschermingsniveau verschilt bij gegevensverwerkingen die door de Wbp worden gereguleerd en genormeerd niet van de gegevensverwerkingen die door de Wpolr en Wpolg worden gereguleerd en genormeerd. De Wbp implementeert de Europese standaard van het gegevensbeschermingsrecht in Nederland. In deze Europese standaard is een minimumniveau van bescherming bepaald, waaraan iedere lidstaat dient te voldoen. Het gaat daarbij om de werkingssfeer, de normstelling, de zelfregulering, de controle daarop, alsmede het toezicht. Daarnaast wordt bij de vaststelling van het Europese minimum speciale aandacht besteed aan het beperken van de uitvoeringskosten en de techniekonafhankelijkheid van de regeling.²⁰⁸ In hoofdstuk 3 hebben we reeds de doelstelling van de privacy-richtlijn beschreven, en dus ook de doelstelling van de Wbp.

Ad (2) We merken allereerst op dat er economische belangen bij de uitvaardiging van de privacy-richtlijn zijn. Achteraf gezien kunnen we stellen dat de opkomst van het gegevensbeschermingsrecht in de periode tussen 1970 – 1990 handelsbelemmerend werkte.²⁰⁹ In die tijd ontstond in de verschillende Europese landen evenals in Nederland wetgeving die regels stelde voor de verwerking van persoonsgegevens. Voor internationaal opererende ondernemingen was het vrij eenvoudig om met gebruikmaking van moderne communicatiemiddelen deze wetgeving te omzeilen. Persoonsgegevens werden eenvoudig verzonden naar een land waar geen privacywetgeving bestond en waar gegevens dus verwerkt konden worden zonder daarbij gehinderd te worden door enige privacywetgeving. Het gevolg van deze praktijk was dat landen met een privacywet het doorzenden van persoonsgegevens naar andere landen aan strenge regels onderwierpen of zelfs gingen verbieden. Het moge duidelijk zijn dat dergelijke maatregelen voor internationaal opererende ondernemingen de handel aanzienlijk belemmerde. Daarmee raakte het onderwerp van het gegevensbeschermingsrecht aan een van de fundamenteën van de EG, namelijk het bevorderen van de interne Europese markt. Ter bescherming van de interne markt heeft de EG toen de privacyrichtlijn uitgevaardigd (95/46/EG), die voor harmonisatie in het gegevensbeschermingsrecht moest zorgen. Deze harmonisatie moest op haar beurt weer zorgen voor een gelijkwaardig beschermingsniveau in alle lidstaten van de EG.

205 Preambule Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, PbEG L 281 van 23/11/1995, p. 31-50.

206 Zwenne e.a., 2007, p. 24.

207 Cuijpers, 2004, p. 39-49.

208 Zwenne e.a., 2007, p. 26-37.

209 Van der Klaauw-Koops & Prins, 2002, p. 497. *Kamerstukken II 1992/93*, 22 800 VI, nr. 43.

Twee overeenkomsten tussen de Wpolg (Wpolr) en de Wbp

Er zijn twee duidelijke overeenkomsten tussen de doelstellingen van de Wpolg (en vroeger de Wpolr) enerzijds en de doelstellingen van de Wbp anderzijds. Ten eerste beogen ze beide de informationele privacy van de burger te beschermen. Het verschil dat de regelingen vertonen is gelegen in de reikwijdte van het werkingsgebied, zoals hierboven is beschreven (politietask vs. ruime doelbinding), en in mindere mate in de wijze waarop inbreuk wordt gemaakt op de informationele privacy van de burger. De notie dat de informationele privacybescherming behoeft, blijft evenwel bij elk van de regelingen het uitgangspunt. Ten tweede bevatten beide regelingen een bevoegdheidstoedeling. In hoofdstuk 3 hebben we dit geduid met de term instrumentele belangen. Gelet op het verschil in werkingsgebied van beide regelingen verschilt de manier waarop de Wpolg en de Wbp met deze bevoegdheidstoedeling omgaan aanzienlijk. De Wpolg (en Wpolr) geven de politie de bevoegdheid om gegevens te verwerken ter uitvoering van hun politietask. De bevoegdheid die de Wbp toedeelt is echter breder dan dat. Niet alleen is het aantal personen en instanties dat gegevens onder het regime van de Wbp kan verwerken onbepaald, ook het doel is dat. Daarmee is het belangrijkste verschil tussen aan de ene kant de Wpolg (en Wpolr) en aan de andere kant de Wbp gegeven. Op dit werkingsverschil wordt in de navolgende sectie uitgebreid ingegaan.

4.2 SECTORALE WETGEVING VERSUS OMNIBUSWETGEVING

In het gegevensbeschermingsrecht kan onderscheid gemaakt worden tussen een sectorale benadering en een omnibusbenadering. De sectorale benadering gaat uit van een specialistische vorm van gegevensbeschermingsrecht voor ieder deelgebied. Voorbeelden zijn (1) de medische sector, (2) de financiële sector, en (3) de politieke en justitie sector. De wetgever heeft een aantal sectorale privacyregelingen ingevoerd. De Wpolr en de Wpolg zijn daarvan voorbeelden. Andere sectorale informationele privacyregelingen zijn de Wet gemeentelijke basisadministratie (Wgba) en de Wet justitie sector en strafvorderlijke gegevens (Wjs). De wetgever vindt deze sectoren dusdanig bijzonder dat hij separate wetgeving noodzakelijk achtte. De Wbp reguleert en normeert de gebieden, waar wel persoonsgegevens worden verwerkt, maar waar geen sectorale regeling voor is afgekondigd. Om deze reden wordt in de literatuur de Wbp aangeduid als omnibuswet. In de Wbp zijn in art. 2 de sectoren uitgesloten waarop een sectorale regeling van toepassing is.

Het omnibuskarakter van de Wbp heeft tot gevolg dat de onderdelen ruim en open zijn geformuleerd. Dit leidt in de praktijk tot toepassingsproblemen.²¹⁰ Er is naar aanleiding daarvan veel discussie over de wijze waarop het gegevensbeschermingsrecht vorm zou moeten worden gegeven.

210 Zwenne e.a. 2007, p. 61-65.

We geven een korte beschrijving van deze discussie aan de hand van de meningen van Blok (2002, 2005b), Berkvens (2004b), Cuijpers (2004) en Hustinx (2004). We denken dat het resultaat bruikbare inzichten oplevert voor ons onderzoek. Ook geven we in deze discussie onze eigen mening.

Blok is één van de auteurs die voorstander is van een meer sectorale benadering.²¹¹ Zijn argument is dat de open en vage formuleringen van een omnibuswet tot gevolg hebben dat de toepassing ervan ernstig wordt bemoeilijkt en daardoor aan effectiviteit te wensen overlaat. Sectorale regelingen kunnen specifiekere worden geformuleerd, zodat de toepassing daarvan eenvoudiger is. Daarnaast zou er volgens Blok op deze wijze meer ruimte zijn voor zelfregulering. Bij sectorale wetgeving kan immers per sector worden gezien of regulering wel noodzakelijk is of dat vanwege succesvolle zelfregulering in die sector wetgeving achterwege kan blijven.²¹² Berkvens is om deze redenen vanaf het begin voorstander geweest van een sectorale benadering en pleit ervoor de informatieve privacyregels voor de private sector op te nemen in het burgerlijk wetboek.²¹³ Cuijpers heeft in haar proefschrift deze mogelijkheid onderzocht en concludeert dat dit voor de private sector een aantal knelpunten zou oplossen.²¹⁴

Tegenover deze drie meningen die dezelfde richting uitwijzen waarschuwt Hustinx voor een sectorale benadering.²¹⁵ Dit zou volgens hem leiden tot versnippering met als gevolg dat er een onoverzichtelijk systeem ontstaat waarin allerlei gebieden ongereguleerd blijven. In de eerste fase van de evaluatie Wet bescherming persoonsgegevens kwam eenzelfde kritiek naar voren uit de praktijk van de gegevensbescherming.²¹⁶ Daarnaast biedt volgens Hustinx de omnibusbenadering een aantal voordelen. Zo kunnen daardoor verschillende ontwikkelingen op sectoraal gebied in onderling verband worden aangepakt. Ook is het door de omnibusbenadering beter mogelijk om op nieuwe ontwikkelingen in te springen.²¹⁷

De Wpolr en Wpolg zijn voorbeelden van sectorale privacyregelingen. Ze komen voor een deel overeen met de Wbp, maar zijn op onderdelen ingevuld, aangevuld of gewijzigd met het oog op sectorale elementen die voortvloeien uit de praktijk van politieke gegevensverwerking. Waar in de Wbp bijvoorbeeld is gekozen voor een brede definiëring van begrippen zijn deze in de Wpolr en Wpolg toegesneden op de politiepraktijk. We zullen zien dat veel van de knelpunten die onder de Wpolr in de politiepraktijk zijn geconstateerd voortkomen uit de wijze van regulering. Veel van deze knelpunten worden door de Wpolg niet opgelost. We zullen daarnaast zien dat deze of soortgelijke knelpunten ook onder de werking van de Wbp voorkomen.

211 Blok 2002, p. 304. Blok, 2005, p. 246-252.

212 Blok 2005, p. 246-252.

213 Berkvens 2004b, p. 269.

214 Cuijpers, 2004 p. 375-382.

215 Hustinx 2004, p. 270-272.

216 Zwenne e.a. 2007, p. 67.

217 Hustinx 2004, p. 270-272.

Op basis daarvan mogen we concluderen dat, wat de politieke gegevensverwerking betreft, een groot deel van de problemen die zich bij het gebruik van omnibuswetgeving voordoen, ook niet met sectorale wetgeving kunnen worden opgelost. Onze mening is derhalve dat de bepleite voordelen van sectorale wetgeving slechts enkele deelgebieden beslaan. Het gaat er dan vooral om de specifieke belangen in regelgeving te incorporeren. Ook daar zien we echter dat vaagheid en open normen voor knelpunten zorgen, zoals we ten aanzien van politieke gegevensverwerking in de secties 4.5 tot en met 4.9 zullen zien. Sectorale wetgeving in plaats van omnibuswetgeving biedt echter geen oplossing voor de meeste knelpunten die zich onder de werking van het gegevensbeschermingsrecht voordoen.

4.3 VERSCHIL IN WIJZE VAN REGULERING TUSSEN DE WPOLR EN WPOLG

De doelstellingen van de Wpolr en de Wpolg komen voor een belangrijk deel goed met elkaar overeen, maar er zit een duidelijk verschil in de wijze waarop de Wpolr en Wpolg hun doelstellingen trachten te bereiken. Het gaat hier om precieze definitiebepalingen in beide regelingen die bepalen op welke handelingen het regime van de wet van toepassing is. Voor een groot deel zijn de verschillen ingegeven door het feit dat de Wpolr gebaseerd is op de Wet persoonregistraties en de Wpolg op de Wet bescherming persoonsgegevens.²¹⁸ Hieronder behandelen we alleen de begrippen die relevant zijn voor de reikwijdte van de beide regelingen. Het gaat achtereenvolgens om de definitie van (1) de politietaak, (2) het politieregister, en (3) de persoonsgegevens.

Politietaak

In subsectie 3.3.1 is een uitgebreide beschrijving gegeven van de politietaak zoals die in art. 1 onder b Wpolr is omschreven. Het betreft de uitvoering van de in art. 2 Pw1993 omschreven taak. Onder de Wpolg is de definitie van de politietaak uitgebreid. Blijkens art. 1 onder b Wpolg valt hieronder niet alleen de taak zoals in art. 2 Pw1993 is omschreven, maar ook de taak, “bedoeld in (...) art. 6, eerste lid, van de Politiewet 1993”. In dat artikel is de taakomschrijving van de Koninklijke Marechaussee opgenomen. Het gaat dan om veel zaken met een grote verscheidenheid. We noemen er zes: (1) het waken voor de veiligheid van de leden van het Koninklijk Huis, (2) de uitvoering van de politietaak ten behoeve van (2a) Nederlandse en (2b) andere strijdkrachten, en (2c) de luchthaven Schiphol, alsmede (3) de beveiliging van de burgerluchtvaart, (4) de verlening van bijstand alsmede de samenwerking met de politie, (5) de bestrijding van (5a) mensensmokkel en van (5b) fraude met reis- en identiteitsdocumenten, en (6) het ten behoeve van

218 De Wet persoonregistraties is de voorloper van de Wet bescherming persoonsgegevens, deze laatste is op 1 september 2001 in werking getreden.

De Nederlandsche Bank N.V. verrichten van beveiligingswerkzaamheden. Ten behoeve van die taken beschikt de Koninklijke Marechaussee ook over een CIE.

Politieregister

Hieronder behandelen we het politieregister ten aanzien van de Wpolr en ten aanzien van de Wpolg. De Wpolr ging uit van het registerbegrip. Het register was gedefinieerd als:

- “een samenhangende verzameling van op verschillende personen betrekking hebbende persoonsgegevens*
– *die langs geautomatiseerde weg wordt gevoerd of met het oog op een doeltreffende raadpleging van die gegevens systematisch is aangelegd, en*
– *die is aangelegd ten dienste van de uitvoering van de politietaak”*²¹⁹

De Wpolr stelde voorwaarden aan het oprichten van een register en bepaalde welke gegevens in die registers mochten worden opgeslagen. In de praktijk betekende dit dat de politietaak was opgedeeld in deeltaken en was voorzien van een eigen register. Zo maakt het register rijverboden het mogelijk de opgelegde rijverboden te handhaven. Ieder register moest voorts worden voorzien van een reglement²²⁰, waarin werd opgenomen (1) het doel van het register, (2) de categorie van personen over wie informatie in het register werd opgeslagen, en (3) het soort gegevens dat over die persoon werd verwerkt²²¹. Het aantal (soorten) politieregisters was vanuit juridisch oogpunt onbeperkt. Het aanleggen van een politieregister was onder de Wpolr toegestaan indien dit noodzakelijk was voor de goede uitvoering van de politietaak en het doel voldoende duidelijk was bepaald.²²² Een precies aantal verschillende soorten gevoerde politieregisters is dan ook niet te geven. Het Cbp heeft destijds voor 45 soorten registers een modelreglement afgekondigd, hetgeen betekent dat er in ieder geval 45 soorten registers bestaan in de praktijk.²²³

Het verwerken van persoonsgegevens onder de Wpolg

Zoals eerder is opgemerkt is onder de Wpolg het register als aangrijpingspunt losgelaten. Onder de Wpolg staat het *verwerken* van politiegegevens centraal. Voor de toepasselijkheid van de Wpolg is van belang of (1) een politiegegeven wordt verwerkt, (2) met welk doel het politiegegeven wordt verwerkt, en (3) of het politiegegeven in een bestand wordt opgenomen of bestemd is om daarin te worden opgenomen.²²⁴ We behandelen de drie onderdelen afzonderlijk.

219 Art. 1 onder c Wpolr.

220 Art. 1 onder g, jo. art. 9 Wpolr.

221 Art. 10 Wpolr.

222 Art. 4 lid 1 Wpolr.

223 Zie voor een overzicht <http://www.cbpweb.nl/indexen/ind_wetten_wpolr_model.stm>.

224 Art. 2 lid 1 Wpolg.

Ten eerste bezien we het begrip verwerken. De Wpolg definieert het verwerken van politiegegevens als “elke handeling of elk geheel van handelingen met betrekking tot politiegegevens”.²²⁵ Onder handelingen moeten onder meer de volgende activiteiten worden begrepen: opslaan, verwijderen, bewaren, verstrekken, koppelen, en analyseren. Ten tweede bezien we het doel van de verwerking. Evenals onder de Wpolr mogen gegevens alleen verwerkt worden wanneer dat gebeurt met een doel dat past binnen de politietaken. De verschillende verwerkingsdoelen staan in de Wpolg opgesomd.²²⁶ Ten derde bezien we de Wpolg ten aanzien van de opslag. De Wpolg is alleen van toepassing indien de gegevens worden opgeslagen in een bestand of bestemd zijn voor opslag in een bestand. Dit is iets anders dan de registerbenadering van de Wpolr. Het belangrijkste verschil is dat de doelbinding niet aan het register/bestand kleef, maar op elk individueel gegeven. Daarmee kunnen er in het register/de database gegevens zitten die voor verschillende doeleinden worden verwerkt. Voorts is de reglementplicht komen te vervallen. Deze vorm van reguleren maakt via de Wpolg het verwerken van gegevens door de politie flexibeler.

Persoonsgegevens

Zoals vaker gezegd was het register voor de Wpolr het aangrijpingspunt. Het centrale thema dat daar nauw mee verbonden was, was het begrip persoonsgegevens. Voor een definitie hiervan verwijst de Wpolr naar de Wbp. De Wbp definieert het begrip persoonsgegevens als:

“elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon”.

Het begrip persoonsgegevens is ingevoerd onder de voorganger van de Wbp, de Wet persoonsregistraties. Onder het begrip persoonsgegevens wordt ieder gegeven verstaan dat herleidbaar is tot een natuurlijk persoon. Twee elementen zijn hierbij van belang. Ten eerste moet het gegeven een identificerend element bevatten. Ten tweede moet het voor de gegevensverwerker een niet onevenredige inspanning opleveren om op basis van dat identificerende element het gegeven te herleiden tot een natuurlijk persoon. De registratiekamer (de voorloper van het CBP) heeft voor de beoordeling van de herleidbaarheid het volgende criterium aangelegd: “de identiteit van de persoon [moet] redelijkerwijs, zonder onevenredige inspanning, vastgesteld [kunnen] worden”.²²⁷ Daarbij kan onderscheid worden gemaakt tussen (1) het criterium van “de redelijk toegeruste houder” en (2) het subjectievere criterium van de omstandigheden. Bij het eerste criterium geldt dat van een normaal burger bijvoorbeeld mag worden verwacht dat hij in staat is een telefoonnummer te vinden via de daarvoor op internet beschikbare websites, waar op nummer kan worden gezocht. Voor het tweede, meer subjectieve

²²⁵ Art. 1, aanhef onder c Wpolg.

²²⁶ Art. 8 t/m 10 Wpolg.

²²⁷ Uitspraak Cbp, z2000-0340, p. 4.

criterium dient rekening te worden gehouden met de omstandigheden waarin de houder van de gegevens zich bevindt. Het gaat daarbij vooral om het expertiseniveau van de houder en de bij hem ter beschikking staande instrumenten.²²⁸ Zo is voor een normaal burger een voor hem onbekend nummerbord geen persoonsgegevens, omdat het voor hem niet herleidbaar is tot een individueel persoon zonder onevenredige inspanning. Dit ligt echter anders voor bijvoorbeeld een verkeersschadebehandelaar bij een verzekeringsmaatschappij. Deze heeft in de regel rechtstreekse toegang tot de registers van de RDW en kan een voor hem onbekend nummerbord wel op eenvoudige wijze herleiden tot een individueel persoon. Holvast (1996) merkte destijds in dit verband op dat deze criteria verwarring in de hand werken doordat het begrip persoonsgegevens een dynamisch begrip is geworden. Als gevolg hiervan verschilt het per houder en in tijd of een gegeven moet worden aangemerkt als persoonsgegevens.²²⁹

De Wpolg reguleert en normeert de verwerking van politiegegevens in plaats van persoonsgegevens. Politiegegevens worden gedefinieerd als:

“elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon dat in het kader van de uitoefening van de politietaak wordt verwerkt”²³⁰

Blijkens de memorie van toelichting heeft de wetgever met deze definitie aan willen sluiten bij de definitie van persoonsgegevens van de Wbp.²³¹ Met het vervangen van de term persoonsgegevens door politiegegevens heeft de wetgever slechts tot uitdrukking gebracht dat de Wpolg alleen op verwerkingen van persoonsgegevens in het kader van de politietaak reguleert en normeert. Feitelijk brengt dit geen verschil in reikwijdte van de wet met zich mee.

4.4 DRIESTAPPENBEHANDELING

Voor alle vijf onderwerpen (opslaan, bewaren, verstrekken, koppelen, en analyseren) volgen we een driestappenbehandeling. We behandelen (in stap 1) het theoretisch kader van deze activiteiten, zoals dat gold onder de Wpolr, (in stap 2) de knelpunten die daarbij in de praktijk zijn geconstateerd en (in stap 3) de mogelijke oplossingen die de Wpolg daarvoor aandraagt. Een en ander plaatsen we vervolgens in het licht van de ervaringen met de Wbp. Daardoor kunnen we de analyse in dit hoofdstuk beschouwen als een soort case-studie betreffende een aantal van de genoemde voor- en nadelen van een sectorale benadering (zie sectie 4.2). De geconstateerde knelpunten ten aanzien van de sectorale regeling worden nu geplaatst in het licht van de ervaringen met de Wbp.

228 Uitspraak Cbp, z2000-0340, p. 5.

229 Holvast, 1996.

230 Art. 1 onder a Wpolg.

231 *Kamerstukken II*, 2005/06, 30 327, nr. 3, p. 24-25.

In de secties 4.5 tot en met 4.9 worden de knelpunten in het huidige wettelijke regime besproken. Het gaat om opslaan (4.5), bewaren (4.6), verstrekken (4.7), koppelen (4.8), en analyseren (4.9). We voeren een *driestappenbehandeling* uit om een weloverwogen oordeel te kunnen vormen over de vraag of de Wpolg zijn waarborgende taak beter vervult dan de Wpolr. Daarmee wordt een antwoord gegeven op de tweede en derde onderzoeksvraag voor zover het het gebruik van politiegegevens betreft. Hieronder geven we in 4.4.1 kort de ontwikkeling van het politieke gegevensverwerkingsrecht (schematisch) weer, daarna volgt in 4.4.2 een beschrijving van de *driestappenbehandeling*.

4.4.1 De ontwikkeling van het politieke gegevensbeschermingsrecht

De Wpolr en Wpolg zijn in beginsel op zichzelf staande regelingen. De structuur en wijze van regulering zijn echter gestoeld op hun privaatrechtelijke tegenhangers. Dit zijn respectievelijk de Wet persoonsregistraties en de Wet bescherming persoonsgegevens. De data van het inwerking treden van de verschillende regelingen is in figuur 4.1 schematisch weergegeven. Zoals in hoofdstuk 3 is beschreven is de totstandkoming van de Wpr het gevolg van de discussie die in de jaren zeventig is gevoerd naar aanleiding van de ontstane maatschappelijke onrust.²³² De Wpr is in 1988 in werking getreden. Onder de Wpr viel het gebruik van persoonsgegevens door de politie buiten het bereik van de wet. Een speciale wet voor dat deelgebied werd noodzakelijk geacht. Het heeft tot 1990 geduurd voordat de Wpolr werd ingevoerd en dus ook politieke gegevensverwerking door een formele wet werd gereguleerd en genormeerd. De systematiek van de Wpolr werd logischerwijs afgeleid van de Wpr. Zo was in beide regelingen het registerbegrip uitgangspunt.²³³ Naar aanleiding van de bevindingen van de commissie-Van Traa is in 1999 de Wet bijzondere politieregisters ingevoerd, waarbij wettelijke regelingen zijn opgenomen in de Wpolr ten aanzien van de registers die door de CIE worden gevoerd. Dit is uitgebreid in hoofdstuk 2 besproken. In 2000 is de Wpr vervangen door de Wbp. Met die wijziging is de Europese richtlijn 95/46/EG geïmplementeerd. Door de invoering van de Wbp is ook de systematiek van het particuliere gegevensbeschermingsrecht gewijzigd. In 2008 is de Wpolr gewijzigd in de Wpolg en is aansluiting gezocht bij de systematiek van de Wbp. Tussen 2000 en 2008 bestond er dus een verschil in systematiek van het gegevensbeschermingsrecht tussen de 'particuliere' sector en de politieke sector. De gevolgen van deze gewijzigde systematiek voor de Wpolr en de Wpolg zijn in sectie 4.2 besproken. De verschillende data, en derhalve de diverse overgangen van het ene regime naar het andere regime, zijn weer gegeven in figuur 4.1.

232 Zie uitgebreid subsectie 3.2.1.

233 Zie artt. 1 onder c en art. 4 lid 1 Wpolr respectievelijk artt. 1 en 4 lid 1 Wpr.

Omnibuswetgeving	Wpr (1988)	Wpr	Wpr	Wpb (2000)	Wpb
Wetgeving op politiek gebied		Wpolr (1990)	Wpolr Wpolr (1999)	Wpolr Wpolr (1999)	Wpolr (2008)

Figuur 4.1: Schematische weergave inwerkingtreding van Nederlandse privacywetgeving.

Het spreekt voor zichzelf dat de datum waarop een regeling in werking treedt formeel als moment wordt aangemerkt waarop de daarin opgenomen veranderingen van kracht worden. In de praktijk is deze scheidslijn echter niet zo strak te trekken. Op het moment dat een nieuwe regeling wordt ontworpen heeft dit informeel al zijn invloed op de praktijk. De nieuwe regeling is immers gebaseerd op een op dat moment bestaand evenwicht in de in hoofdstuk 3 beschreven belangen. De ontwikkeling van die normen en waarden is een continu proces. Het is dan ook vanzelfsprekend dat een aantal bestaande regelingen wordt uitgelegd in overeenstemming met de op dat moment geldende normen en waarden. Bij de bepaling van de ‘stand’ van de normen en waarden van dat moment wordt in de rechtsgeleerdheid veelal gebruik gemaakt van “soortgelijke” regelingen. Het gaat dan om regelingen die soortgelijke belangen vertegenwoordigen, maar voor een ander deelgebied. Als het gaat om politieke gegevensverwerking hebben de wijzigingen die zijn doorgevoerd met de vervanging van de Wpr door de Wbp onmiskenbaar hun invloed gehad op de manier waarop begrippen uit de Wpolr worden uitgelegd. Daarmee werd feitelijk dus vooruitgelopen op de invoering van de Wpolg. Bij onze analyse van (1) de Wpolr, (2) de daarbij geconstateerde knelpunten, en (3) de oplossingen die de Wpolg daarvoor biedt, laten we deze informele beïnvloeding buiten beschouwing.

4.4.2 De inhoud van de stappen

De *driestappenbehandeling* bestaat uit drie onderdelen (drie stappen). Ten eerste wordt het theoretisch kader besproken aan de hand van de verschillende soorten verwerkingselementen (opslaan, bewaren, verstrekken, koppelen en analyseren van gegevens). Ten tweede worden aan de hand van dezelfde verwerkingselementen de juridische knelpunten onder de Wpolr in de gegevensverwerking door de CIE-en beschreven. Ten derde wordt besproken op welke wijze de Wpolg tegemoet komt aan de geconstateerde knelpunten. Het laatste onderdeel wordt tevens gezien in het licht van de ervaringen die zijn opgedaan bij de uitvoering van de Wet bescherming persoonsgegevens. De driestappenbehandeling komt derhalve telkens terug in de onderstaande vijf secties.

Omdat de wijze van regulering en opbouw van de Wpolr en de Wpolg van elkaar verschillen²³⁴ kunnen we de twee regelingen niet één op één vergelijken. We hebben er daarom voor gekozen om bij de driestappenbehandeling

234 Dit is uitgewerkt in subsectie 4.1.2.

ling uit te gaan van het informatieverwerkingsproces bij de CIE (opslaan, bewaren, verstrekken, koppelen, en analyseren van gegevens).²³⁵ In sectie 4.5 wordt de driestappenbehandeling uitgevoerd op het opslaan van gegevens door de CIE. In secties 4.6 tot en met 4.9 ondergaan de verwerkingselementen bewaren (sectie 4.6), verstrekken (sectie 4.7), koppelen (sectie 4.8), en analyseren (sectie 4.9) dezelfde driestappenbehandeling.

4.5 OPSLAAN

De Wpolr en Wpolg gaan over de wijze waarop de politie met gegevens om mag gaan. Onder de Wpolg duiden we dit met gegevensverwerking aan. Het proces start met het opslaan van informatie. Het verzamelen van informatie valt volgens de wetgever in beginsel niet onder het bereik van de Wpolr en Wpolg, maar onder de werking van het Wetboek van Strafvordering. Wij hebben ons standpunt hierover uitgebreid gegeven in hoofdstuk 3. We voeren hieronder de driestappenbehandeling²³⁶ uit op de activiteit 'opslaan'. In subsectie 4.5.1 bespreken we de theorie van het opslaan zoals deze gold onder de Wpolr. In subsectie 4.5.2 bespreken we de daarbij in de praktijk onder de Wpolr geconstateerde knelpunten. Voorts behandelen we in subsectie 4.5.3 op welke wijze de Wpolg aan deze knelpunten tegemoet is gekomen. In subsectie 4.5.4 geven we een tussenconclusie.

4.5.1 Theoretisch kader

Elk van de 33 CIE-en maakte bij de verwerking van CIE-informatie gebruik van dezelfde registers. Het systeem van de Wpolr schreef dwingend voor welke drie registers de CIE mocht voeren ter ondersteuning van haar taakuitvoering. Met andere woorden: de CIE mocht persoonsgegevens slechts opslaan indien de Wpolr daar een grondslag voor bood. De drie registers waren: (1) het register zware criminaliteit, ook wel het zwacri-register genoemd, (2) het voorlopig register, en (3) het informantenregister. Van die registers mocht de CIE alleen gebruik maken volgens de regels die daartoe in de Wpolr waren neergelegd. Hieronder behandelen we de drie registers.

Het register zware criminaliteit

In het register zware criminaliteit werd de informatie van de informant die nuttig kon zijn voor andere CIE-en en voor rechercheonderzoeken opgeslagen, inclusief een afhandelingscode. Deze codes werden aan een informatie-item 'gehangen' en maakten duidelijk of die informatie al dan niet operatio-

235 Koelewijn, 2009, 148-152.

236 Zoals beschreven in sectie 4.4.

neel gebruikt kon worden. Aan de hand van die codes kon bepaald worden welke informatie wel (elektronisch) vrij uitwisselbaar was en welke niet.

In het zwacri-register mocht volgens de Wpolr slechts over een beperkt aantal delicten informatie worden opgeslagen. De Wpolr definieerde het zwacri-register als volgt.

“register zware criminaliteit: een politieregister dat is aangelegd met het oog op de uitvoering van de politietaak, voor zover het betreft:

1°.

misdrijven als omschreven in art. 67, eerste lid, van het Wetboek van Strafvordering, die in georganiseerd verband worden beraamd of gepleegd en gezien hun aard of de samenhang met andere misdrijven die in het georganiseerd verband worden beraamd of gepleegd, een ernstige inbreuk op de rechtsorde opleveren of

2°.

misdrijven waarop naar de wettelijke omschrijving een gevangenisstraf van acht jaar of meer is gesteld;

3°.

bij algemene maatregel van bestuur te omschrijven misdrijven als omschreven in art. 67, eerste lid, van het Wetboek van Strafvordering, die gezien hun aard of de samenhang met andere door betrokkene begane misdrijven een ernstige inbreuk op de rechtsorde opleveren;”²³⁷

Art. 13a lid 1 Wpolr definieerde vervolgens over welke personen informatie mocht worden geregistreerd. Het ging om onder meer:

a. verdachten van misdrijven, waarvoor het register is aangelegd;

b. personen, ten aanzien van wie een redelijk vermoeden bestaat dat zij betrokken zijn bij het beraamen of plegen van misdrijven als bedoeld onder a;

c. personen die in een bepaalde relatie staan tot degenen, bedoeld onder a en b.”

In art. 6 van het modelreglement register zware criminaliteit (Mreg Zwacri) was opgenomen wat voor typen gegevens over deze personen mochten worden geregistreerd. Het ging onder andere om gegevens over karaktereigenschappen, uiterlijk, persoonlijke omstandigheden, levenswijzen en vervoermiddelen. Hoewel ongebreidelde registratie van gegevens niet was toegestaan was de reikwijdte van art. 6 Mreg Zwacri dusdanig ruim dat een compleet beeld van een persoon kon worden verkregen. Bij opname van gegevens diende geregistreerd te worden onder welke categorie van art. 13a lid 1 de registratie viel. Het type registratie bepaalde namelijk welke regels op het gebruik van die registratie van toepassing waren. Zo gold voor de personen die in een bepaalde relatie stonden tot een verdachte van zware criminaliteit (art. 13a lid 1 onder c Wpolr) een strenger verstrekkingssysteem dan voor de verdachte zelf (art. 13a lid 1 onder a Wpolr).

Naast de drie categorieën van personen uit art. 13a lid 1 Wpolr kende de Wpolr ook een algemene regeling omtrent onverdachte personen in art. 5a Wpolr. Met deze bepaling was getracht het verschil tussen de bijzondere

237 Art. 1 lid 1 onder l Wpolr.

politierregisters en de gewone politierregisters te benadrukken.²³⁸ Noch de Wpolr, noch het Bpolr of de modelreglementen gaven een definitie van het begrip ‘onverdachte personen’. Het begrip moest in ieder geval niet worden aangemerkt als tegenhanger van het verdachtebegrip zoals we dat kennen uit art. 27 Sv.²³⁹ Het Cbp stelde dat het moet gaan om verdachtmakingen en geruchten die niet kunnen worden gestaafd met gebruikmaking van andere bronnen.²⁴⁰ De onderzoekers van het evaluatieonderzoek kwamen op basis van onder meer deze bronnen tot drie voorwaarden waaraan voldaan moet zijn wil er sprake zijn van een ‘onverdachte persoon’.²⁴¹ Omdat de regeling omtrent onverdachte personen in de algemene bepalingen was opgenomen gold deze ook voor het voorlopig register en het informantenregister.

Het voorlopig register

De CIE had onder de Wpolr het voorlopig register tot zijn beschikking. Informatie waarvan de juistheid niet in voldoende mate (voor opname in het zwacri-register) kon worden vastgesteld diende in dit register te worden opgeslagen. Het voorlopig register was daarmee het voorportaal voor het register zware criminaliteit. Informatie uit het voorlopig register werd door de CIE zo mogelijk opgewaardeerd. Dit betekende dat de CIE vaststelde of de geregistreerde in samenhang met andere gegevens kon worden opgenomen in het zwacri-register van die regio.²⁴² Vanzelfsprekend mocht in het voorlopig register alleen informatie worden opgenomen over personen ten aanzien van wie reden bestond dat zij in het zwacri-register zouden kunnen worden opgenomen.²⁴³ In art. 6 van het modelreglement voorlopig register was vastgelegd welke gegevens van de geregistreerde mochten worden opgenomen. Een ongebreidelde vastlegging van gegevens was dus niet toegestaan.

Het informantenregister

In het informantenregister werden onder meer de personalia van de informant opgenomen en het ICS-nummer²⁴⁴ waaronder hij in de overige registers stond geregistreerd, om zijn anonimiteit te waarborgen. Daarnaast werd in het informantenregister ook een bruto-verslag opgeslagen van de gesprekken die met de informant waren gevoerd. Het bruto-verslag is een zo letterlijk mogelijk weergegeven verslag van de gesprekken die een runner heeft

²³⁸ Muijen, 2004, p.58.

²³⁹ Circulaire bijzondere politierregisters, Stcrt. 1999,221.

²⁴⁰ Registratiekamer benadrukt naleving wettelijk verplichte schoning politiegegevens, 29 maart 2001, z2000-1166.

²⁴¹ Schreuders e.a, 2005, p. 72.

²⁴² Art. 1 lid 1 onder k Wpolr.

²⁴³ Art. 5 onder a modelreglement Voorlopig register.

²⁴⁴ Art. 1 onder g modelreglement informantenregister. De ICS-code is een code samengesteld aan de hand van de personalia van de informant, door een landelijk vastgesteld coderingsprogramma.

gehad met de informant. Een goed voorbeeld hiervan zijn de in boekvorm uitgegeven 'Endstra-tapes'.²⁴⁵ Naast een letterlijke weergave van het gesprek werd zoveel mogelijk informatie opgenomen over de omstandigheden waarin de informatie is gegeven en de persoonlijke omstandigheden van de informant die van belang kunnen zijn voor de bepalingen van de juistheid en betrouwbaarheid van de verschaft informatie. Op die manier fungeerde het informantenregister als het geheugen van de CIE en was daarmee onmisbaar in de communicatie met de verschillende informanten. Het informantenregister was een instrument om het informantenbestand te kunnen beheeren. Het was een belangrijk middel bij de beoordeling van de door de informant gegeven informatie op onder meer betrouwbaarheid. Het moge duidelijk zijn dat (1) de gegevens in het informantenregister uitermate gevoelig waren (met name de informatie die herleidbaar is tot de informant) en (2) het register om die reden vergaand werd afgeschermd. Het was dan ook voor slechts enkele CIE-rechercheurs toegankelijk. Vanuit het informantenregister werden tekstgedeelten uit het bruto-verslag gehaald en, indien ze voldeden aan de daaraan gestelde eisen, opgenomen in het register zware-criminaliteit. Dit wordt in de praktijk aangeduid met 'netto informatie'.

In de Wpolr was geen bepaling opgenomen over het informantenregister. Omdat het gebruik van het informantenregister voor de dagelijkse taakuitvoering van de CIE onmisbaar is heeft het Cbp ingestemd met het bestaan ervan en heeft een modelreglement voor het register afgekondigd. Het modelreglement definieerde een informant als een persoon die een politieagent informatie verstrekt over door anderen gepleegde of nog te plegen strafbare feiten. Een voorwaarde bij de definitie was dat de verstrekking van deze informatie gevaar oplevert voor de informant of voor derden.²⁴⁶ Het informantenregister had tot doel de informatievoorziening rond informantengegevens te beheeren in het kader van de uitvoering van de politietaak zoals die in art. 2 Pw1993 is neergelegd.²⁴⁷ Het informantenregister kende voorts drie typen informanten; (1) voorlopig geregistreerde informanten, (2) geregistreerde informanten, en (3) uitgeschreven informanten.²⁴⁸ Een ambtenaar van de CIE kon een informant registreren als 'voorlopig informant' in het informantenregister. Pas nadat toestemming daartoe van de CIE-officier van justitie was verkregen, mocht deze informant worden "bevorderd" naar een 'geregistreerd informant'. Voor informanten die de geregistreerde status verloren, kende het modelreglement de term 'uitgeschreven informant'. Zo'n uitgeschreven informant mocht niet meer actief gerund²⁴⁹ worden. Er werd in het informantenregister informatie opgenomen over de informanten zelf en over de personen over wie zij informatie verschaft hadden.²⁵⁰

245 Middelburg en Vugts, 2006.

246 Art. 1 onder e modelreglement informantenregister.

247 Art. 2 modelreglement informantenregister.

248 Art. 5 modelreglement informantenregister.

249 Zie voor uitleg over het begrip runnen hoofdstuk 2.

250 Art. 6 modelreglement informantenregister.

Art. 7 van het modelreglement informantenregister bepaalde wat voor soort gegevens mochten worden geregistreerd over informanten en de personen over wie de informanten gegevens verschaft hadden. Het ging dan onder meer om de personalia van deze personen, en de genoemde ICS-code.²⁵¹ De belangrijkste soort gegevens die geregistreerd mochten worden was het verslag van het gesprek, afhankelijk van de wijze van registreren van het gesprek zowel in papieren vorm als een geluidsopname daarvan.²⁵² De registratie van het verslag in het informantenregister wordt aangeduid met de term ‘bruto-verslag’.

4.5.2 De knelpunten beschreven

In deze subsectie behandelen we de praktijkervaringen die de CIE heeft met het opslaan van informatie in het kader van haar taakuitvoering. Daarbij spelen de hierboven genoemde drie registers een centrale rol. De gegevens die voor het in deze sectie beschreven onderzoek zijn gebruikt, zijn afkomstig uit de evaluatie van de Wet bijzondere politieregisters die in 2005 in opdracht van het Wetenschappelijk Onderzoek en Documentatie Centrum (WODC) is uitgevoerd. Deze empirische onderzoeksgegevens worden daarnaast aangevuld met resultaten uit het onderzoek dat door Kielman en Koelewijn in 2005 en 2006 is uitgevoerd.²⁵³

Onder de Wpolr zijn bij het opslaan van politiegegevens drie knelpunten te onderscheiden. Het gaat dan om (1) het ontbreken van een wettelijke regeling voor het informantenregister, (2) een afbakeningsknelpunt, en (3) een classificatieknelpunt. We behandelen deze drie knelpunten hieronder.

Ad (1) Knelpunt informantenregister

Wat de knelpunten betreft die zich voordeden bij het informantenregister kunnen we kort zijn. In de Wpolr bestond geen regeling voor het informantenregister, zodat alleen het ontbreken van een regeling als knelpunt aangemerkt kan worden. We zullen dit evenwel niet verder als knelpunt behandelen, maar wel als knelpunt in figuur 4.2 opnemen. Voorts bestond er het modelreglement dat bij gebrek aan een wettelijke regeling reguleerde wat in het informantenregister mocht worden opgeslagen. Wat de opslag betreft heeft de toepassing hiervan in de praktijk voor zover wij hebben kunnen nagaan niet tot knelpunten geleid. Hieronder vermelden we kort welke informatie tot verdere verwerking leidt en hoe dat gebeurt.

Het eerste selectie criterium voor de opslag van (ontvangen) informatie in het zwacri-register werd gevormd door de misdaden die als ‘zwacri-waardig’ werden aangemerkt, zoals in subsectie 4.2.1 is beschreven. Dit werd in de

251 Art. 7 modelreglement informantenregister.

252 Art. 7 lid 1 onder c modelreglement informantenregister.

253 Zie hoofdstuk 1 voor een beschrijving van de methodologie van dit onderzoek.

praktijk als zeer praktisch ervaren. Het invoeren van informatie in het zwacri-register werd veelal door de administratieve ondersteuning van de CIE gedaan. Zij maakten daarbij gebruik van lijsten waarop de 'zwacri-waardige' delicten waren opgesomd. Indien een informatie-item paste binnen een op de lijst genoemd delict, dan werd het opgenomen in het zwacri-register.²⁵⁴ Elke CIE die in het kader van ons eigen empirisch onderzoek was bezocht bleek, indien mogelijk, een informatie-item ergens anders binnen de politieorganisatie uit te zetten wanneer dat informatie-item niet voor opneming in het zwacri-register in aanmerking kwam.

Ad (2) Afbakeningsknelpunt

Het tweede knelpunt bij de opname van gegevens in het zwacri-register was de afbakening tussen het voorlopig register en het zwacri-register. Er bleken problemen te zijn met de vraag of gegevens in het voorlopig register moesten worden opgeslagen of dat ze voldeden aan het criterium voor opname in het register zware criminaliteit. Er was sprake van een afbakeningsknelpunt tussen de opslag van een informatie-item in het zwacri-register en de opslag van een informatie-item in het voorlopig register. Bij opslag in het zwacri-register diende uit de informatie te blijken dat er een redelijk vermoeden²⁵⁵ bestond dat een persoon zich met zwacri-waardige misdrijven bezig hield, hetgeen registratie in het zwacri-register zou rechtvaardigen. Was dit niet het geval, dan diende de betreffende informatie in het voorlopig register geregistreerd te worden. In de toelichtingen op de modelreglementen van het zwacri-register en het voorlopig register bestond onduidelijkheid of alle subjecten eerst in het voorlopig register dienden te worden opgenomen of dat ze ook direct geregistreerd mochten worden in het register zware criminaliteit.²⁵⁶ De grens tussen het voorlopig register en het register zware criminaliteit was, met andere woorden, vaag. Onduidelijk was wanneer informatie over een bepaald subject dusdanig hard was dat het de status van voorlopig voorbij was en mocht worden opgenomen in het zwacri-register. Om deze redenen merken wij dit probleem aan als een afbakeningsknelpunt.

Het WODC-evaluatieonderzoek onderscheidt in het afbakeningsknelpunt drie specifieke punten waar men in de praktijk veelvuldig tegen aan liep.²⁵⁷ Ten eerste, de vraag of en zo ja in welke mate (1) de betrouwbaarheid van de gegeven informatie en (2) de reden van wetenschap de 'hardheid' van de informatie mochten beïnvloeden. Ten tweede, de vraag of aanvullende informatie over een reeds bekend subject uit het zwacri-register direct in het zwacri-register mocht worden opgenomen of dat de nieuwe informatie zelfstandig de toets moest doorstaan. Ten derde, de vraag of informatie

254 Schreuders e.a., 2005, p. 68.

255 Art. 13a lid 1 onder b Wpolr.

256 Schreuders e.a., 2005, p. 68.

257 Schreuders e.a., 2005, p. 69.

over een zwacri-subject dat een ander misdrijf betrof dan waarvoor hij in het zwacri-register geregistreerd stond direct in het zwacri-register mocht worden geplaatst of ook zelfstandig de toets moest doorstaan.

Dat het afbakeningsknelpunt een belangrijk knelpunt betrof blijkt uit (1) het WODC-evaluatieonderzoek en (2) het onderzoek van Kielman en Koelewijn. Uit beide onderzoeken is gebleken dat vanwege het afbakeningsknelpunt in de praktijk slechts mondjesmaat gebruik werd gemaakt van het voorlopig register. De subjecten die in het voorlopig register werden geregistreerd werden feitelijk als zwacri-subject geregistreerd in het zwacri-register en voorzien van een digitaal label 'vl' zodat duidelijk was dat het om een voorlopige registratie ging. Ook in de memorie van toelichting op de Wpolg wordt het beperkte gebruik van het voorlopig register genoemd.²⁵⁸ De meeste door Kielman en Koelewijn gesproken CIE-en hanteerden als uitgangspunt dat informatie uit één bron in het voorlopig register werd opgenomen. Zodra deze informatie uit een andere bron werd bevestigd, mocht de informatie worden opgewaardeerd naar het zwacri-register.²⁵⁹

Ad (3) Classificatieknelpunt

Het derde knelpunt betrof een classificatieknelpunt. Indien een informatie-item geschikt bleek voor registratie in het zwacri-register dan vond registratie plaats. Uit het onderzoek van Kielman en Koelewijn blijkt dat bij registraties er door de verschillende soorten subjecten verwarring kon ontstaan. De Wpolr maakt onderscheid tussen drie subjecten, te weten: (1) verdachten, (2) betrokkenen, en (3) contacten. Dit onderscheid is in subsectie 4.5.1 besproken. Elk van deze geregistreerde subjecten werd weliswaar opgenomen in het register zware criminaliteit, maar voor elke categorie gold een apart verwerkingsregime.²⁶⁰ Bij de registratie van deze gegevens diende dan ook vermeld te worden om wat voor soort registratie het ging. Zes van de zeven CIE-en gaven in het onderzoek van Kielman en Koelewijn te kennen dat het onderscheid tussen betrokkenen en contacten lastig te maken was. In de verschillende officiële regelingen en beleidsstukken waren geen heldere en duidelijke richtlijnen gegeven die hielpen bij het invullen van deze criteria. Voorts werd de opname van informatie-items in het zwacri-register onder de classificatie 'verdachte' bemoeilijkt doordat er geen definitie van dit begrip was gegeven. Bij de definitie van het begrip 'verdachte' kon niet worden uitgegaan van het in het strafrecht bekende verdachte-begrip. Aangezien het werk van de CIE zich tegenwoordig vooral in de pro-actieve fase afspeelt is er in dit geval geen sprake van een verdenking in de zin van art. 27 Sv. Naast het feit dat de toepassing van de verschillende begrippen (zoals 'verdachte') te maken heeft met een afbakeningsprobleem, wordt door de verschillende CIE-en in het onderzoek van Kielman en Koelewijn aangege-

258 *Kamerstukken II*, 2005/06, 30 327, nr. 3, p. 48.

259 Zie voor een beschrijving van de methodologie van dit onderzoek hoofdstuk 1.

260 Zie bijvoorbeeld de verschillende bewaartermijnen (subsectie 4.6.1).

ven dat op het moment dat vroeger een persoon geregistreerd werd het vaak nog niet duidelijk was of het om een betrokkene ging of om een contact.

Een variant van dit knelpunt is binnen het WODC-evaluatieonderzoek geconstateerd als het ging om 'onverdachte personen'. De Wpolr bevatte in art. 5a een algemene regeling voor de opname van gegevens omtrent onverdachte personen. Deze regeling gold in beginsel ook voor de opname van gegevens door de CIE. Uit zowel het WODC-evaluatieonderzoek als het empirisch onderzoek van Kielman en Koelewijn blijkt dat het begrip 'onverdachte personen' in de CIE-praktijk nauwelijks werd gebruikt. Daarnaast werd aangegeven dat het begrip te open en te vaag was om in de praktijk mee om te gaan. Zoals eerder beschreven is, wordt in geen van de regelingen een uitwerking van het begrip 'onverdachte personen' gegeven.

Als we het bovenstaande samenvatten, dan zien we dat het classificatieknelpunt zich voordeed bij vier van de behandelde begrippen, te weten 'verdachte', 'betrokkenen', 'contact', en 'onverdachte personen'. Bij de registratie van een informatie-item diende dit item onder een of meerdere van deze begrippen te worden geplaatst. Aangezien van ieder van de vier verschillende klassen een heldere definitie ontbrak leidde het classificeren van de te registreren informatie-items in de praktijk tot problemen.

4.5.3 Uitwerking onder de Wpolg

Onder de Wpolg wordt geen gebruik meer gemaakt van het registerbegrip. Dat brengt met zich mee – in tegenstelling tot bij de Wpolr – dat de nadruk minder ligt op de opname van gegevens en meer op het 'verwerken' van politiegegevens. Theoretisch zouden daarmee de registers kunnen worden afgeschaft en een grote bak worden gemaakt waarin alle gegevens zijn opgenomen die zijn voorzien van een label waarin het verwerkingsdoel is opgenomen. Vanzelfsprekend kan het verwerkingsdoel van een gegeven in de tijd veranderen, waardoor er ook een ander verwerkingsregime van toepassing wordt. Daarmee wordt beoogd de gegevensverwerking flexibeler te laten verlopen. Het is echter sterk de vraag of dit bij de CIE-en veel verschil in werkwijze zal opleveren. Vanwege de in hoofdstuk 2 behandelde afbreukrisico's zullen de informantgegevens in een afgesloten database worden ingevoerd, waarop een stringent toegangsregime van toepassing zal (moeten) zijn. De verruiming van de toegang tot de informantgegevens behandelen we in sectie 4.7. Het huidige register zware criminaliteit bestaat feitelijk uit informatie-items die ontleend zijn aan het informantenregister (voor een uitgebreide beschrijving zie subsectie 4.5.1) en zal om die reden ook vergaand worden afgeschermd.

Oude knelpunten aangepakt

De in de vorige subsectie geconstateerde knelpunten zullen hieronder worden behandeld vanuit het gezichtspunt van de Wpolg. Daarmee wordt duidelijk in hoeverre de wetgever met de introductie van de Wpolg de onder de

Wpolr geconstateerde knelpunten heeft opgelost. We behandelen achtereenvolgens (1) het knelpunt informantenregister, (2) het afbakeningsknelpunt en (3) het classificatieknelpunt. Daarnaast behandelen we (4) de met de invoering van de Wpolg geïntroduceerde zogenaamde themaverwerkingen.

Ad (1) Knelpunt informantenregister

Wat de regeling rond het informantenregister betreft, is het opnemen van de informantenregeling in de Wpolg een significante verbetering is ten opzichte van de Wpolr, waarin het informantenregister niet bestond. Gezien het doel van deze vorm van gegevenswerking (zie hoofdstuk 2) is een zo volledig mogelijke verslaglegging van de informant en de informatie die hij heeft gegeven wenselijk. Ook het feit dat de informant zelf toestemming geeft voor de opname van zijn gegevens, maakt dat aan de opname weinige beperkingen worden gesteld.

Voor registratie van gegevens in het register zware-criminaliteit zijn de voorwaarden grotendeels hetzelfde gebleven. Er wordt vastgehouden aan de lijst van misdrijven waarvoor gegevens mogen worden verwerkt door de CIE. Die lijstsystematiek blijkt in de praktijk, zoals hierboven beschreven, ook goed te werken.

Ad (2) Afbakeningsknelpunt

Met betrekking tot het afbakeningsknelpunt biedt de Wpolg een duidelijke oplossing. Het voorlopig register, dat onder de Wpolg als het voorlopig verwerken van zwacri-gegevens zou kunnen worden aangemerkt, verdwijnt. In de memorie van toelichting worden de hierboven beschreven problemen (die tezamen het afbakeningsknelpunt vormen) als reden voor afschaffing van het voorlopig register aangevoerd.²⁶¹ De minister stelde dat de afscheiding tussen het voorlopig register en het register zware criminaliteit te vaag en onbepaald was en dat het voorlopig register in de praktijk bijna niet gebruikt werd. Dit is als reden aangevoerd om het voorlopig register af te schaffen. Opvallend genoeg wordt in de memorie van toelichting niet ingegaan op de argumenten van de commissie-Van Traa die er in 1996 toe hebben geleid dat het voorlopig register werd ingevoerd. De toenmalige praktijk, waarbij het voorlopig register ook niet bestond, kon volgens de commissie-Van Traa niet door de beugel. In onze tussenconclusie komen wij terug op deze problematiek.

Ad (3) Classificatieknelpunt

De Wpolg heeft het classificatieknelpunt, als het gaat om het probleem rond het begrip 'onverdachte personen', op een zelfde manier opgelost als het afbakeningsknelpunt. De algemene regeling rond de 'onverdachte personen' is geschrapt. Reden hiervoor is de onwerkbaarheid van art. 5a Wpolr in de

²⁶¹ Kamerstukken II, 2005/06, 30 327, nr. 3, p. 18.

praktijk.²⁶² Het Cbp heeft hier stevige kritiek op gegeven.²⁶³ Naar onze mening had de oude regeling 'onverdachte personen' weinig van doen met de gegevensverwerkingspraktijk bij de CIE-en. Hoewel het begrip 'onverdachte personen' in de evaluatie Wet bijzondere politieregisters is behandeld, betwijfelen wij of het begrip veel belang heeft bij het werken met de politieregisters. Het werk van de CIE brengt, zoals beschreven in hoofdstuk 2, voor een belangrijk deel met zich mee dat gegevens worden geregistreerd over personen die nog niet kunnen worden aangemerkt als verdachte in de zin van art. 27 Sv. Juist om de extra gevoeligheid die dat met zich meebrengt is de Wet bijzondere politieregisters ingevoerd. Een dergelijke redenering wordt ook door de meeste CIE-en zelf gevoerd.²⁶⁴

Ten aanzien van de overige drie beschreven probleembegrippen (verdachten, betrokkenen en contacten) bij het classificatieknelpunt kunnen we kort zijn. In de Wpolg worden deze classificatiecriteria ongewijzigd gehandhaafd. De begrippen zijn in de Wpolg of het daaraan verbonden besluit ook niet nader gespecificeerd. Wat deze begrippen betreft, biedt de Wpolg geen oplossing voor de in de praktijk geconstateerde knelpunten.

Ad (4) Nieuw knelpunt geïntroduceerd

De enig andere belangrijke wijziging die verder is doorgevoerd ligt in de structuur. Het gaat om de komst van zogenaamde themaverwerkingen.²⁶⁵ De Wpolg omschrijft het doel van deze verwerking als het verwerken van gegevens om inzicht te krijgen in de betrokkenheid van personen bij:

"handelingen die kunnen wijzen op het beramen of plegen van bij algemene maatregel van bestuur aan te wijzen categorieën van misdrijven die door hun omvang of ernst of hun samenhang met andere misdrijven een ernstig gevaar voor de rechtsorde opleveren".²⁶⁶

De themaverwerking is bedoeld om in een zeer vroeg stadium inzicht te krijgen in het beramen en plegen van zeer ernstige misdrijven. Er is op een aantal punten stevige kritiek geleverd op deze themaverwerkingen. Allereerst hebben verschillende schrijvers en instanties fundamentele kritiek op de toedeling van deze bevoegdheid aan de politie. Het verwerken van gegevens in een dergelijk prematuur stadium behoort volgens hen niet tot de taak van de

262 *Kamerstukken I*, 2006/2007, 30 327, nr. C, p. 3.

263 Cbp, *Advies over Wet politiegegevens: uitbreiding bevoegdheden vereist ook waarborgen*, z2004-0467, 29 maart 2004.

264 Schreuders, e.a., 2005, p. 70, alsmede verkennend onderzoek Kielman en Koelewijn.

265 Formeel gezien is ook de verwerkingsgrond van art. 10 lid 1 onder 3 c nieuw. Hiermee is echter de verwerking van gegevens door de RID, in het kader van haar openbare-orde-taak, geformaliseerd. Het gaat dan bijvoorbeeld om de registratie van gegevens in verband met voetbalsupportersrellen. Tenzij er een samenvoeging van de taken tussen de RID en de CIE plaatsvindt, waartoe sommige regio's hun wens hebben uitgesproken, behoort dit niet tot de taak van de CIE. *Kamerstukken II*, 2005/06, 30 327, nr. 3, p. 38.

266 Art. 10 lid 1 onder 3 b.

politie maar tot de taak van de inlichtingendiensten.²⁶⁷ Deze discussie gaat buiten het bereik van ons onderzoek. Het geeft echter wel aan dat de themaverwerkingen plaatsvinden met gevoelige gegevens en dat er een beweging waarneembaar is waar de politie met steeds zachtere informatie gaat werken. In het kader van het IPOL-project doet collega Vis onderzoek naar deze verhouding tussen de politie en veiligheidsdiensten.²⁶⁸

Als het gaat om de privacy-aspecten van de themaverwerking geeft de minister van justitie aan dat de toepassing van de themaverwerking erg beperkt is. De 'thema's' zijn beperkt tot (1) terrorisme en (2) mensenhandel. Hoewel er discussie bestaat waarom nu juist deze onderwerpen als 'thema's' zijn aangemerkt – met name de mensenhandel is onderwerp van discussie²⁶⁹ – zal de toepassing hiervan geen problemen opleveren voor de politiepraktijk aangezien in het Besluit politiegegevens de artikelnummers van de misdrijven zijn vermeld die als 'thema' mogen worden aangemerkt. In het Besluit politiegegevens – hier gezien als de bedoelde Algemene Maatregel van Bestuur – zijn evenwel meer misdrijven opgenomen dan terrorisme en mensenhandel. Zo is (3) het in- of uitvoeren van bepaalde drugs reden om als subject in een themaverwerking te worden opgenomen. Hetzelfde geldt voor (4) het omkopen van een opsporingsambtenaar, (5) het plegen van valsheid in geschrifte waarbij de schade groter is dan € 50.000,- en (6) het voorhanden hebben van een vuurwapen.²⁷⁰ Als het gaat om de toepassing van themaverwerkingen is het bereik dus, in tegenstelling tot dat wat de minister beweert, aanzienlijk breder dan terrorisme en mensenhandel. Het is voor ons onbegrijpelijk waarom de misdrijven waarvoor een themaverwerking is toegelaten zo breed zijn geformuleerd. Als het de minister alleen om terrorisme en mensenhandel te doen is, zou dat als oogmerk in het betreffende artikel van het Besluit politiegegevens vermeld dienen te worden. De wijze waarop dit onderdeel van het besluit is geformuleerd, lijkt in strijd met het specialiteitsbeginsel, dat eist dat wetgeving zo specifiek mogelijk wordt geformuleerd. Gezien het gat dat bestaat tussen de wens van de minister (themaverwerkingen voor terrorisme en mensenhandel) en de uitwerking in het besluit (ook themaverwerkingen voor relatief lichte misdrijven zoals verboden wapenbezit) wordt hier ons inziens niet aan voldaan.

In het licht van deze constatering is de kritiek van (1) Kielman en Koelewijn en (2) het CBP interessant. Zij verzetten zich tegen het feit dat het aanmerken van misdrijven als 'thema's' bij AMvB plaatsvindt.²⁷¹ Daardoor ont-

267 Kielman en Koelewijn, 2005, p. 454.

268 Dergelijk onderzoek vindt momenteel plaats in het kader van het NWO-onderzoek IPOL, Intelligence Led Policing, in een samenwerkingsverband tussen de universiteiten van Leiden en Universiteit van Tilburg. Zie ook: De Hert, Huisman & Vis 2005. Meesters, Kortekaas en Tragter, 2000.

269 Zie advies CBP over het eerste concept Besluit politiegegevens en de plenaire behandeling van de Wet politiegegevens in de Eerste Kamer, *Kamerstukken I*, 2006/07, 30 027.

270 Art. 3:1 Besluit politiegegevens.

271 Kielman en Koelewijn, 2005a, p. 454.

breekt volgens hen de democratische controle die noodzakelijk is op dergelijke ingrijpende beslissingen. Wanneer het politiek opportuun is, kan de minister van justitie in samenspraak met zijn collega's van binnenlandse zaken en defensie het aantal misdrijven uitbreiden waarvoor themaverwerkingen mogen worden uitgevoerd. Gezien het verstrekkende karakter van deze verwerkingen zou dit ons inziens bij formele wet dienen te worden bepaald, met bijpassende waarborgen.

Voor de politiepraktijk introduceren de themaverwerkingen een nieuw interpretatieprobleem. Het is thans de vraag over welke personen gegevens mogen worden geregistreerd in een themaregister. Volgens de wet dient de themaverwerking om "inzicht te krijgen in de betrokkenheid van personen bij handelingen die kunnen wijzen op het beramen of plegen van genoemde misdrijven".²⁷² Vanuit drie kanten is hierop stevige kritiek geuit.²⁷³ Het gaat dan met name om "handelingen die *kunnen wijzen op*". In de woorden 'kunnen wijzen' ligt een toekomstvoorspelling besloten. Op basis van de incidenten die zich in het verleden hebben voorgedaan, zal via de politie dienen te worden ingeschat of er in een individueel geval sprake is van handelingen die zouden kunnen wijzen op de betrokkenheid van die persoon bij het beramen of plegen van terroristische activiteiten. Het nemen van vlieglessen als moslim wordt daarmee juridisch gezien reden om door de politie in een themaverwerking terecht te komen. Als we dit in samenhang bezien met de constatering dat het bij themaverwerkingen niet alleen om terrorisme gaat, maar ook om het in- en uitvoeren van drugs en bijvoorbeeld het voorhanden hebben van een vuurwapen, zet het de deur open tot een grootschalige gegevensverwerking. Deze laatste opmerking stoelen wij op de constatering bij ons eigen veldwerk dat er aan de kant van de politie weinig terughoudendheid te bespeuren valt bij de inzet van de themaverwerkingen. In ons onderzoek in de CIE-praktijk is door meerdere CIE-en aangegeven dat ze graag gebruik gaan maken van de mogelijkheid die de themaverwerkingen bieden. Laten we voorop stellen dat we hiermee niet de CIE-en in een kwaad daglicht willen stellen, maar slechts willen aangeven dat zij geneigd zijn ten volle gebruik te maken van de mogelijkheden die door de wet aan hen worden geboden. Dat is hun goed recht, sterker nog, dat is hun plicht en dat wordt dan ook van hen verwacht door de samenleving. Nu echter (1) de afgrenzing van de personen over wie informatie mag worden verwerkt in deze themaverwerkingen onduidelijk is *en* (2) de gronden waarop dit is toegestaan ruimer zijn dan alleen de thema's terrorisme en mensenhandel, is een ongebreidelde gegevensverzameling en -verwerking onvermijdelijk.

272 Art. 10 lid 1 aanhef en onder c Wpolg.

273 Kielman en Koelewijn, 2005, p. 454. Advies CBP over het eerste concept Wet Politiegegevens en de plenaire behandeling van de Wet politiegegevens in de Eerste Kamer, *Kamerstukken I* 2006/2007, 30 327.

4.5.4 Tussenconclusie aangaande het opslaan

Alvorens we onze tussenconclusie aangaande het opslaan formuleren, geven we eerst het resultaat van de analyse schematisch weer. In figuur 4.2 zien we (a) de knelpunten, (b) de inhoud van de knelpunten, (c) de uitwerking daarvan onder de Wpolg, en (d) de (te verwachten) resultaten van die uitwerking.

Volg-nummer	Knelpunten Wpolr	Wpolg	Resultaat
1	Geen regeling informantregister	Verwerking van informantgegevens ingevoerd	Knelpunt opgelost
2	Afbakeningsknelpunt	De verwerking die vroeger onder het regime van het voorlopig register viel, is geschrapt	De gegevens vallen nu onder de 'normale' zwacriverwerking. Knelpunt opgelost, maar feitelijk leidt dit tot een verruiming van verwerkingsmogelijkheden.
3	Classificatieknelpunt a. Verdachte b. Betrokkene c. Contact d. Onverdachte personen	a. Onverkort gehandhaafd b. Onverkort gehandhaafd c. Onverkort gehandhaafd d. Opgelost door deze te schrappen	a. Knelpunt zal blijven bestaan b. Knelpunt zal blijven bestaan c. Knelpunt zal blijven bestaan d. Geen regeling voor onverdachte personen
4		Themaverwerking	Nieuw knelpunt geïntroduceerd

Figuur 4.2 Schematische weergave van de knelpunten 'opslaan'.

Wat het opslaan van gegevens betreft, komt de Wpolg voor een deel tegemoet aan de knelpunten die in 2007 in de praktijk leefden. Zo is het informantregister geformaliseerd en is regeling rond onverdachte personen geschrapt die voor de CIE-praktijk niet van toepassing was. Ook zijn de problemen die bestonden rond de toepassing van het voorlopig register opgelost. Feitelijk moet echter geconstateerd worden dat door de afschaffing van het voorlopig register een verruiming is geïntroduceerd (doordat de gegevens nu onder het zwacri-regime vallen). Door de verruiming is het afbakeningsknelpunt binnen de Wpolg opgelost en het classificatieknelpunt gedeeltelijk opgelost. Wat het onderscheid betreft naar 'verdachten', 'betrokkenen' en 'contacten' blijft het classificatieknelpunt echter bestaan.

Met de invoering van de themaverwerkingen haalt de Wpolg de grens voor de opslag van gegevens meer naar voren. Gelet op de formulering van de criteria voor de toepassing van deze verwerkingsgrond zullen bij de toepassing van de themaverwerking in de praktijk interpretatieproblemen ont-

staan. Om deze reden is de reikwijdte van de verwerkingsgrond, en daarmee ook de mate waarin deze afbreuk doet aan de vrijheid van gegevens, thans onbepaald. Gezien de houding van de CIE-en ten aanzien van die regelingen lijkt haar waarborgende werking ten aanzien van de opslag van gegevens tekort te schieten.

Samenvattend mogen we concluderen dat de Wpolg de onder de Wpolr geconstateerde knelpunten slechts voor een klein gedeelte heeft opgelost. Met name zien we dat de oplossing voor het afbakeningsknelpunt (afschaffing voorlopig register) weliswaar het knelpunt oplost, maar dat dit wel tot gevolg heeft dat het extra beschermende regime van dit voorlopig register in de verdere verwerking van die gegevens ook verloren is gegaan. Voorts is het classificatieknelpunt voor de onverdachte personen opgelost, maar zoals gezien speelde dit in de CIE-praktijk slechts een marginale rol. Het classificatieknelpunt deed zich juist voor bij de overige drie begrippen (verdachten, betrokkenen en contacten) en daar biedt de Wpolg geen oplossing voor.

Nu niet alle onder de Wpolr geconstateerde knelpunten zijn opgelost, en er zelfs een nieuw knelpunt geïntroduceerd lijkt te zijn, kan ten aanzien van het opslaan van gegevens worden geconcludeerd dat de Wpolg tekortschiet in zijn doelstelling de bestaande knelpunten op te lossen. De wetgever heeft echter zelf gesteld dat het zwaartepunt van de waarborgende werking van de wet is verschoven van het opslaan van gegevens naar het gebruik, in wettelijk termen: het verwerken (van gegevens). In dat licht mogen we hier als tussenconclusie formuleren dat bij de verwerking van gegevens steviger waarborgen noodzakelijk zijn, gezien de verruiming ten aanzien van het opslaan van gegevens. Dit maakt de problematiek, zoals die door Van Traa aan de orde werd gesteld, weer actueel.

4.6 BEWAREN

Wanneer gegevens in de systemen van de CIE zijn opgeslagen, dient zich ogenblikkelijk de vraag aan voor hoelang die informatie in die systemen mag blijven staan. Met andere woorden: wat zijn de bewaartermijnen? In deze sectie voeren we de driestappenbehandeling²⁷⁴ uit op het verwerkings-element 'bewaren'. Daaronder verstaan we ook de handelingen 'verwijderen' en 'vernietigen'. In sectie 4.6.1 bespreken we de theorie van het opslaan zoals die gold onder de Wpolr. In sectie 4.6.2 bespreken we de daarbij in de praktijk geconstateerde knelpunten. Voorts behandelen we in sectie 4.6.3 op welke wijze de Wpolg tegemoet komt aan de geconstateerde knelpunten met betrekking tot het bewaren van gegevens. In 4.6.4 geven we een tussenconclusie.

274 Zoals beschreven in sectie 4.4.

4.6.1 Theoretisch kader

De bewaartermijnen waren in de Wpolr als gevolg van de registerstructuur uitgesplitst per register. Daarnaast kende de Wpolr een aantal algemene bepalingen die op de bewaartermijnen van invloed waren. Ten eerste bepaalde art. 4 lid 2 Wpolr dat in een register slechts gegevens mochten worden opgeslagen voor zover dat noodzakelijk was voor het doel van het register. Dit betekent dat gegevens die niet (meer) in overeenstemming waren met het doel uit het register verwijderd dienden te worden. Ten tweede werd in art. 10 lid 2 onder d Wpolr opgedragen in het reglement van een register op te nemen, dat gegevens die verwijderd werden ook vernietigd dienden te worden zodra dit mogelijk was. Wat precies de betekenis was van de toevoeging 'zodra dit mogelijk is' is niet duidelijk, de memorie van toelichting vermeldt daar niets over. De onderzoekers van het WODC-evaluatierapport stellen dat dit in ieder geval niet de mogelijkheid biedt voor een archieffunctie.²⁷⁵ We gaan hier nader op in bij de behandeling van de bewaartermijnen per register.

Het register zware criminaliteit

Art. 13 a lid 8 Wpolr bevatte de regeling aangaande het verwijderen en vernietigen van gegevens uit het register zware criminaliteit. Daarmee gaf zij impliciet de bewaartermijn voor de gegevens die in dit register waren geregistreerd. Art. 13 a lid 8 Wpolr bepaalde het volgende:

“Gegevens als bedoeld in het eerste lid worden uit het register zware criminaliteit verwijderd en vernietigd indien zij niet langer noodzakelijk zijn voor het doel van het register dan wel na verloop van vijf jaar na datum van de laatste opname van gegevens die blijken geven van de noodzaak tot registratie van betrokkene met het oog op het doel van het register.”

Het register zware criminaliteit kende blijkens de wettekst twee momenten waarop opgenomen gegevens verwijderd dienden te worden. Ten eerste was dat op het moment dat de in het register opgenomen gegevens niet meer noodzakelijk bleken te zijn voor het doel van het register. Hiertoe moesten de gegevens op een regelmatige basis worden beoordeeld. Ten tweede was er een hardere termijn van 5 jaar. Het moment waarop deze 5 jaar termijn ging lopen was echter flexibel. In beginsel ging de 5-jaar-termijn lopen op het moment dat een gegeven in het register zware criminaliteit werd geregistreerd. Waren de 5 jaren vervolgens verstreken, dan diende het betreffende gegeven te worden verwijderd. Werd er echter in de tussentijd een nieuw gegeven geregistreerd dat bleek gaf van de noodzaak van de registratie van het eerste gegeven, dan ving de 5-jaar-termijn opnieuw aan. Het ging dan veelal om aanvullende gegevens. De condities waaronder nieuwe gegevens de noodzaak van registratie van de eerdere gegevens aantoonde, waren

275 Schreuders e.a., 2005, p. 129.

niet geheel duidelijk. Het was een afweging die veelal afhing van de omstandigheden van het geval. Pas als dus 5 jaar lang geen aanvullende gegevens in het register waren opgenomen, was de uiterste bewaartermijn voor de gegevens verstreken. Het kon daarom in de praktijk voorkomen dat gegevens voor langere tijd in het register stonden geregistreerd. Het was derhalve niet ondenkbaar dat over personen, die er een criminele carrière op na hielden, er druppelsgewijs informatie bij de CIE binnenkwam, waardoor de noodzaak van de registratie van eerdere informatie telkenmale werd aangetoond. Registratie van gegevens door de CIE voor bijvoorbeeld een periode van 20 jaar was dan denkbaar. Een keiharde uiterlijke termijn was niet in de regelingen opgenomen.

In art. 9 lid 3 van het modelreglement van het register zware criminaliteit staat voorts dat gegevens die verwijderd worden terstond dienden te worden vernietigd. Verwijderen stond dus in theorie gelijk aan vernietigen.

Het voorlopig register

Het doel van het voorlopig register was om te dienen als voorportaal van het register zware criminaliteit. Gegevens werden in het voorlopig register opgenomen om te bezien of deze gegevens in aanmerking kwamen voor registratie in het register zware criminaliteit. De bewaartermijn was op deze doelstelling afgestemd. Art. 13 b lid 5 Wpolr bepaalde:

“Gegevens als bedoeld in het eerste lid worden uit het voorlopig register verwijderd en vernietigd indien zij niet langer noodzakelijk zijn voor het doel van het register dan wel na verloop van zes maanden na datum eerste opname.”

Ook het voorlopig register kende een tweeledig verwijderingsregime. Ten eerste was verwijdering aan de orde indien gegevens niet meer noodzakelijk bleken voor het doel van het register. Gezien het doel van het voorlopig register betekende dit dat verwijdering aan de orde was zodra was gebleken dat de verkregen gegevens onjuist waren of om andere redenen nooit in aanmerking zouden komen voor registratie in het register zware criminaliteit. Ten tweede kende het voorlopig register, in tegenstelling tot het register zware criminaliteit, wel een harde verwijderingstermijn. Indien het 6 maanden na de opname van gegevens in het register niet was gelukt om ze zwacri-waardig te maken dan dienden ze verwijderd te worden. De uiterlijke bewaartermijn was 6 maanden. Daarna diende een gegeven ofwel te worden opgewaardeerd naar het register zware criminaliteit ofwel te worden verwijderd.

Het was ten aanzien van het voorlopig register onduidelijk of na verwijdering van de gegevens deze ook vernietigd dienden te worden. Art. 13b lid 5 van de Wpolr stelde dat gegevens uit het voorlopig register verwijderd en vernietigd dienden te worden indien één van de twee hierboven beschreven omstandigheden zich voordeed. We hebben in de aanhef van sectie 4.6 betoogd dat in de algemene bepalingen van de wet ruimte leek te zijn voor een bepaalde tijdspanne tussen het verwijderen en het vernietigen van gegevens. Anders dan bij het register zware criminaliteit werd in het modelreglement

dat van toepassing was op het voorlopig register niet gesteld dat gegevens die verwijderd dienden te worden ook terstond vernietigd dienden te worden.

Het informantenregister

Zoals in sectie 4.5 beschreven is, kende het informantenregister geen wettelijke regeling onder de Wpolr. Het CBP heeft aangegeven het gebruik van het informantenregister te gedogen zolang de CIE-en het register voeren in overeenstemming met het door het CBP opgestelde modelreglement. Het modelreglement bevatte een regeling in art. 8 betreffende het verwijderen en vernietigen van de in dit register opgenomen gegevens, die stelt:

“Informantgegevens worden uit het register verwijderd en terstond vernietigd wanneer deze niet meer noodzakelijk zijn voor het doel van het register. Hiertoe wordt het register minimaal tweemaal per jaar gecontroleerd.”

Anders dan bij het register zware criminaliteit en het voorlopig register was ten aanzien van het informantenregister geen sprake van twee eindtermijnen. Slechts wanneer een gegeven niet meer noodzakelijk was voor het doel van het informantenregister diende het gegeven te worden verwijderd. Dit betekende dat de in het informantenregister opgenomen gegevens voor lange tijd daarin zouden worden opgeslagen. Met het oog op het doel van het register (het beheer van de informanten en de beoordeling van de door informanten gegeven informatie op juistheid en volledigheid) was dit ook te rechtvaardigen. Wanneer een informant informatie aan de CIE geeft, is het van belang te weten of die informant eerder informatie aan de CIE heeft gegeven en wat daar toen mee is gebeurd. Verwijdering en vernietiging van gegevens uit het informantenregister was om die reden niet aan een maximale termijn gebonden.

4.6.2 De knelpunten beschreven

In de praktijk van de CIE werd niet gesproken over verwijdering en vernietiging van gegevens, maar over schoning. Met de behandelde 5-jaar-termijn in het register zware criminaliteit werd vrij strikt omgegaan. Gegevens die 5 jaar onaangevuld in een register zware criminaliteit zaten, werden verwijderd.²⁷⁶ Ook het CBP constateerde in een uitgevoerde steekproef in 2003/2004 dat in het algemeen netjes met de bewaartermijn werd omgesprongen.²⁷⁷

In het onderzoek van Kielman en Koelewijn kwam naar voren dat CIE-en zelf ook weinig moeite hebben met het schonen van de registers na 5 jaar. Indien in 5 jaar informatie niet was aangevuld, was deze toch vrijwel waar-

²⁷⁶ Schreuders e.a., 2005, p. 130.

²⁷⁷ *Algemene bevindingen CIE-onderzoeken College bescherming persoonsgegevens*, september 2004.

deloos geworden voor de CIE. In het onderzoek kwam verder naar voren dat op deze regel één praktische uitzondering was. Wanneer een subject gedurende langere tijd gedetineerd had gezeten, was het volgens een aantal CIE-en wenselijk dat ook de gegevens die zij aangaande dat subject hadden geregistreerd bewaard bleven in het register zware criminaliteit. Het was vanzelfsprekend dat wanneer een subject voor 8 jaar gedetineerd was, het gedurende die 8 jaar niet waarschijnlijk is dat informatie over hem werd aangevuld. Gezien de recidive-cijfers was er daarentegen wel een goede kans dat hij na vrijlating zijn oude 'beroep' weer op zou pakken. De bij de CIE aanwezige 'verouderde' informatie was dan nog relevant. De CIE-en die wij gesproken hebben, kiezen er in een dergelijke situatie voor de wettelijke bewaartermijn te laten voor wat hij is en de gegevens in het register te laten staan. Zo blijkt ook het WODC-evaluatieonderzoek.²⁷⁸

De maximale bewaartermijn van het voorlopig register bleek in de praktijk streng te worden nageleefd. Na het verlopen van de 6 maanden werd beoordeeld of een gegeven nog kon worden aangevuld om het zodoende op te waarderen naar het register zware criminaliteit. Lukte dit niet dan werd het gegeven verwijderd uit het voorlopig register. Voor zover wij hebben kunnen nagaan in de beschikbare bronnen, werd het dan ook vernietigd.

Ad (1) Drie knelpunten door noodzakelijkheidseis

Het begrip noodzakelijkheid speelt een belangrijk rol bij het bewaren van gegevens en de daarmee gepaard gaande termijnen. Bij elk van de drie registers (informantenregister, voorlopig register, en het register zware criminaliteit) dienden onder de Wpolr gegevens verwijderd te worden indien deze niet meer noodzakelijk waren voor het doel waarvoor het register was aangelegd. Bij de toepassing van dit begrip in de praktijk stuitte we op drie knelpunten, (a) de onbepaaldheid van het begrip, (b) de werkdruk die de toepassing ervan met zich meebrengt en (c) de tegenstrijdigheid met het doel van het informantenregister. We beschrijven knelpunten hieronder als (1a), (1b), en (1c).

Ad (1a) De onbepaaldheid

Uit zowel het onderzoek van Kielman en Koelewijn als het WODC-evaluatieonderzoek is gebleken dat CIE-en niet in staat waren te bepalen of gegevens die op dat moment in hun register stonden geregistreerd nog noodzakelijk waren voor het doel van het register.²⁷⁹ Het kon immers altijd gebeuren dat na het beoordelingsmoment nog nieuwe informatie bekend zou worden, waardoor wel weer een noodzaak zou ontstaan. Informatie die op moment x niet meer noodzakelijk lijkt, kan op een later moment y toch noodzakelijk blijken. We noemen dit de onbepaaldheid van de noodzakelijkheid. Op dit gebied was de geconstateerde onduidelijkheid inherent aan het werken met zachte informatie in de pro-actieve fase.

²⁷⁸ Schreuders e.a., 2005, p. 130.

²⁷⁹ Schreuders e.a., 2005, p. 131.

Ad (1b) De werkdruk

In de twee genoemde onderzoeken van Kielman en Koelewijn en het WODC gaven CIE-en aan dat het op regelmatige basis uitvoeren van een noodzakelijkheidsonderzoek op de aanwezige gegevens een dusdanige arbeidsintensieve klus was dat daarvoor de mankracht ontbrak. Het gaat dan om de werkdruk in relatie tot de noodzakelijkheid. De samenloop van de onbepaaldheid van het begrip noodzakelijkheid aan de ene kant en de werkdruk aan de andere kant heeft er in de praktijk toe geleid dat er mondesmaat werd geschoond op basis van het noodzakelijkheids criterium.

Ad (1c) De tegenstrijdigheid met het doel van het informantenregister

Met betrekking tot de informatie in het informantenregister werden dezelfde problemen geconstateerd ten aanzien van het noodzakelijkheids criterium. Het was voor de CIE niet mogelijk te bepalen of de in het informantenregister opgeslagen informatie in de toekomst nog noodzakelijk zou zijn. Zelfs na het overlijden van de informant kan de opgeslagen informatie nog nodig zijn, bijvoorbeeld ter verantwoording van het optreden van de CIE tijdens een strafzaak.²⁸⁰ Een maximale bewaartermijn voor het informantenregister was er niet. In de praktijk werden de informantenregisters niet geschoond. Levenslang bewaren van informanteninformatie was om twee redenen minder bezwaarlijk dan het bewaren van de informatie over subjecten die in het zwacri-register waren opgenomen. Ten eerste had de informant een contract met de CIE afgesloten en daarin was opgenomen, althans de informant moest dat begrijpen, dat zijn gegevens werden opgeslagen in een geautomatiseerd systeem. Het subject in het zwacri-register heeft, in het algemeen, er geen weet van dat er informatie over hem in het register is opgeslagen.²⁸¹ Ten tweede was de informatie, die de informant had gegeven en die tot hem herleidbaar was, voor andere personen en instellingen dan de CIE afgesloten en deed de CIE alles wat in haar macht lag om dat ook zo te houden. Het levenslang bewaren van informanteninformatie – we hebben het dan over de bruto-verslagen – was daarnaast van belang omdat de CIE zich op die manier bijvoorbeeld een oordeel kon vormen over de betrouwbaarheid van de door de informant geleverde informatie. Dit gold ook voor de informant als hij in de toekomst informatie zou leveren die geen betrekking had op de eerder geleverde informatie.

Op dit punt zij echter opgemerkt dat dit knelpunt voor het informantenregister niet als knelpunt van de Wpolr aangemerkt kan worden omdat een regeling rond het informantenregister daarover ontbreekt. Niettemin hebben we dit punt wel in het schema in subsectie 4.6.4 opgenomen.

280 Schreuders e.a., 2005, p. 103.

281 Op de problematiek van kennisneming van de informatie uit de registers van de CIE wordt in hoofdstuk 5 uitgebreid ingegaan.

4.6.3 Uitwerking onder de Wpolg

Onder de Wpolg is vanwege het afschaffen van het voorlopig register vanzelfsprekend geen regeling opgenomen over de bewaartermijnen in dat register. Wat het register zware criminaliteit en het informantenregister betreft blijven de geconstateerde knelpunten bestaan.

Oude knelpunten aangepakt

Gegevens die op grond van art. 10 Wpolg worden verwerkt (de 'opvolger' van het register zware criminaliteit), dienen te worden verwijderd indien deze niet meer noodzakelijk zijn voor het doel van de verwerking. Tot zover zijn er geen wijzigingen ten opzichte van de regeling onder de Wpolr. De Wpolg voorziet ook niet in een nadere specificering van het noodzakelijkheids criterium. Dit betekent ook dat het onder de Wpolr geconstateerde knelpunt aangaande de toepassing van het noodzakelijkheids criterium onder de Wpolg niet is opgelost.

Nieuw is de regeling dat de gegevens hiertoe ieder half jaar dienen te worden gecontroleerd. Het gaat hier blijkens de bewoordingen om een verplichting die het argument van de CIE-en opzij zet dat er geen tijd is voor dergelijke controles. Er wordt niet ingegaan op de manier waarop deze controles uitgevoerd dienen te worden en hoe de CIE dient om te gaan met het feit dat ze niet in staat is om te bepalen of een gegeven in de toekomst wellicht aan het noodzakelijkheids criterium gaat voldoen.

Nieuwe knelpunten geïntroduceerd

Naast de knelpunten rond het noodzakelijkheids criterium introduceert de Wpolg ook een knelpunt bij het 5-jaars-criterium dat het bewaren van art.-10-gegevens reguleert. Onder de Wpolg moet een gegeven verwijderd worden 5 jaar na de laatste verwerking die blijkt geeft van de noodzaak tot registratie. Art. 10 lid 6 Wpolg stelt:

"[...] De gegevens worden verwijderd uiterlijk vijf jaar na de datum van de laatste verwerking van gegevens die blijkt geeft van de noodzaak tot het verwerken van de politiegegevens [...]"

Wanneer men de tekst van art. 10 bekijkt, wordt er gesproken over de "laatste verwerking van gegevens". Naar de letter van de wet kan deze verwerking een opname van nieuwe gegevens zijn, maar kan de 5-jaar-termijn ook opnieuw aanvangen bij een hernieuwde verwerking van dezelfde gegevens. Hoewel in art. 10 lid 6 Wpolg wordt gesproken van "de laatste verwerking van gegevens" is blijkens de memorie van toelichting bedoeld dezelfde situatie te handhaven waarvan onder de Wpolr sprake was.²⁸² De wetgever stelt daar dat er sprake dient te zijn van nieuwe (aanvullende) gegevens die blijkt geven van de noodzaak tot registratie. Over een eventueel breder bereik, dat

282 Kamerstukken II 2005/06, 30 327, nr. 3, p. 51.

het begrip verwerken in beginsel wel met zich meebrengt, wordt niet gesproken. Hieronder bespreken we (a) verwijderen is niet vernietigen en (b) de 10-jaar-termijn voor de art.-11-verwerking.

A. Verwijderen is niet vernietigen

Als gegevens, die op grond van art. 10 Wpolg zijn verwerkt, dienen te worden verwijderd, dan hoeven deze onder het regime van de Wpolg niet te worden vernietigd. Gegevens die verwijderd dienen te worden, mogen voor nog eens 5 jaar worden bewaard. Na deze 5 jaar dienen ze vernietigd te worden. Onder een eerdere versie van het wetsvoorstel werd gesproken over het plaatsen van gegevens achter een 'schot', waar ze onder bepaalde omstandigheden vandaan mochten worden gehaald om ze opnieuw te verwerken.²⁸³ Wij duiden de gegevens die zijn verwijderd en achter het 'schot' zijn geplaatst aan als *shotgegevens*. Onder de huidige versie van de Wpolg bestaan de shotgegevens nog steeds, maar zijn de bewaartermijn en de redenen voor hernieuwde verwerking beperkt. In beginsel mogen deze gegevens alleen worden bewaard voor het afhandelen van klachten en voor de verantwoording van de verrichtingen van de CIE.²⁸⁴ Op grond van art. 14 lid 3 Wpolg kunnen deze shotgegevens in 'bijzondere gevallen' in opdracht van de officier van justitie²⁸⁵ opnieuw worden verwerkt onder het regime van art. 10 Wpolg. Kort gezegd mogen de shotgegevens gedurende de 5 jaar dat ze daar bewaard worden in bijzondere gevallen achter het schot vandaan worden gehaald om ze op de gebruikelijke CIE-wijze te verwerken. In de memorie wordt aangegeven dat deze hernieuwde verwerking uitzondering dient te zijn. Op voorhand moet duidelijk zijn voor welk doel de shotgegevens worden teruggehaald; voorts moet de terughaling noodzakelijk zijn en de daarvoor benodigde gegevens moeten bekend zijn. De officier van de justitie dient opdracht te geven voor het opnieuw verwerken van deze shotgegevens.²⁸⁶

Noch in de memorie van toelichting, noch in het besluit Wpolg is uitgelegd wanneer van deze bijzondere gevallen sprake is. Daarnaast verbaast het ons dat niet is ingegaan op de vraag wie er in de praktijk bepaalt welke gegevens voor een hernieuwde verwerking in aanmerking komen. Gezien de criteria die gelden voor een hernieuwde verwerking zijn er twee mogelijkheden om te bepalen of shotgegevens in aanmerking komen voor hernieuwde verwerking. Ten eerste kan de CIE-officier van justitie de shotgegevens regelmatig controleren en beoordelen of deze voor hernieuwde verwerking in aanmerking komen. Hij wordt dan feitelijk beheerder van de shotgegevens. Ten tweede kunnen de CIE-runners de shotgegevens met

283 Kielman en Koelewijn, 2005, p. 455-456.

284 Art. 14 lid 1 Wpolg.

285 En volgens het artikel ook de burgemeester, deze zal in de praktijk ten aanzien van de CIE echter geen feitelijke zeggenschap hebben. Deze ligt bij de CIE-officier van justitie. Zie over de taakverdeling uitgebreid hoofdstuk 6.

286 *Kamerstukken II* 2005/06, 30 327, nr. 3, p. 65-66.

enige regelmaat controleren op de noodzakelijkheid tot hernieuwde verwerking. Vanzelfsprekend gaat het hier om twee uiterste mogelijkheden, waarbij vele tussenvarianten denkbaar zijn. Zo kan bijvoorbeeld het hoofd van de CIE worden belast met taak om te beoordelen of er in een lopend onderzoek ruimte is voor een hernieuwde verwerking van de schotgegevens. Wanneer iemand anders dan het bevoegd gezag deze beslissing neemt, dient dit met het bevoegde gezag overlegd te worden zodat deze zijn toestemming kan geven voor de hernieuwde verwerking. Gezien het feit dat de CIE-runners en het hoofd CIE inhoudelijk beter op de hoogte zijn van de aanwezige informatie dan de CIE-officier van justitie ligt het voor de hand dat zij de eerste selectie uitvoeren. Naar onze verwachting zullen gegevens die als schotgegevens dienen te worden aangemerkt tezamen met de 'gewone' gegevens in dezelfde database worden bewaard. De schotgegevens zullen daarbij een 'label' krijgen waaruit blijkt dat het om schotgegevens gaat en dat voor een verwerking van die gegevens dus de toestemming van het bevoegde gezag nodig is.

Dit systeem is vergelijkbaar met de wijze waarop onder de Wpolr een onderscheid wordt gemaakt tussen het voorlopig register en het zwacri-register. De gegevens die onder het regime van het voorlopig register vielen, werden in register zware criminaliteit opgeslagen en voorzien van het label 'vl'.²⁸⁷ In de Wpolg of het Bpolg is niets opgenomen over de wijze waarop het bewaren van de schotgegevens en de toegang daartoe moet worden georganiseerd.

B. De 10-jaars-termijn voor de art.-11-verwerking

Met een wettelijke regeling rond het informantenregister is ook de bewaartermijn voor deze soort gegevens aangescherpt. Evenals onder de Wpolr geldt voor informantgegevens de noodzakelijkheidseis. Zodra informantgegevens niet meer noodzakelijk zijn voor het doel van de verwerking dienen de gegevens vernietigd te worden.²⁸⁸ Een belangrijk verschil met de zware-criminaliteitsverwerking is dat art. 12 lid 6 geen verwijdering van gegevens eist, maar vernietiging. Ook hier eist de wet dat de gegevens elk half jaar worden gecontroleerd op noodzakelijkheid. Daarnaast is onder de Wpolg een uiterlijke termijn ingevoerd voor het bewaren van informantgegevens. Art. 12 lid 6 Wpolg derde volzin bepaalt dat 10 jaar na de laatste gegevensverwerking die blijkt geeft van de noodzaak van registratie van de betreffende informantgegevens, deze gegevens vernietigd dienen te worden. De memorie van toelichting geeft in de toelichting op het artikel geen duidelijkheid of met de zinsnede 'verwerking van gegevens' uitsluitend wordt bedoeld op de opname van nieuwe (aanvullende) gegevens. Zo stelt de toelichting:

287 Zie uitgebreid subsectie 4.5.2.

288 Art. 12 lid 6 eerste volzin Wpolg.

*“In dit lid wordt bepaald dat de gegevens worden vernietigd uiterlijk na verloop van tien jaren na de datum van de laatste opname van gegevens die blijken geven van de noodzaak tot het verwerken van de persoonsgegevens van betrokkene met het oog op het doel [...]”*²⁸⁹

Even verderop stelt de memorie van toelichting bij lid 6 echter:

*“Na verloop van tien jaar na de laatste verwerking van gegevens die blijken geeft van de noodzaak tot het verwerken van persoonsgegevens van betrokkene [...] moeten de gegevens worden vernietigd.”*²⁹⁰

En even verderop in de toelichting op hetzelfde lid:

*“Na verloop van tien jaar moeten de gegevens worden vernietigd, behoudens wanneer er binnen die termijn aanleiding bestaat voor het verwerken van politiegegevens [...]”*²⁹¹

Kennelijk is de opname van gegevens toch niet bepalend voor de aanvang van de bewaartermijn, maar de ‘verwerking van gegevens’. Zoals hierboven beschreven is, valt naast het opslaan van gegevens nog menig andere handeling onder het begrip verwerken (bijvoorbeeld bewaren, verstrekken, wijzigen enz.). Een belangrijk verschil is dat er geen sprake hoeft te zijn van een nieuw (aanvullend) gegeven om de 5-jaar-termijn opnieuw te laten aanvangen. Onder de Wpolg gaat de bewaartermijn lopen vanaf de laatste verwerking die blijken geeft van de noodzaak tot registratie. Een belangrijk verschil tussen deze twee benaderingen is dat de registratie van een nieuw gegeven een van buitenaf komende factor is die bepaalt of het oorspronkelijke gegeven nog geregistreerd kan blijven. We merken hier op dat de verwerking die onder de Wpolg bepalend wordt een handeling is die een ambtenaar van politie verricht met het gegeven. Dit kan een opname van nieuwe (aanvullende) gegevens zijn, maar bijvoorbeeld ook het feit dat het betreffende gegeven onderdeel is geweest van een analyse die is losgelaten op verschillende gegevensbestanden of een verstrekking aan een andere CIE. Het begrip verwerken omvat immers iedere handeling die je met een gegeven kan uitvoeren. Het antwoord op de vraag wanneer uit die handeling een noodzaak voor registratie blijkt, is sterk afhankelijk van het resultaat dat met de verwerking van het gegeven behaald wordt. Het enkele feit dat een gegeven wordt bewaard (een vorm van verwerken) brengt nog niet direct met zich mee dat registratie voor nog eens 10 jaar noodzakelijk is. Ook het verstrekken aan een andere regio leidt naar onze mening niet automatisch tot een dergelijke noodzakelijkheid. Dat hangt in zo’n geval namelijk af van de vraag of de ontvangende regio iets met dat gegeven heeft kunnen doen of dat het voor hen nutteloos is gebleken. Ten slotte is er bij de verwerking van informanteninformatie geen onderscheid tussen verwijderen en vernietigen.

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

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

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

Zoals hierboven beschreven wordt in art. 12 alleen de term vernietigen gebruikt en niet verwijderen. Er is met betrekking tot informantgegevens dan ook geen sprake van een schot waarachter gegevens kunnen worden geplaatst.

4.6.4 Tussenconclusie aangaande het bewaren

Alvorens we onze tussenconclusie aangaande het bewaren formuleren geven we eerst schematisch weer (a) het aantal onder de Wpolr geconstateerde knelpunten, (b) de inhoud van die knelpunten, (c) de uitwerking daarvan onder de Wpolg en (d) de (te verwachten) resultaten van de uitwerking onder de Wpolg.

Aantal	Knelpunten Wpolr	Wpolg	Resultaat
1	Onbepaaldheid van de noodzakelijkheidseis	Hanteert eis onverkort zonder afdoende precisering	Knelpunt niet opgelost
2	Werkdruk i.v.m. noodzakelijkheidseis	Halfjaarlijkse controle is verplicht gesteld	Knelpunt opgelost, gaat ten koste van andere werkzaamheden
3	Noodzakelijkheidseis strijdig met doel van het informantenregister	Hanteert eis onverkort	Knelpunt niet opgelost
4	–	Noodzakelijkheidseis bij 5-jaar-termijn ingevoerd	Nieuw knelpunt geïntroduceerd

Figuur 4.3. Schematische weergave knelpunt 'bewaren'.

In deze sectie hebben we de driestappenbehandeling uitgevoerd op de regels die gelden voor het bewaren van informatie door de CIE. Bij de analyse van de knelpunten in de uitwerking van de huidige regelgeving hebben we twee belangrijke constatering gedaan: (1) de in de praktijk geldende eindtermijn van 5 jaar na de laatste gegevensopname, die blijkt geeft van een noodzaak tot registratie van de betreffende gegevens, functioneerde goed. Hetzelfde geldt voor de 6-maandentermijn die van toepassing is op de gegevens in het voorlopig register; (2) de knelpunten die de praktijk ervaart met de toepassing van het noodzakelijkheids criterium zijn moeilijk oplosbaar. Het gaat dan om drie verschillende toepassingen van het noodzakelijkheids criterium. Ten eerste blijkt het inhoudelijk onmogelijk voor de CIE om het criterium toe te passen. Door de wetgever zijn geen criteria gegeven op basis waarvan kan worden bepaald of een gegeven nog noodzakelijk is voor het doel van de verwerking. Ten tweede wordt vanuit de CIE aangegeven dat het eenvoudig aan tijd ontbreekt om de controle uit te voeren. Ten derde verhoudt de noodzakelijkheidseis zich niet tot het doel van het informantenregister. Het blijkt onmogelijk om te bepalen of een gegeven in de toekomst noodzakelijk is voor het doel van dat register. Op basis van informanteninformatie probeert de CIE inzicht te krijgen in de zware criminaliteit en de ontwikkelingen daarin.

Dit opbouwen van de informatiepositie en het pro-actieve karakter van het werk brengen met zich mee dat achteraf pas kan worden bepaald of gegevens die de afgelopen jaren door de CIE zijn verwerkt daarvoor noodzakelijk waren. Vooraf is die beslissing voor de CIE onmogelijk.

Onder de Wpolg worden deze knelpunten niet opgelost, integendeel. Voor zowel de zware criminaliteitsverwerkingen als de informantieverwerkingen laat de Wpolg het noodzakelijkheids criterium intact. Aan de knelpunten die de praktijk ondervindt met de toepassing hiervan wordt geen oplossing geboden.

Van de wetgever had evenwel verwacht mogen worden dat zij de praktijk met de Wpolg had voorzien van een verduidelijking van de noodzakelijkheidsstoets. Noch voor de inhoudelijke problemen bij de toepassing ervan, noch voor het tijdsgebrek dat CIE-en ondervinden bij de toepassing ervan, werden oplossingen geboden. Wel gunstig is dat de CIE-en onder de Wpolg worden verplicht de noodzakelijkheidstoets twee maal per jaar uit te voeren. Dat is vanuit de optiek van gegevensbescherming een positieve ontwikkeling. CIE-en worden op die manier immers verplicht om twee keer per jaar hun systeem te schonen. Vanuit het oogpunt van de politietaak is het evenwel de vraag of dit een wenselijke ontwikkeling is. Vanuit de praktijk is immers aangegeven dat de uitvoering van de noodzakelijkheidstoets veel tijd kost. Die tijd zullen de CIE-en onder het regime van de Wpolg niet kunnen besteden aan hun overige taken.

We mogen derhalve concluderen dat de Wpolg de helderheid rond de bewaartermijnen niet verbetert. Ten eerste is het voor de CIE ontoepasbare noodzakelijkheids criterium in zowel het geval van verwerkingen op grond van art. 10 Wpolg als art. 11 Wpolg ongewijzigd gebleven. Ten tweede is de toepassing van de uiterlijke registratietermijn op grond van art. 10 Wpolg bemoeilijkt door de aanvang van de 5-jaar-termijn te koppelen aan de laatste verwerking van het betreffende gegeven, in plaats van aan de laatste nieuwe registratie die blijkt geeft van de noodzaak van die registratie. Hoewel de Wpolg de bewaartermijnen oprekt, zijn er in de regelingen over het verwijderen en vernietigen geen aanvullende waarborgen ter bescherming van de grondrechten van de burger geformuleerd.

4.7 VERSTREKKEN

Hierboven hebben we het opslaan en bewaren van gegevens behandeld. Daarmee wordt het begin en het einde van de opslag in een geautomatiseerd systeem van een gegeven bij de CIE bepaald. In de tijd dat een gegeven door de CIE wordt bewaard mag zij daar vanzelfsprekend iets mee doen. Het verstrekken van de gegevens is daarvan de belangrijkste taak. In deze sectie voeren we de driestappenbehandeling²⁹² uit op het verwerkingselement 'verstrekken'. In subsectie 4.7.1 bespreken we de theorie van het verstrekken

292 Zoals beschreven in sectie 4.4.

zoals die gold onder de Wpolr. In subsectie 4.7.2 bespreken we de daarbij in de praktijk geconstateerde knelpunten. Voorts behandelen we in subsectie 4.7.3 op welke wijze de Wpolg tegemoet komt aan de geconstateerde knelpunten met betrekking tot het verstrekken van gegevens. In subsectie 4.7.4 geven we een tussenconclusie aangaande het verstrekken.

4.7.1. Theoretisch kader

Ook ten aanzien van het verstrekken werd in de Wpolr onderscheid gemaakt tussen de verschillende soorten registers. In de algemene bepalingen van de Wpolr was in art. 1, lid 1 onder h Wpolr het verstrekken van gegevens uit een politieregister gedefinieerd als:

“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 verwerking daarvan, al dan niet in verband met andere gegevens, zijn verkregen”

Het begrip verstrekken was een wat misleidend begrip, doordat van het begrip de implicatie uitging dat het gaat om het actief verstrekken van informatie door een persoon aan een ander. Dat was gelet op de wettelijke definitie van het begrip ‘verstrekken’, zoals hierboven weergegeven, echter niet het geval. Aan een ambtenaar die geautoriseerd was om in een bepaald register informatie te kunnen inzien werd die informatie ‘ter beschikking gesteld’, zodat het enkele inzien van die informatie een verstrekking was in de zin van de wet. Ook die verstrekkingen moesten plaatsvinden conform het op het geraadpleegde register toepasselijke verstrekkingssysteem.

Voorts moet vooropgesteld worden dat het verstrekkingssysteem van de Wpolr een gesloten karakter had. Dit wil zeggen dat gegevens alleen aan die personen of instanties verstrekt mochten worden die expliciet in de Wpolr waren genoemd. Het verstrekkingssysteem kende binnen dat gesloten stelsel evenwel een verplichtend karakter. Dat wil zeggen dat indien een persoon of instantie was aangemerkt als ontvangstgerechtigde deze ook recht had op informatie, tenzij de verstrekking partij een beroep kon doen op een weigeringsgrond. Binnen het gesloten stelsel van verstrekkingen moest informatie dus zo veel mogelijk verstrekt worden.

Alvorens het wettelijk verstrekkingssysteem dat toepasselijk was op het register zware criminaliteit, het voorlopig register en het informantenregister te behandelen, merken wij op dat Koelewijn uitgebreid onderzoek heeft gedaan naar de mogelijkheden tot het verstrekken van gegevens en de daarbij geconstateerde knelpunten in de politiepraktijk. Om die reden wordt in dit onderzoek volstaan met een globale weergave van het verstrekken van gegevens en de daarbij geconstateerde knelpunten. Waar nodig wordt verwezen naar het onderzoek van Koelewijn voor meer achtergrondinformatie.

Het register zware criminaliteit

Het verstrekkingssysteem van het register zware criminaliteit ging uit van de verschillende soorten gegevens die in het register zijn opgeslagen. Het ging dan onder meer om (1) 'verdachten', (2) 'betrokkenen', en (3) 'contacten'.²⁹³ Op verstrekkingen uit het register zware criminaliteit was voor een groot deel het verstrekkingssysteem van toepassing dat ook op de reguliere politieregisters van toepassing was. Het ging dan om het systeem zoals dat was neergelegd in de artt. 14 tot en met 19 Wpolr. Kort gezegd bracht dit met zich mee dat gegevens uit het register zware-criminaliteit verstrekt mochten worden aan:²⁹⁴

- ambtenaren van politie, voor zover zij de gegevens nodig hadden voor de vervulling van hun taak (art. 14 onder a Wpolr);
- ambtenaren van de Koninklijke marechaussee (art. 14 onder b Wpolr);
- opsporingsambtenaren, voor zover aangewezen (art. 14 onder c en d Wpolr);
- bij AMvB aan te wijzen ambtenaren ter signalering van personen (art. 14 onder e Wpolr);
- leden van het openbaar ministerie, voor zover zij de gegevens nodig hebben voor hun taak (art. 15, lid 1 onder a Wpolr);
- de burgemeester, voor zover hij deze behoeft in verband met zijn gezag en zeggenschap over de politie en de handhaving van de openbare orde (art. 15 onder b Wpolr);
- in bepaalde gevallen de korpschef van een regionaal politiekorps en de commandant van de Koninklijke marechaussee (art. 15 onder c en d Wpolr);
- ambtenaren van bureau BIBOB, voor zover nodig voor hun taak (art. 15 onder e Wpolr);
- de minister van Justitie, voor zover nodig voor de afgifte van verklaringen omtrent het gedrag en antecedentenonderzoek²⁹⁵ (art. 15 onder f Wpolr, respectievelijk art. 16 lid 1 onder a Wpolr);
- Nederlandse rechterlijke ambtenaren, met rechtspraak belast, voor zover zij deze behoeven voor de uitoefening van hun taak (art. 16, lid 1 onder b Wpolr);
- reclasseringsmedewerkers en ambtenaren van de kinderbescherming voor zover zij deze behoeven voor hun taak (art. 16, lid 1 onder c Wpolr);
- benadeelden (uitsluitend antecedenten) van strafbare feiten, voor zover zij deze behoeven om in rechte voor hun belangen op te kunnen komen (art. 16, lid 2 Wpolr).

Art. 18 Wpolr opende een aantal mogelijkheden om bij het Bpolr te bepalen

²⁹³ Zie subsectie 4.5.1 voor een beschrijving van de verschillende categorieën.

²⁹⁴ Hier zijn niet alle ontvangstgerechtigden genoemd, maar uitsluitend diegenen, die voor de politiepraktijk van belang zijn.

²⁹⁵ Het begrip antecedent is nader uitgewerkt in art. 2 Besluit politieregisters.

dat aan andere instanties en/of personen gegevens mochten worden verstrekt. Dit betrof paragraaf 5 van het besluit politieregisters. In de artt. 13, 13a, 14, 14a en 15 waren tientallen verstrekkingsgerechtigden opgenomen die werkzaam zijn in de publieke of semi-publieke sector en uit hoofde van hun functie de beschikking over politiegegevens behoeven. Het ging dan om bijvoorbeeld directeuren van penitentiaire inrichtingen (art. 14, lid 1 onder g Wpolr) en de minister van Justitie in het kader van de afgifte van een verklaring van geen bezwaar in verband met de oprichting van een naamloze of besloten vennootschap dan wel de wijziging van de statuten daarvan (art. 14, lid 1 onder l Wpolr).

Voor de verstrekking van gegevens uit het zwacri-register tussen CIE-en onderling is een aparte regeling opgenomen in de CIE-regeling. Art. 6, lid 2 van die regeling bepaalt dat aan twee medewerkers van een andere CIE rechtstreeks toegang wordt verleend tot het eigen register zware criminaliteit van de CIE. De bepaling vormt daarmee een nadere invulling van de wijze van het verstrekken van gegevens uit het zwacri-register aan ambtenaren van politie (art. 14 onder a Wpolr), zijnde CIE-ers.

In art. 17 Wpolr was voorts bepaald dat in het Bpolr ten aanzien van bepaalde categorieën gegevens de verstrekkingverplichting kon worden beperkt door verstrekking in zijn geheel te weigeren of door verstrekking aan bepaalde personen te weigeren. De in art. 11 Bpolr genoemde gronden waren toepasselijk op ieder politieregister, zo ook op het register zware-criminaliteit. Er werd de beheerder van het register de bevoegdheid gegeven om een verstrekking ingevolge de artt. 14 en 15, lid 1 onder b en c Wpolr te weigeren. Voor de CIE-praktijk had deze bepaling evenwel weinig praktische waarde, aangezien voor het register zware criminaliteit een apart weigeringsregime was opgenomen in art. 13a lid 2 Wpolr. Dat artikel bood de CIE een ruimere afschermingsmogelijkheid van de gegevens dan art. 11 Bpolr. Ten eerste vielen, naast de verstrekkingen op grond van artt. 14 en 15, lid 1 onder b en c Wpolr, ook de gegevens die ingevolge art. 15, lid onder f werden verstrekt onder de werking van die bepaling. Ten tweede was de enige voorwaarde voor een verstrekkingseigening dat de weigering noodzakelijk was voor een goede uitvoering van de politietaak. Koelewijn heeft in zijn onderzoek aan de orde gesteld hoe de 'goede uitvoering van de politietaak' geïnterpreteerd dient te worden.²⁹⁶ Uit zijn analyse blijkt dat deze norm erg ruim werd uitgelegd, wat een ruim bereik van de weigeringsgrond voor de CIE tot gevolg had. Ten derde was de in de Wpolr geboden weigeringsgrond ruimer dan de weigeringsgrond in het Bpolr doordat de CIE ook de mogelijkheid was geboden om gegevens onder voorwaarden te verstrekken. Een en ander brengt met zich mee dat de CIE voor die verstrekkingverzoeken waarop een weigeringsgrond van toepassing was een ruime mogelijkheid heeft om

296 Koelewijn, 2009, p. 148-152.

deze verstrekking te weigeren dan wel onder voorwaarden te laten plaatsvinden.

De beperking van de weigeringsmogelijkheden tot de artt. 14 en 15, lid 1 onder b, c, en f Wpolr bracht vervolgens met zich mee dat kennelijk voor de overige verstrekkingen geen weigeringsbevoegdheid was opgenomen. Dit had tot gevolg dat verzoeken van de in art. 15, lid 1 onder a, d, Wpolr, lid 2 van datzelfde artikel, en art. 16 Wpolr genoemde personen en instanties door de CIE niet geweigerd konden worden of aan beperkende voorwaarden onderworpen konden worden. Het gaat dan vooral om het verstrekken van antecedenten (art. 16 Wpolr), maar ook om bijvoorbeeld het verstrekken van gegevens aan het bureau BIBOB. Dit bracht met zich mee dat een CIE alle beschikbare gegevens op verzoek van bureau BIBOB aan dat bureau moet verstrekken.

Het voorlopig register

De gegevens die waren opgenomen in het voorlopig register waren van gevoelige aard. Het voorlopig register diende immers als voorportaal voor het register zware criminaliteit, omdat de informatie nog niet aan de opnamecriteria voor dat register voldeed. Van de informatie in het voorlopig register staat de juistheid en volledigheid dan ook geenszins vast. Als gevolg hiervan was in de Wpolr bepaald dat deze informatie zeer terughoudend dient te worden verstrekt. In art. 13b lid 2 Wpolr was bepaald dat uit het voorlopig register informatie mag worden verstrekt voor zover dat nodig was voor de vaststelling of de betreffende informatie in aanmerking komt om te worden opgenomen in het register zware criminaliteit. Het ging dan om het zogenaamd 'opwaarderen' van informatie. Daarnaast mocht informatie uit het voorlopig register worden verstrekt indien het daadwerkelijk opgenomen kon worden in een ander politieregister, hetgeen in de praktijk over het algemeen het register zware-criminaliteit was. Dergelijke verstrekkingen konden echter ook worden gedaan ten behoeve van registratie in het MOT-register. In de praktijk werd in geval van opneming in het register zware criminaliteit of in het geval van een verstrekking om dat mogelijk te maken ook wel gesproken over het 'opwaarderen' van informatie.

Omtrent de vraag aan wie de informatie mocht worden verstrekt om deze op te waarderen bepaalde noch de Wpolr noch de Bpolr iets. Indien het nodig was om informatie 'op te waarderen' kon informatie uit het voorlopig register kennelijk worden verstrekt volgens de algemene regels van de Wpolr en dus worden verstrekt aan de verstrekkingsgerechtigden zoals deze hierboven zijn behandeld.

Naast deze operationele vorm van verstrekkingen waren er ook in het kader van controle en toezicht een aantal verstrekkingverplichtingen, zoals aan het Cbp en leden van het openbaar ministerie. Op het mechanisme van controle en toezicht zal in hoofdstuk 6 nader worden ingegaan. Ook kunnen er gegevens worden verstrekt ten behoeve van wetenschappelijk onderzoek.

Het informantenregister

Het moge duidelijk zijn dat gelet op hetgeen in subsectie 4.5.1. is behandeld, de gegevens in het informantenregister van uiterst gevoelige aard waren en met het verstrekken daarvan zeer terughoudend diende te worden omgegaan. In het informantenregister waren immers de bruto-verslagen van de gesprekken met de informant opgeslagen, waarin onder meer de personalia van die informant waren opgenomen. Nu het informantenregister geen wettelijke basis kende, was het modelreglement de enige regeling waarin bepalingen waren opgenomen over het verstrekken van gegevens uit dit register. De bepalingen die daarin waren opgenomen ten aanzien van het verstrekken van gegevens waren evenwel summier. In art. 9 van het modelreglement was bepaald dat uit het register slechts verstrekking kon plaatsvinden in overeenstemming met het doel van het register, dat was omschreven als:

*"[...] informatievoorziening met betrekking tot informantgegevens [...] mogelijk te maken voor zover dit noodzakelijk is voor de verantwoording van de verrichtingen naar aanleiding van de opgenomen gegevens."*²⁹⁷

Het verstrekken van gegevens uit het informantenregister was hiermee beperkt tot het verstrekken ten behoeve van controle en toezicht. Het verstrekken van informatie uit het informantenregister voor operationeel gebruik was uitgesloten. De rechtstreekse toegang tot het register was in art. 11 van het modelreglement dan ook beperkt tot het hoofd van de CIE, zijn plaatsvervanger, en de CIE-coördinatoren.²⁹⁸

4.7.2. De knelpunten beschreven

In de gegevensverstrekking door de CIE maken we onderscheid tussen (1) interne verstrekkingen, (2) horizontale verstrekkingen, en (3) verticale verstrekkingen. Interne verstrekkingen betreffen de verstrekkingen die binnen een eigen CIE plaatsvinden, horizontale verstrekkingen betreffen de verstrekkingen tussen CIE-en onderling, en verticale verstrekkingen betreffen de verstrekkingen van een CIE naar een persoon of instantie anders dan een (onderdeel van een) CIE. We behandelen deze vormen van verstrekkingen en de knelpunten die daarbij in de praktijk worden geconstateerd hieronder.

(1) Interne verstrekkingen

In de verstrekkingen binnen de eigen CIE gold het uitgangspunt dat medewerkers van de CIE gegevens verstrekt konden krijgen indien zij deze behoefden voor de goede uitvoering van hun taak. De enige beperking die daarop gold waren de gegevens die in het informantenregister waren opge-

²⁹⁷ Art. 2 modelreglement informantenregister.

²⁹⁸ Zie voor een beschrijving van de organisatorische samenstelling van de CIE op regionaal niveau subsectie 2.4.2.

nomen, waar volgens het in het modelreglement bepaalde alleen het hoofd van de CIE, de coördinatoren en de beheerder toegang toe hadden. In de praktijk bleken echter CIE-runners voor een groot deel toegang te hebben tot het informantenregister, in ieder geval tot hun eigen bruto-verslagen. Deze bruto-verslagen werden onder meer gebruikt in de voorbereiding van een gesprek met een informant.²⁹⁹ De verslagen dienden feitelijk als het geheugen van de runner in de contacten die hij met de informant had. Het knelpunt is de beperkte toegang die in het modelreglement was voorgeschreven. Deze werd in de praktijk als onwerkbaar beschouwd.³⁰⁰

(2) Horizontale verstrekkingen

Het verstrekken van informatie tussen CIE-en onderling werd gekenmerkt door een sterke regiocultuur. Dit betekende dat iedere regionale CIE eigen registers beheerde en bepaalde welke informatie zij uit die registers verstreekte. CIE-en benaderden elkaar via de telefoon, fax of e-mail met informatieverzoeken. Ook kwam het voor dat een lid van de CIE van regio A een dag bij regio B op bezoek ging om het register te doorzoeken naar relevante informatie, die na overleg met het betreffende CIE-hoofd, kon worden verstrekt. De verstrekking van informatie tussen CIE-en onderling vond in beginsel plaats via een zogenaamd 4x4-tje. Een papier met standaardvelden die met informatie gevuld kunnen worden.

Onderlinge automatische gegevensuitwisseling vond plaats, zij het dat de handmatige wijze van gegevensverstrekking nog altijd de boventoon voerde. Dit vindt zijn oorzaak in de verschillende ict-systemen.³⁰¹ Er waren in de praktijk een aantal systemen ontwikkeld die automatisch gegevens vergeleken tussen onder meer de CIE-en. Deze systemen zullen in de navolgende secties worden behandeld, aangezien die wettelijk gezien onder het regime van het 'koppelen' en 'analyseren' vallen.

De wijze waarop elektronisch vorm wordt gegeven aan het voorschrift uit de CIE-regeling dat twee CIE-ers uit een andere regio rechtstreeks toegang krijgen tot het zwacri-register gebeurde door middel van het PZU-systeem (Platform Zwacri Uitwisseling). Ten tijde van het onderzoek waren echter slechts 18 van de 25 regio's op het systeem aangesloten, zodat raadpleging ervan geen volledig beeld van de aanwezige informatie gaf en nog deels handmatig moest worden gedaan. Bovendien gaf het PZU-systeem geen volledige toegang tot het zwacri-register.³⁰² Voor een volledig beeld van de bij een regio aanwezige informatie moest dus alsnog worden teruggегреpen naar de handmatige verstrekking. Daarnaast gaven een aantal regio's aan dat bij het handmatig verstrekken van gegevens, indien nodig, overleg kon worden gevoerd over een eventuele voorwaarde waaronder gegevens konden

299 Schreuders e.a., 2005, p. 104.

300 *Idem.*

301 Rietveld, Slump en Beerepoot, 2004, p. 40.

302 Zie voor een beschrijving van de verschillende wijzen van elektronische informatie-uitwisseling, Koelewijn, 2009, p. 111.

worden verstrekt. Ten slotte werd ten aanzien van het PZU-systeem opgemerkt dat het systeem traag werkte doordat het systeem zwaar beveiligd was.

Zoals in subsectie 4.7.1 is behandeld golden er weinig wettelijke beperkingen voor de horizontale verstrekkingen. De wetgever stond immers in de horizontale verhouding een *free flow* van informatie voor. De praktijk liet echter een heel ander beeld zien. Het knelpunt was de praktijk, die botste namelijk met het wettelijke regime uit de Wpolr doordat het de *free flow* in de weg stond. Vanuit de praktijk werd aangegeven dat de regionale CIE vanwege de in hoofdstuk 2 behandelde afbreukrisico's zicht wilde houden op 'haar' informatie, zodat een ongehinderde toegang tot alle informatie onwenselijk was. De praktijk stond daarmee dan weliswaar de *free flow* van informatie in de weg, maar dat was volgens de CIE-en – beschreven in wettelijke termen – noodzakelijk voor de goede uitvoering van hun taak. Deze geconstrueerde noodzaak vormde daarmee een invulling van de wettelijke grond voor weigering van informatieverzoeken. Hier wreekt zich opnieuw het gebrek dat geen invulling is gegeven aan het noodzakelijkheids criterium. Doordat deze ontbreekt heeft de praktijk de vrijheid om deze op een dusdanige manier in te vullen dat daarmee afbreuk wordt gedaan aan de voorgestane *free flow* van informatie.

(3) Verticale verstrekkingen

Verstrekkingen van de CIE aan een andere instantie of persoon was een vorm van verstrekken die in de praktijk tot meer problemen leidde dan de andere twee typen van verstrekkingen. We maken in de behandeling van deze vorm van verstrekkingen onderscheid tussen verstrekkingen binnen de politie-organisatie en verstrekkingen naar organisaties en personen buiten de organisatie. Bij beide soorten verstrekkingen kwam één gemeenschappelijk knelpunt naar voren en dat is de gedetailleerdheid van het wettelijk systeem van ontvangstgerechtigden. Zoals in subsectie 4.7.1 is uiteengezet, is er sprake van een gesloten verstrekkingssysteem wat tot gevolg had dat in de wet niet alleen uitgebreid was beschreven wie gerechtigd is informatie te ontvangen, maar ook voor de uitvoering van welke specifieke taak zij die informatie mochten ontvangen. In de praktijk bleek dit wettelijk systeem voor de CIE-ers die ermee moesten werken moeilijk te doorgronden. Slechts enkelen binnen de CIE waren dan ook op hoofdlijnen bekend met het wettelijke regime. Voor degenen die het benodigde kennisniveau wel hadden bleek het vervolgens lastig het benodigde kennisniveau te behouden.³⁰³ Uit eerder onderzoek was al gebleken dat de kennis van deze regelgeving bij veel politieambtenaren niet of onvoldoende aanwezig is.³⁰⁴ Dit probleem trad zelfs in die mate op dat soms ten onrechte informatieverstrekkingen

303 Schreuders e.a., 2005, p. 125.

304 Cozijn 1996, p. 7.

werden geweigerd in de veronderstelling dat het verstrekken in strijd met de wet zou zijn.³⁰⁵

Daarnaast was vanuit de praktijk aangegeven dat het verstrekkingssysteem statisch was. Er bestond de behoefte om in bepaalde gevallen informatie uit te wisselen met instanties of personen die niet in de lijst van ontvangstgerechtigden waren opgenomen. Binnen het verstrekkingssysteem onder de Wpolr bestond daarvoor echter geen ruimte.

4.7.3 Uitwerking onder de Wpolg

Onder de Wpolg wordt onderscheid gemaakt tussen het 'ter beschikking stellen' van gegevens en het 'verstrekken' ervan. Kort gezegd komt het onderscheid erop neer dat ambtenaren die zelf toegang hebben tot een bepaalde gegevensverzameling (en deze dus vanaf hun werkplek zelf kunnen benaderen) deze gegevens wettelijk gezien ter beschikking gesteld krijgen. Op het moment dat zij deze autorisatie niet hebben, maar gegevens via een andere ambtenaar kunnen opvragen, dan spreekt de Wpolg over het verstrekken van gegevens.

Oude knelpunten aangepakt

Hieronder zullen wij de wijze beschrijven waarop de Wpolg de oude knelpunten heeft aangepakt. Evenals in de vorige sectie doen we dat aan de hand van (1) interne verstrekkingen, (2) horizontale verstrekkingen en (3) verticale verstrekkingen.

(1) Interne verstrekkingen

Gegevens worden ter beschikking gesteld aan ambtenaren van de politie die geautoriseerd zijn voor het verwerken van politiegegevens door de korpschef voor zover deze ambtenaren de gegevens behoeven voor de goede uitvoering van hun taak.³⁰⁶ Voor de gegevensverwerking als bedoeld in art. 10 Wpolg, de gegevensverwerking die overeenkomt met de gegevens die onder de Wpolr in het register zware criminaliteit werden opgeslagen, kunnen blijkens art. 2:5 Bpolg de medewerkers van de CIE worden geautoriseerd. Blijkens art. 2:3 Bpolg worden CIE-ers ook geautoriseerd voor de verwerking van gegevens omtrent informanten, het informantenregister. De beperking van deze toegang tot de leidinggevenden van de CIE, zoals onder de Wpolr, wordt hier dus losgelaten.

(2) Horizontale verstrekkingen

Wat betreft het verstrekken van zwacri-gegevens gebeurt dit onder de Wpolg op grond van de terbeschikkingstelling-bepaling, zowel binnen de eigen

³⁰⁵ Rozenbeek 2003, p. 28-29.

³⁰⁶ Art. 15 lid 1 jo. Art. 6 jo. Art. 1 onder f Wpolg.

CIE als met andere CIE-en. Gelet op de bewoordingen ('de verantwoordelijke stelt (...) ter beschikking (...)') gaat het hier om een verplichting voor de verantwoordelijke. Ook onder de Wpolg kunnen deze 'verstrekkingen' echter geweigerd worden indien dit noodzakelijk is voor de goede uitvoering van de politietaak. In plaats van een verstrekkingenweigeringsmogelijkheid kan in zo een geval ook 'ter beschikking worden gesteld onder voorwaarden'. In art. 2:13 Bpolr is uitgewerkt dat de terbeschikkingstelling van gegevens *alleen* kan worden geweigerd of aan voorwaarden worden verbonden in het geval – voor zover relevant voor de CIE – (a) het gegevens betreft omtrent informanten (onder de Wpolr het informantenregister), (b) gevaar voor het leven of gezondheid van betrokkenen of derden is te duchten, of (c) het gaat om de eerder genoemde themaverwerkingen. Dit brengt met zich mee dat onder de Wpolg de terbeschikkingstelling van zwacri-gegevens niet kan worden geweigerd aan een andere CIE, hetgeen een aanzienlijke beperking betreft van de weigeringsmogelijkheden onder de Wpolr.

(3) Verticale verstrekkingen

De wetgever stelt dat voor zover ambtenaren van politie niet geautoriseerd zijn voor bepaalde gegevens, maar die gegevens wel op incidentele basis nodig hebben voor de uitvoering van hun taak, de korpsbeheerder deze gegevens op basis van art. 15 lid 1 aan hen ter beschikking moet stellen.³⁰⁷ Het gaat dus om een tijdelijke autorisatie voor een specifiek bepaalde verzameling gegevens. In het geval van verticale verstrekkingen door de CIE aan politieambtenaren van tactische teams, die niet tot het zwacri-gedeelte geautoriseerd zullen zijn, betekent dit dat deze gegevens aan hen ter beschikking zullen worden gesteld op grond van art. 15 lid 1, waarop ook de weigeringsmogelijkheid van lid 2 van toepassing is. Zoals gezien is deze weigeringsmogelijkheid in het Bpolr echter beperkt tot slechts een gedeelte van de gegevens die door de CIE worden verwerkt. De gegevens die daar niet onder vallen dienen dus ook voor het operationele gebruik aan de betreffende ambtenaar van politie ter beschikking te worden gesteld, zonder dat daarbij een beroep kan worden gedaan op de weigeringsgrond.

Naast de terbeschikkingstelling van gegevens aan politieambtenaren die reeds geautoriseerd zijn tot het verwerken van politiegegevens geeft de Wpolg in art. 16 de korpschef de verplichting om politiegegevens te verstrekken aan buitengewone opsporingsambtenaren, leden van het openbaar ministerie, burgemeesters en aan de bevoegde persoon in verband met de afhandeling van klachten en disciplinaire maatregelen. In lid 2 van art. 16 wordt de weigeringsmogelijkheid van het tweede lid van art. 15 van overeenkomstige toepassing verklaard op verstrekkingen aan buitengewone opsporingsambtenaren en de verstrekking in verband met de afhandeling van klachten of disciplinaire maatregelen, zodat ook hier verstrekkingen slechts in bepaalde gevallen kunnen worden geweigerd.

307 Kamerstukken II, 2005/06, 30 327 nr. 3, p. 34.

In art. 18 Wpolg is de mogelijkheid opgenomen om gegevens aan derden, die in het Bpolg zijn aangewezen, te verstrekken indien er sprake is van een zwaarwegend algemeen belang. Blijkens artt. 4:3 en 4:4 Bpolg komt deze lijst van instanties en personen voor een groot deel overeen met de personen en instanties die onder Wpolr ook als ontvangstgerechtigd waren aangewezen.

In het tweede lid van art. 18 Wpolg is bepaald dat in bijzondere gevallen de minister van Justitie of de minister van Binnenlandse Zaken toestemming of opdracht kan geven tot het verstrekken van gegevens. Het onder de Wpolr geldende criterium van een openbare taak is komen te vervallen, zodat ook aan particuliere instanties gegevens kunnen worden verstrekt indien er sprake is van een zwaarwegend algemeen belang. Wat betreft de invulling van het begrip zwaarwegend algemeen belang wordt verwezen naar het verslag inzake de wijziging van de Wet justitiële gegevens.³⁰⁸ Onder het zwaarwegend belang dient blijkens dat verslag te worden verstaan het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van een land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of de bescherming van de rechten en vrijheden van anderen. Het bereik van het 'zwaarwegend algemeen belang' is daarmee beperkter dan het 'gerechtvaardigd belang'³⁰⁹, zodat een gegevensverwerking van meer dan gewone betekenis moet zijn om aan dat criterium te voldoen, aldus de wetgever.³¹⁰

Blijkens de in art. 18 Wpolg gebezigde woorden 'kunnen worden verstrekt' is er geen verplichting tot verstrekking van gegevens aan de in die artikelen genoemde instanties, maar zal steeds een belangenafweging moeten worden gemaakt of er in het geval van een verzoek sprake is van een voldoende zwaarwegend algemeen belang, afgewogen tegen de persoonlijke levenssfeer van diegene wie de gegevens betreft.³¹¹ Het in art. 18 Wpolg bepaalde betreft een algemene bepaling. De wetgever heeft overwogen dat, in tegenstelling tot de Wpolr, geen specifieke regeling voor de verwerking van de zwacri-gegevens nodig is. Anders dan ten aanzien van de terbeschikkingstellingen en verstrekkingen op grond van de artt. 15 en 16 Wpolg is er geen aparte bepaling opgenomen op grond waarvan de CIE een verstrekking op grond van art. 18 Wpolg kan weigeren. Noch in de Wpolg noch in het Bpolg is dan ook aandacht besteed aan de mogelijkheid van CIE-en om bij een dergelijk verstrekingsverzoek een belangenafweging te maken waarbij het eigen belang van de CIE-en voor het afschermen van hun informatie kan worden betrokken.

Voorts is in de artt. 19 en 20 Wpolg een regeling gegeven voor de incidentele respectievelijk structurele verstrekking van politiegegevens aan derden. Ook in dat geval moet er sprake zijn van een zwaarwegend algemeen belang en

308 *Kamerstukken II*, 2005/06, 30 327, nr. 3, p. 74.

309 Zoals gebruikt in art. 23 onder e Wbp.

310 *Kamerstukken II*, 2003/04, 28 886, nr. 5, p. 2.

311 *Kamerstukken II*, 2005/06, 30 327, nr. 3, p. 75.

moet de verstrekking tot doel hebben (a) het voorkomen en opsporen van strafbare feiten, (b) het handhaven van de openbare orde, (c) het verlenen van hulp aan hen die deze behoeven, of (d) het uitoefenen van toezicht op het naleven van regelgeving. In het geval van de CIE kan de korpschef, als verantwoordelijke, beslissen tot het verstrekken van politiegegevens, waarbij hij in het geval van een structurele verstrekking de formaliteiten van art. 20, lid 2 Wpolg in acht dient te nemen. De grootste beperking van de toepassing van de artt. 19 en 20 Wpolg is echter gelegen in art. 4:5 van het Bpolg, waarin is bepaald dat in beginsel geen CIE-gegevens worden verstrekt op grond van de artt. 19 en 20 Wpolg. Slechts indien dit 'dringend noodzakelijk' is voor een goede uitvoering van de politietaak kan de korpschef, enkel na overleg met het hoofd CIE, CIE-gegevens (met uitzondering van themaverwerkingen) aan derden verstrekken. Wat met dringend noodzakelijk wordt bedoeld is niet nader uitgewerkt, maar lijkt – gelet op de verhouding tussen lid 2 en lid 1 van het artikel – een zwaardere toets te zijn dan het 'zwaarwegend algemeen belang'.

Nieuwe knelpunten geïntroduceerd

Wat het verstrekken van gegevens betreft is opvallend dat onder het regime van de Wpolg geen nieuwe knelpunten geïntroduceerd lijken te zijn.

4.7.4 Tussenconclusie aangaande het verstrekken

Alvorens we onze tussenconclusie aangaande het verstrekken formuleren geven we schematisch weer (a) het aantal onder de Wpolr geconstateerde knelpunten, (b) de inhoud van die knelpunten, (c) de uitwerking daarvan onder de Wpolg en (d) de (te verwachten) resultaten van de uitwerking onder de Wpolg (zie figuur 4.4).

Aantal	Knelpunten Wpolr	Wpolg	Resultaat
1	Interne verstrekkingen Beperkte toegang tot informantenregister	Ruimere toegang mogelijk	Knelpunt opgelost
2	Horizontale verstrekkingen a. vaag noodzakelijkheids- criterium b. beperkte <i>free flow</i>	a. begrip behouden, nader uitgewerkt in besluit b. <i>free flow</i> afgedwongen	Knelpunt opgelost, wettelijk uitgangspunt botst echter met cultuur; vraagt meer van controle en toezicht.
3	Verticale verstrekkingen a. moeilijk toepasbaar regime b. statische verstrekking- mogelijkheden	a. regime blijft lastig b. wordt dynamisch	a. knelpunt niet opgelost b. knelpunt opgelost, zwaartepunt verschuift naar controle en toezicht

Figuur 4.4 Schematisch weergave knelpunt 'verstrekken'.

Wat het verstrekken van politiegegevens door de CIE betreft, is in subsectie 4.7.2 geconstateerd dat onder de Wpolr de beperkte toegang tot informantenregisters als onwerkbaar werd beschouwd. De CIE-ers konden na verloop van tijd niet meer het door henzelf opgestelde brutoverslag raadplegen. Dit knelpunt is onder de Wpolg opgelost, door de bepalingen omtrent de autorisaties tot de verwerking van informantgegevens ruimer vast te stellen dan in het modelreglement informantenregister het geval was.

Een tweede geconstateerd knelpunt betreft de onder de CIE aanwezige sterke regiocultuur. Deze werd onder de Wpolr gefaciliteerd door de normering te baseren op het registerbegrip. Onder de Wpolg is het registerbegrip losgelaten en wordt de toegang tot de zware-criminaliteitsgegevens gebaseerd op autorisaties. Zoals de wetgever echter zelf in de memorie van toelichting naar voren brengt, is dat nieuwe systeem toegeschreven op een nieuw informatiesysteem dat bij de politie zal worden uitgerold. Dat nieuwe informatiesysteem, PSO2 (Police Suite Opsporing 2), is er echter nooit in zijn oorspronkelijke vorm gekomen. Uit het onderzoek van Koelewijn blijkt dat standarisatie van de ICT-systemen binnen de politie al jaren een knelpunt is.³¹² Daarmee ziet de politie zich geconfronteerd met nieuwe wetgeving, maar oude systemen. Dit brengt met zich mee dat de doorbreking van regionaal georganiseerde informatiehuishouding weliswaar wettelijk opgelost lijkt te zijn, maar praktisch gezien nog bestaat. Daarenboven is het sterk de vraag of de wettelijke oplossing in de vorm van autorisaties ook zal passen op de systemen die in de toekomst zullen worden ontwikkeld. Vooralsnog zullen de registers behouden blijven en zullen de wettelijke autorisaties sterk overeenkomen met de vroegere toegang tot een specifiek register.

Voorts is ook onder de nieuwe wetgeving geen nadere invulling gegeven aan de verplichting voor iedere regio om twee CIE-ers van andere regio's voor hun systemen te autoriseren. Dat is aan de ene kant begrijpelijk aangezien de regel aan duidelijkheid niet te wensen overlaat. Aan de andere kant blijkt dat dit in de praktijk nog niet altijd is gebeurd ondanks dat de regel al sinds de invoering van de Regeling Criminele Inlichtingen Eenheid in 2000 bestond. De wetgever had een sterker signaal over de noodzakelijkheid van deze toegang af kunnen geven door deze toegangsverplichting in de Wet politiegegevens zelf neer te leggen en mogelijk zelfs te sanctioneren.

Free flow of information

Onder het oude regime van de Wpolr werd de *free flow of information* ten onrechte door de politiepraktijk beperkt. Onder de Wpolg wordt de *free flow* afgedwongen doordat er simpelweg geen wettelijke mogelijkheid tot weigering meer is. Daarmee geeft de wetgever te kennen dat de wijze waarop door de praktijk invulling was gegeven aan de weigeringsgrond – de goede uitvoering van de politietaak – te ruim was.

312 Koelewijn, 2009, p, 115-129.

De weigeringsgrond is echter niet helemaal verdwenen. Zeker voor de CIE is er een aanzienlijke hoeveelheid informatie waarvan de verstrekking aan anderen geweigerd kan worden. Daarbij wordt ook onder de nieuwe wetgeving aansluiting gezocht bij het criterium van de 'goede uitvoering van de politietaak'. Gelet op de kennelijk te ruime uitleg van die weigeringsgrond in de praktijk, zoals we hiervoor zagen, rijst daarmee wel de vraag op welke wijze de praktijk aan deze weigeringsgrond invulling dient te geven. De wetgever heeft in het besluit aangegeven in welke gevallen geweigerd kan worden. Ook op die manier dwingt zij de *free flow* van informatie af. Wijziging van de wetgeving verandert de beschreven terughoudende cultuur bij de CIE echter niet, zodat het de vraag is of de CIE zich bij weigering aan de genoemde beperkingen zal houden. Het afdwingen van verstrekking heeft het gevaar in zich dat de CIE, als gevolg van de afschermingsbelangen, andere manieren gaat zoeken om informatie alsnog af te schermen. Daarbij kan gedacht worden aan het voeren van alleen de informantenverwerking (art. 11, welke een ruimere weigeringsmogelijkheid kent dan art. 10) en op die grond weigeren, terwijl feitelijk sprake is van een zwacri-verwerking (art. 10) die niet geweigerd zou kunnen worden. Strikt toezicht op deze gang van zaken is om die reden naar onze mening noodzakelijk.

Lastig regime

Vanwege de gedetailleerdheid van het verstrekkingssysteem blijft ook onder de Wpolg het verstrekkingssysteem voor de politiepraktijk moeilijk toepasbaar. Er is nog steeds een uitgebreide lijst met verstrekkingsgerechtigden die zijn gekoppeld aan een specifiek doel waarvoor verstrekt mag worden. Daarnaast is er een verschil tussen het ter beschikking stellen en het verstrekken. Tevens is de weigeringsmogelijkheid op deelgebieden blijven bestaan, waarbij niet altijd is voorzien in een (adequate) uitleg over het toepassingsbereik van die weigeringsmogelijkheid.

Van statisch naar dynamisch verstrekken

Met de gedetailleerde regeling voor verstrekkingen aan derden komt de Wpolg tegemoet aan het knelpunt dat het verstrekkingssysteem te statisch was. Er is een ruime mogelijkheid tot het verstrekken aan derden opgenomen. De groep van derden – de ontvangstgerechtigden van politieinformatie – zijn niet limitatief in de wet of het besluit gedefinieerd. Dat is aan de politiepraktijk en haar gezagdragers (ovj en burgemeester) overgelaten. De Wpolg geeft aan hen een discretionaire bevoegdheid om te bepalen wanneer verstrekken aan derden aan de orde is. Daarmee krijgt het verstrekkingssysteem een meer dynamisch karakter, namelijk het karakter dat de praktijk wenst. Het statische karakter van de verstrekkingssysteem onder de Wpolr is daarmee verdwenen. De wet en de toelichting daarop voorzien daarbij echter op summere wijze in voorbeelden en een toelichting op situaties waarin een dergelijke verstrekking toegestaan is. De verschuiving van een strikt wettelijk regime naar een meer open regime waarbij de beslissing wordt gedelegeerd aan de ovj of burgemeester, brengt vanuit het oogpunt van het gegevens-

beschermingsrecht wel met zich mee dat scherpere eisen moeten worden gesteld aan de controle en het toezicht op de wijze waarop die gezagsdragers hun taak vervullen.

4.8 KOPPELEN

Verskillende gegevensverwerkingen kunnen met elkaar worden gekoppeld. In deze sectie voeren we de driestappenbehandeling³¹³ uit op het werkingselement 'koppelen'. We maken, anders dan de wetgever ten tijde van de totstandkoming van de Wpolr, een onderscheid tussen koppelen en analyseren. Onder koppelen verstaan we het samensmelten van meerdere bestanden tot één bestand met als doel om de daartussen bestaande overeenkomsten in de aanwezige informatie zichtbaar te maken. Het gaat er om een vergelijking van de aanwezige informatie op zogenaamde 'hits' te genereren. Onder analyseren verstaan we het doorzoeken van een of meerdere bestanden met technieken die meer omvatten dan een één-op-één-vergelijking van gegevens. We behandelen de activiteit analyseren in sectie 4.9.

In subsectie 4.8.1 bespreken we de theorie van het koppelen onder de Wpolr. In subsectie 4.8.2 bespreken we de daarbij in de praktijk geconstateerde knelpunten. Voorts behandelen we in subsectie 4.8.3 op welke wijze de Wpolg aan de met betrekking tot het koppelen van gegevens geconstateerde knelpunten tegemoet komt. Uiteindelijk formuleren we in subsectie 4.8.4 onze tussenconclusie.

4.8.1 Theoretisch kader

Het koppelen van gegevensbestanden was in art. 1, lid 1 onder d Wpolr gedefinieerd als:

"het treffen van technische of organisatorische voorzieningen, waardoor verschillende verzamelingen van persoonsgegevens systematisch met elkaar kunnen worden vergeleken"

Blijkens de memorie van toelichting was slechts sprake van koppelen indien daarmee:

*"nieuwe informatie wordt verkregen over een in beginsel onbepaalde groep van personen, welke informatie niet kan worden ontleend aan één van de betrokken registers afzonderlijk."*³¹⁴

Art. 6 Wpolr bepaalde vervolgens dat een politieregister slechts met een ander politieregister kon worden gekoppeld indien dit noodzakelijk was

313 Zoals beschreven in sectie 4.4.

314 *Kamerstukken II*, 1985/86, 19 589, nr. 3, p. 16.

voor de goede uitvoering van de politietaak en in overeenstemming met het in het Bpolr bepaalde. In het Bpolr was in art. 4 bepaald dat de koppeling van een politieregister slechts was toegestaan met een ander politieregister of met een bestand van het Rijk, provincies, gemeenten en andere openbare lichamen. Daarnaast bepaalde art. 5 van het Bpolr dat van een koppeling proces-verbaal werd opgemaakt waarin zo nauwkeurig mogelijk diende te worden vermeld: (a) het doel van de koppeling, (b) de datum van koppeling, (c) degene in wiens opdracht de koppeling plaatsvond, (d) de bestanden die werden gekoppeld, alsmede de naam van de beheerder of de houder van die bestanden, (e) of de koppeling heeft geleid tot nieuwe persoonsgegevens en zo ja, welke, (f) of de gegevens, bedoeld onder (e) zijn opgenomen in een register en zo ja, in welk, en (g) eventuele bijzonderheden. In het registerreglement kon van deze voorschriften worden afgeweken. Als er evenwel een proces-verbaal werd opgesteld dan diende dit twee jaar te worden bewaard.

De normering van het koppelen van registers werd daarmee bepaald door 'de goede uitvoering van de politietaak'. De overige voorschriften betroffen vormvoorschriften en zien niet op de inhoudelijk besluitvorming of tot het koppelen van registers kon worden overgegaan. Bovendien kon ingevolge art. 6 lid 4 Wpolr worden afgeweken van hetgeen in het Bpolr en het betreffende modelreglement was voorgesteld in het geval dat dit noodzakelijk was voor de opsporing van een misdrijf waardoor de rechtsorde ernstig geschokt was.

Art. 17 van het modelreglement register zware criminaliteit bepaalde ten aanzien van een koppeling van het zwacri-register met een ander register dat de koppeling slechts kon plaatsvinden voor zover deze koppeling noodzakelijk was voor het voorkomen en opsporen van misdrijven die een ernstige inbreuk op de rechtsorde opleveren. Daarmee was de norm om tot koppelen van een zwacri-register met een ander register over te gaan in beginsel zwaarder dan de algemene regeling uit art. 6 Wpolr waar immers slechts de goede uitvoering van de politietaak gediend moest zijn met een koppeling. Net als de 'goede uitvoering van de politietaak' was ook het criterium de 'ernstige inbreuk op de rechtsorde' door de wetgever niet nader uitgewerkt. Wel kon aansluiting gezocht worden bij hetgeen in art. 132a Sv is bepaald, waar de 'ernstige inbreuk op de rechtsorde' ziet op zwaardere delicten zoals moord, wapenhandel, handel in drugs, omvangrijke milieudelicten en fraude.³¹⁵

Ten aanzien van het voorlopig register was in art. 14 van het modelreglement voorlopig register bepaald dat koppeling van dit register met een ander *bijzonder* register plaats kon vinden indien dit noodzakelijk was voor het doel van het voorlopig register zelf; het opwaarderen van de in het voorlopig register opgenomen informatie. Van een koppeling diende, blijkens het tweede lid, een proces-verbaal te worden opgemaakt, tenzij het een koppeling betrof in het kader van een misdaadanalyse.³¹⁶

315 Zie <<http://archieff.om.nl/bob/docs/11.htm>>.

316 Art. 14 lid 2 respectievelijk lid 3 Modelreglement voorlopig register.

In het modelreglement van het informantenregister was geen bepaling opgenomen over het koppelen van gegevens. Gelet op de bijzondere inhoud van het register is dat ook logisch. Wel was in art. 9 van het modelreglement informantenregister, net zoals in art. 15 van het modelreglement voorlopig register, bepaald dat de aan een informant toegekende ICS-code stelselmatig werd verstrekt aan de NCIE.

4.8.2 De knelpunten beschreven

In de praktijk van de CIE leken zich weinig knelpunten voor te doen met betrekking tot het koppelen van registers en de daarop van toepassing zijnde wettelijke regeling. Dit leek vooral zijn oorzaak te vinden in de summiere regeling die ten aanzien van het koppelen was opgenomen in de Wpolr.

Ten eerste stelde de Wpolr weinig inhoudelijke eisen aan het koppelen van registers. Voor een koppeling van het register zware criminaliteit moest er sprake zijn van een noodzaak om misdrijven, die een ernstige inbreuk op de rechtsorde zijn, te voorkomen en op te sporen. Blijkens de opnamecriteria voor het register zware criminaliteit³¹⁷ gold voor alle opgenomen gegevens dat deze betrekking moesten hebben op misdrijven die een ernstige inbreuk op de rechtsorde opleverden³¹⁸. Voor het koppelen van CIE gegevens bleef derhalve uitsluitend de eis over dat de koppeling noodzakelijk moest zijn om dergelijke misdrijven te voorkomen of op te sporen. We hebben reeds gezien dat dit begrip, zonder nadere specificatie, tot toepassingsproblemen heeft geleid. Gelet op de taak van de CIE (kort gezegd informatievoorziening aangaande zware criminaliteit) is het echter de vraag wanneer een koppeling om nieuwe of aanvullende informatie te verkrijgen niet noodzakelijk zou zijn. De in het register opgeslagen informatie voldoet reeds aan deze noodzakelijkheidseis (anders zou zij, theoretisch gezien, verwijderd moeten worden). Voorts zal de koppeling slechts uitgevoerd worden om nieuwe informatie te verkrijgen of informatie te verduidelijken. De noodzaak tot koppelen ligt feitelijk dus reeds in de taak van de CIE besloten. Met het opslaan van informatie in het register zware criminaliteit is koppeling daarvan ook toegestaan.

Indien de koppeling was toegestaan, normeerde de Wpolr de wijze van koppelen niet, zodat de CIE de vrije hand had in de toepassing van verschillende technieken. Sietsma concludeerde in dit verband dat de Wpolr te weinig regels bevatte voor de wijze waarop gegevens tijdens een koppeling verwerkt mochten worden.³¹⁹

317 Zie voor een uitgebreide behandeling van deze criteria subsectie 4.5.1.

318 Strikt genomen geldt deze eis niet voor de gegevens genoemd onder categorie 2, nu daar alleen wordt gesproken over misdrijven waarop 8 jaar of meer gevangenisstraf is gesteld. Gelet op de ernst van die misdrijven betreft het evenwel misdrijven die een ernstige inbreuk maken op de rechtsorde.

319 Sietsma, 2006, p. 390.

Ten tweede heeft het koppelen niet tot grote knelpunten binnen de CIE geleid omdat het koppelen van registers pas de laatste jaren in opkomst is. Door het merendeel van de CIE-en zelf was in 2005 aangegeven dat meer in faciliteiten en kennis diende te worden geïnvesteerd.³²⁰ In plaats van juridische zijn dan ook met name technische en organisatorische obstakels de oorzaak van het weinige koppelen in de praktijk.³²¹ Koelewijn heeft een aantal van de thans bestaande koppelingen uitgebreid beschreven. Het gaat dan wat de CIE betreft met name om het VROS-systeem.³²²

Op basis van bovengenoemde mogen we concluderen dat het enige knelpunt van de Wpolr erin gelegen was dat er weinig normerend effect vanuit ging aangezien het koppelen van verschillende bestanden voor de CIE feitelijk niet werd genormeerd. Als de CIE toegang had tot de betreffende bestanden, kon zij die ook koppelen.

4.8.3 Uitwerking onder de Wpolg

In de memorie van toelichting op de Wpolg is aangegeven dat aan geautomatiseerd vergelijken en het in combinatie zoeken naar politiegegevens strikte voorwaarden dienen te worden verbonden. Daarbij acht de wetgever het van belang dat de politie gegevens verwerkt van verschillende typen betrokkenen (verdachten, betrokkenen, en contacten) en dat diezelfde gegevens naar hun aard verschillende betrouwbaarheidsgraden hebben. Bij iedere verwerking waarbij gegevens geautomatiseerd worden vergeleken of in combinatie met elkaar worden doorzocht, dient de verantwoordelijke een afweging te maken tussen het belang van die verwerking en het belang van de personen van wie de gegevens worden betrokken in het onderzoek, waarbij in ieder geval de beginselen van proportionaliteit en subsidiariteit dienen te worden toegepast.³²³

Gegevens die door de CIE worden verwerkt, vallen onder het verwerkingsregime van art. 10 Wpolg. In art. 11 Wpolg zijn normen opgenomen over de wijze waarop gegevens die onder het verwerkingsregime van art. 10 Wpolg vallen geautomatiseerd mogen worden verwerkt of in combinatie met andere gegevens mogen worden doorzocht. Uit het tweede lid van art. 11 Wpolg volgt dat indien dit noodzakelijk is voor verwerking als bedoeld in art. 10 Wpolg (zwacri-gegevens), deze gegevens kunnen worden verwerkt met gegevens uit art. 8 Wpolg (gegevensverwerking ter uitvoering van de dagelijkse politietaak) en art. 9 Wpolg (gegevensverwerking in verband met een onderzoek in een bepaald geval). De CIE krijgt hiermee de mogelijkheid

320 Schreuders e.a., 2005, p. 81.

321 Koelewijn, 2009, p. 129.

322 Overigens is het de vraag of het VROS-systeem als koppeling dient te worden aangemerkt nu in de vergelijking slechts overeenkomsten worden gezocht op naam, zodat niet gezocht wordt naar een onbepaalde groep.

323 *Kamerstukken II*, 2005/06, 30 327, nr. 3, p. 52.

om de gegevens die zij verwerkt geautomatiseerd te vergelijken met de andere genoemde politiegegevens om zo vast te stellen of daartussen verbanden bestaan. Indien dat het geval is, kunnen de gevonden gegevens, met toestemming van de 'eigenaar', onder het regime van art. 10 verder worden verwerkt. Wat de noodzakelijkheidseis betreft om tot een koppeling over te gaan stelt de wetgever dat die toets beheerst wordt door de eisen van proportionaliteit en subsidiariteit.³²⁴ Daarbij zijn echter geen voorbeelden gegeven van mogelijke situaties die wel of niet onder deze noodzakelijkheidseis vallen.

In art. 2:11 Bpolg zijn bepalingen opgenomen over de wijze waarop de gegevensverwerking dient te worden uitgevoerd. Ten aanzien van de zwacri-gegevens is in art. 2:11 onder b bepaald dat na de geautomatiseerde vergelijking alleen de overeenkomende gegevens zichtbaar zijn en de overige vergeleken gegevens alleen na instemming van het hoofd CIE. Wat de themaverwerkingen betreft is in art. 2:11 onder d bepaald dat ook de overeenkomende gegevens niet zichtbaar worden. De zoekresultaten worden in zo'n geval uitsluitend teruggekoppeld naar de CIE die de gegevens heeft ingebracht.³²⁵ Daarnaast kan het hoofd van de CIE een codering aan de te vergelijken gegevens meegeven, zodat ook de zwacri-gegevens bij het geautomatiseerd vergelijken onder het regime van de themaverwerking vallen.³²⁶

Onder het regime van de Wpolg kunnen, in tegenstelling tot onder de Wpolr, ook informantgegevens geautomatiseerd worden vergeleken met andere politiegegevens. De verwerking mag echter alleen plaatsvinden voor het doel waarvoor de informantgegevens worden gehouden. Dit betreft het beheer van de informantgegevens en gebruik voor betrouwbaarheidsinschatting van de informant, zodat operationele inzet van de resultaten niet is toegestaan.

4.8.4 Tussenconclusie aangaande het koppelen

Alvorens we onze tussenconclusie aangaande het koppelen formuleren, geven we schematisch weer (a) het aantal onder de Wpolr geconstateerde knelpunten, (b) de inhoud van die knelpunten, (c) de uitwerking daarvan onder de Wpolg, en (d) de (te verwachten) resultaten van de uitwerking onder de Wpolg.

Aantal	Knelpunten Wpolr	Wpolg	Resultaat
1	Weinig normerend effect	Koppelen beperkt tot politiegegevens	'Knelpunt' opgelost

Figuur 4.5 Schematische weergave knelpunt 'koppelen'.

324 *Kamerstukken II*, 2005/06, 30 327, nr. 3, p. 52.

325 *Kamerstukken II*, 2005/06, 30 327, nr. 3, p. 54.

326 Zo volgt uit art. 2:12 Bpolg.

Het grootste gebrek onder de Wpolr aangaande het koppelen betrof het gebrek aan een juridisch kader. Dit is vooral te verklaren vanuit de tijd waaruit de Wpolr stamt. Logischerwijs komt de Wpolg dan ook aan tegemoet aan dit knelpunt. Wat het koppelen betreft geeft de Wpolg de CIE-en een uitgebreidere regeling dan de Wpolr. Opvallend is dat daarbij in het Bpolr relatief veel aandacht is besteed aan de manier waarop de koppeling dient te worden uitgevoerd. Of onder de Wpolg tot een gegevensvergelijking mag worden overgegaan, wordt bepaald door de vraag of dit noodzakelijk is voor het doel van de gegevensverwerking onder art. 10 Wpolg. We zagen reeds dat deze eis met de enkele opslag van gegevens in de systemen van de CIE is vervuld (daar geldt al een noodzakelijkheidseis). De memorie van toelichting specificeert de noodzakelijkheidseis echter nader door te stellen dat deze vraag beantwoord wordt door de eisen van proportionaliteit en subsidiariteit. Wij vragen ons echter af of voor die eisen – reeds na de opslag van informatie – nog wel plaats is. De wetgever heeft ook geen voorbeelden gegeven waarbij een koppeling van gegevens niet is toegestaan, terwijl gegevens wel onder de zwacri-verwerking mogen worden verwerkt. Ondanks deze onduidelijkheid in de memorie van toelichting verschilt het normerend kader van de Wpolg op één punt van de Wpolr als het gaat om koppelen. De Wpolg geeft expliciet aan met welke gegevensverzamelingen mag worden gekoppeld, hetgeen onder de Wpolr niet was genormeerd. Daarmee mogen we concluderen dat de Wpolg een strikter kader aangeeft dan de Wpolr. Hierbij tekenen we aan dat ons inziens de verdere eisen praktisch gezien van weinig betekenis zullen blijken te zijn.

4.9 ANALYSEREN

Onder de activiteit ‘analyseren’ verstaan we het toepassen van ICT-technieken op een verzameling gegevens om daaruit nieuwe informatie te vergaren. Zoals in de voorgaande sectie is uiteengezet, gaat het bij het analyseren dus om meer dan een één-op-één vergelijking van gegevens om daaruit overeenkomsten te halen. De reikwijdte van de analyse is daardoor sterk afhankelijk van de toegepaste technieken en de omvang en inhoud van de gegevensverzameling waarop deze technieken worden toegepast.

In subsectie 4.9.1 bespreken we de theorie van het analyseren onder de Wpolr. In subsectie 4.9.2 bespreken we de daarbij in de praktijk geconstateerde knelpunten. Voorts behandelen we in subsectie 4.9.3 op welke wijze de Wpolg tegemoet komt aan de geconstateerde knelpunten met betrekking tot het analyseren van gegevens. Uiteindelijk formuleren we in subsectie 4.9.4 onze tussenconclusie.

4.9.1 Theoretisch kader

Onder de oude Wpolr was geen apart artikel opgenomen dat het analyseren van gegevens reguleerde en normeerde. Enkel het koppelen van gegevens

was genormeerd, zoals we reeds in de vorige sectie beschreven. De Wpolr reguleerde en normeerde dus niet de technieken die bij een dergelijke koppeling konden worden ingezet. Daarmee werd het analyseren van gegevens niet door de Wpolr genormeerd en had de CIE vrij spel. Vanzelfsprekend is dit een gevolg van het feit dat in de tijd dat de Wpolr tot stand kwam de activiteit analyseren, zoals wij deze hier hanteren, nog niet tot ontwikkeling was gebracht als gevolg van de toenmalige technologische stand van zaken.

4.9.2 De knelpunten beschreven

Het uitvoeren van analyses werd door de Wpolr niet gereguleerd, zodat daaruit ook geen knelpunten voortvloeien anders dan het gebrek aan een regeling zelf. Deze constatering zet wat ons betreft vraagtekens bij de rechtmatigheid van de onder de Wpolr uitgevoerde analyses die niet onder het koppelingsbegrip vielen. Daartoe was immers geen bevoegdheid in de Wpolr opgenomen en daarmee kan de vraag worden gesteld of met de uitgevoerde analyses niet een ongerechtvaardigde inbreuk op de vrijheid van gegevens van de burgers is gemaakt.

Wel was het onder de Wpolr onduidelijk gebleven (en eigenlijk is dat op dit moment in retrospectief nog zo) of analyseren toegestaan was en zo ja op welke typen analyses het koppelingsbegrip van de Wpolr betrekking had. Het gaat dan om de reikwijdte van de koppelingsbepaling. Zo is het de vraag of er nog sprake was van het koppelen zoals bedoeld in de Wpolr bij de vergelijking van een gedeelte van het register zware criminaliteit met een gedeelte van een ander register. De normering van een koppeling gaat immers uit van het koppelen van registers. Het modelreglement sprak ook van het koppelen van 'het register'. Wat registers zijn, was – zoals we eerder hebben gezien – dwingend in de Wpolr voorgeschreven. Daarnaast was er blijkens de memorie van toelichting slechts sprake van koppelen indien het ging om een onbepaalde groep subjecten; expliciet was door de wetgever overwogen dat het gericht zoeken naar specifieke personen niet onder de werking van de koppelingsbepaling viel. Het doen van persoonsgerichte (operationele) analyses viel derhalve niet onder de koppelingsbepaling van de Wpolr en werd zodoende feitelijk helemaal niet genormeerd door de Wpolr. Het doen van algemene misdaadanalyses viel ook niet onder het koppelingsbegrip, nu het doel van een dergelijke analyse niet was om informatie omtrent personen te verkrijgen, maar een algemeen beeld van de criminaliteitsontwikkelingen.³²⁷ Slechts wanneer registers aan elkaar werden gekoppeld om uit de combinatie van die gegevens de betrokkenheid van personen bij criminaliteit te achterhalen (door bijvoorbeeld een opvallende gelijkenis tussen woonplaats, modus operandi, en strafrechtelijk verleden) leek er sprake van een koppeling in de zin van de Wpolr.

³²⁷ Overigens zitten er juist vanwege de algemeenheid van de uitkomsten van algemene misdaadanalyses vrijwel geen privacybezwaren aan dergelijke onderzoeken.

Vanuit de CIE werd ten slotte aangegeven dat het bij het uitvoeren van analyses lastig was om gegevens uit andere politieregisters erbij te betrekken. Bovendien zou daarbij rekening moeten worden gehouden met de verschillende typen geregistreerden (verdachten, betrokkenen, en contacten).³²⁸ Het wettelijk regime ten aanzien van het koppelen stelde ten aanzien van de type geregistreerde echter geen nadere eisen. Het aangedragen knelpunt komt voort uit het verstrektingsregime dat op dat andere politieregisters van toepassing was, zodat, gelet op de beperkingen van ons onderzoek, dit hier buiten beschouwing wordt gelaten.³²⁹ Zodra de CIE het gegeven heeft ontvangen valt het immers onder het verwerkingsregime van de CIE zelf. In dit verband merken we nog op dat veel analyses buiten de CIE werden uitgevoerd, zodat de betrokkenheid van de CIE beperkt bleef tot het verstrekken van de voor de analyse benodigde informatie, hetgeen logischerwijs werd gereguleerd door de verstrektingsbepalingen die in sectie 4.7 zijn behandeld.³³⁰

4.9.3 Uitwerking onder de Wpolg

Met de invoering van de Wpolg is een specifieke wettelijke regeling ingevoerd voor het analyseren van politiegegevens. Daarmee is het knelpunt onder de Wpolr opgelost. Met de invoering van dit regime zijn echter wel een aantal nieuwe knelpunten geïntroduceerd.

Nieuwe knelpunten geïntroduceerd

Naast de geautomatiseerde vergelijking van gegevens kunnen op grond van lid 4 van art. 11 Wpolg in bijzondere gevallen en op grond van het bevoegde gezag art.-8-gegevens, art.-9-gegevens en art.-10-gegevens in combinatie met elkaar worden verwerkt. Het gaat hier dus om een ruimere bevoegdheid dan het enkel vergelijken van gegevens, maar om de toepassing van geavanceerde technieken. Welke technieken dit zijn, wordt door de wetgever evenwel niet nader toegelicht. De mogelijkheden daartoe zijn echter groot te noemen.

De toepassing van de activiteit van analyseren kan evenwel alleen in bijzondere gevallen en in opdracht van het bevoegde gezag (de officier van justitie of de burgemeester). Wat de CIE betreft moet de analyse noodzakelijk zijn voor het doel waarvoor zij gegevens verwerkt. Voor de invulling van het noodzakelijkheidsbegrip wordt door de wetgever weer verwezen naar proportionaliteit en subsidiariteit. De wetgever geeft als voorbeelden ernstige delicten zoals ontvoeringen, gijzelingen en terroristische aanslagen, maar ook tactische analyses zonder dat er sprake is van een concrete verdachte of

328 Schreuders e.a., 2005, p. 82.

329 Zie sectie 1.3.

330 Schreuders e.a., 2005, p. 81.

verdenking. Er wordt dan gewerkt aan de hand van profielen van daders, slachtoffers of feiten. Op grond van de uitkomst kan worden besloten tot een opsporingsonderzoek dat gericht is op een of meer personen. Bewust is er voor gekozen om niet één criterium te geven maar om de uiteindelijke beslissing bij het bevoegde gezag te leggen, zodat de inzet in de toekomst niet door een te knellend toepassingscriterium gehinderd wordt.³³¹

Onder het regime van de Wpolg kunnen, in tegenstelling tot onder de Wpolr, ook informantgegevens geautomatiseerd worden verwerkt. Gelet op de bewoordingen gaat het hier niet alleen om de geautomatiseerde vergelijking, maar ook analyse-activiteiten. Het doel van de verwerking is wel aanzienlijk beperkt. De verwerking mag namelijk alleen plaatsvinden voor het doel waarvoor de informantgegevens worden gehouden. Dit betreft het beheer van de informantgegevens en gebruik voor betrouwbaarheidsinschatting van de informant, zodat operationele inzet van de resultaten niet is toegestaan.

4.9.4 Tussenconclusie aangaande het analyseren

Alvorens we onze tussenconclusie aangaande het analyseren formuleren, geven we schematisch weer (a) het aantal onder de Wpolr geconstateerde knelpunten, (b) de inhoud van die knelpunten, (c) de uitwerking daarvan onder de Wpolg, en (d) de (te verwachten) resultaten van de uitwerking onder de Wpolg.

Aantal	Knelpunten Wpolr	Wpolg	Resultaat
1	Geen normering	Analyseren genormeerd – toepassingscriterium – toepassingsbereik	'Knelpunt' opgelost, regeling bevat vage criteria, knelpunten in toepassing verwacht

Figuur 4.6 Schematisch weergave knelpunt 'analyseren'.

Onder de Wpolg heeft het analyseren een wettelijke basis gekregen, hetgeen alleen al een aanzienlijke verbetering is ten opzichte van de Wpolr, aangezien daar enige regeling ontbrak. De regeling die in de Wpolg is opgetekend, is op twee punten vaag te noemen. Ten eerste op het punt van het toepassingscriterium en ten tweede op het punt van het toepassingsbereik.

Toepassingscriterium

De activiteit van analyse mag ingezet worden voor zover dit noodzakelijk is voor het doel van de gegevensverwerking bij de CIE. Ook hier heeft de wetgever zich bediend van het noodzakelijkheidscriterium. De wetgever heeft in het geval van analyse expliciet overwogen dat zij dit criterium niet nader wenst in te kaderen aangezien de praktijk een flexibele inzet van deze

331 *Kamerstukken II, 2005/06, 30 327, nr. 3, p. 55.*

activiteit vereist. Feitelijk zal, in het geval van de CIE, de officier van justitie bepalen wanneer de inzet van analyse toegestaan is. Door het ruime toepassingscriterium zal in de praktijk veel afhangen van de wijze waarop hier door de officier van justitie invulling aan zal worden gegeven. Het valt daarbij op dat de memorie van toelichting weinig praktische handvatten biedt voor de vraag wanneer een analyse wel is toegestaan en wanneer niet. Voorbeelden daarvan ontbreken. We zagen al eerder bij de andere activiteiten dat de politiepraktijk daar wel behoefte aan heeft. Dat zal voor de officier van justitie niet anders zijn. Dit geldt te meer, nu de regeling voor de toepassing van analyses onder de Wpolg de eerste is, aangezien deze onder de Wpolr ontbrak.

Toepassingsbereik

Het ontbreken van enige technologische omschrijving van de mogelijke technieken die worden toegepast, brengt daarnaast de vraag met zich mee wat nu onder het koppelen van gegevens valt en wat onder de activiteit analyseren. Er is met andere woorden sprake van een afbakeningsprobleem. Mag er bijvoorbeeld een vergelijking van gegevens plaatsvinden met behulp van agenttechnologie, of hebben we het dan al over analyse? Agenten (in de zin van zelfstandige computerprogramma's die autonoom taken uitvoeren³³²) gaan immers zelfstandig en actief op zoek naar relevante informatie die voldoet aan de voorwaarden die vooraf door de gebruiker zijn opgegeven.

We begrijpen dat de omschrijving van de technieken bij de wetsuitleg sterk afhankelijk zijn van het tijdsverloop, maar ondanks dat bezwaar willen we toch dat enkele technologische beschrijvingen opgenomen worden. Het geeft immers een goed inzicht in het toepassingsbereik dat de wetgever voor ogen heeft gehad. Dit ontbreekt nu geheel en dat zal het toepassen van de wettelijke regeling voor de praktijk lastig maken. Ook voor het houden van controle en toezicht zal het weinige houvast dat de memorie van toelichting biedt een probleem vormen.

Het voorgaande klemmt te meer nu naar onze voorspelling de ontwikkelingen juist op dit punt aanzienlijk zullen zijn in de komende jaren. Er staan ons diverse doorbraken te wachten.³³³ Steeds meer informationele opsporingsmethoden zullen hun intrede doen in het dagelijkse politiewerk en vanuit de samenleving zal de druk op de politie groeien om deze technieken ook daadwerkelijk in te zetten.³³⁴ De onbepaaldheid van die technologische ontwikkeling (zoals we reeds in hoofdstuk 3 hebben besproken) liet, tezamen met de onbepaaldheid van de regeling rond analyse, de invulling ervan aan de praktijk. Het normerend en regulerend effect van de Wpolg is daarmee op dit punt nihil.

332 Zie uitgebreid Koelewijn 2009, p. 35-53.

333 Van den Herik en Postma, 2009.

334 Vanderlooy, 2009.

4.10 VERGELIJKING MET WBP

De ervaringen die sinds 2001 zijn opgedaan met het regime van de Wbp kunnen leerzaam zijn voor de vraag of de Wpolg aan de onder de Wpolr geconstateerde knelpunten tegemoet komt. De Wpolg is immers voor een belangrijk deel op de systematiek van de Wbp gebaseerd. Naar de ervaringen met de Wbp is door het WODC uitgebreid onderzoek gedaan naar aanleiding van de in de wet voorgeschreven evaluatie. Dat heeft geresulteerd in een eerste-fase-onderzoek, waarbij de knelpunten op basis van de bestaande literatuur zijn geduid. Op grond daarvan is een tweede fase onderzoek uitgevoerd, waarbij de ervaringen met de Wbp empirisch zijn onderzocht.

Het verschil in de wijze van regulering tussen de Wbp en de Wpolg is reeds aan het begin van dit hoofdstuk uiteengezet. Op dit punt is het relevant te benadrukken dat de Wbp een algemene verwerkingsgrond kent als gevolg van het omnibuskarakter. Dit betekent dat veel minder dan onder de Wpolg op detailniveau in de wet is opgenomen wanneer gegevens mogen worden opgeslagen, bewaard, verstrekt, gekoppeld en geanalyseerd. In de Wbp wordt alleen gesproken over het verwerken van gegevens; hier dient elk van deze activiteiten onder te worden begrepen. Dat maakt een één-op-één-vergelijking van de geconstateerde knelpunten niet mogelijk. We volstaan met het schetsen van een algemeen beeld dat uit voornoemde onderzoeken naar voren is gekomen.

Ook onder de Wbp blijkt het grootste probleem bij het verwerken van gegevens de vaagheid in de toepasselijke normen en regels. Het gaat dan om de onbekendheid met die normen en de onzekerheid over hoe die dienen te worden toegepast.³³⁵ Opvallend daarbij is dat de ondervraagden in dat onderzoek aangeven dat de verwerking niet anders kan worden geregeld dan met open normen.³³⁶ Daarvoor worden twee algemene redenen aangedragen. Ten eerste bieden de open normen ruimte voor een sectorspecifieke invulling die vanwege het omnibuskarakter van de Wbp gewenst is. Ten tweede bieden open normen volgens de respondenten de mogelijkheid om op technologische ontwikkelingen in te springen.

Invulling van de open normen blijkt in de praktijk echter onvoldoende te gebeuren. De praktijk neemt niet altijd haar eigen verantwoordelijkheid of kan die niet nemen omdat een bedrijfstak te klein of te versnipperd is om gezamenlijk voor nadere invulling daarvan te zorgen. Uit het onderzoek van het WODC blijkt dat een stimulerende rol van de overheid, bijvoorbeeld vanuit het Cbp, gemist wordt. Het gaat naar ons idee dan vooral om een overkoepelende blik die verschillende ervaringen uit de praktijk combineert tot een sectorspecifieke invulling van de normen uit de Wbp.

335 Winter e.a., 2008, p. 147.

336 *Idem*, p. 146.

Commissie Brauer-Korf

In 2009 heeft de commissie Brauer-Korf onderzoek gedaan naar veiligheid en de persoonlijke levenssfeer. Het is een overkoepelend onderzoek dat over de grenzen van de werkingssfeer van de Wbp en de Wpolg heen heeft gekeken. Daarmee was het verwerken van politiegegevens onderdeel van onderzoek, maar dus niet specifiek. De commissie heeft in haar constatering in de praktijk een aantal constatering die onze bevindingen bevestigen. Het gaat dan vooral om onze bevinding dat de regelgeving rond privacy in de praktijk het stempel heeft ingewikkeld te zijn. Daarnaast constateert de commissie dat de privacyspecialisten in een organisatie weinig gelegenheid hebben om zich te verdiepen in de problemen die zich voordoen in de organisatie. Ook wordt privacy ten onrechte gebruikt als doodoener om geen gegevens te hoeven verstrekken.³³⁷ De commissie constateert dat zorgvuldig gegevensbeheer niet in het werk zit ingebakken en dat de discussie gedomineerd wordt door een juridische invalshoek. Dit staat er naar haar mening aan in de weg dat in de praktijk een debat op gang komt over de manier waarop met gegevens om zou moeten worden gegaan en daarmee ook de bewustwording van het belang daarvan in de organisatie tot stand komt.³³⁸ De bevindingen en conclusies van de commissie Brauer-Korf ondersteunen daarmee onze bevindingen zoals we deze in dit hoofdstuk hebben beschreven.

4.11 BEANTWOORDING OV2 EN OV3 AANGAANDE DE WET

In dit hoofdstuk is het proces van informatieverwerking door de CIE-en besproken. Daarbij is antwoord gegeven op OV2 en OV3 voor zover het de wet als waarborg betreft. OV2 luidt: *“Welke knelpunten zijn er in de literatuur en de praktijk geconstateerd ten aanzien van de waarborgende werking van de Wet politieregisters?”* en OV3 luidt: *“In hoeverre komt de Wet politiegegevens, mede in het licht van de ervaringen met de Wet bescherming persoonsgegevens, tegemoet aan deze knelpunten?”* In dit hoofdstuk hebben we beschreven op welke wijze de Wpolg tegemoet komt aan de onder de Wpolr geconstateerde knelpunten als het gaat om (1) het opslaan, (2) het bewaren, (3) het verstrekken, (4) het koppelen en (5) het analyseren van politiegegevens door de CIE. In deze hoofdstukconclusie herhalen we niet alle geconstateerde individuele knelpunten, maar abstraheren we ze tot een hoger niveau. Het gaat dan om (1) de vaagheid in toepassingsvoorwaarden, (2) de oplossingen die vooral instrumenteel van karakter zijn en (3) de noodzaak van sterkere overige waarborgen.

337 Brauer-Korf e.a., 2009, p. 24-25.

338 *Idem*, p. 25-28.

Ad(1) Vaagheid in toepassingsvoorwaarden

Als veruit het belangrijkste knelpunt onder de Wpolr is de vaagheid in de regeling naar voren gekomen. Dit werd vooral veroorzaakt door het gebruik van het begrip 'noodzakelijkheid' als voorwaarde voor de toepassing van bepaalde bevoegdheden in het verwerken van politiegegevens. Noodzakelijkheid als voorwaarde kwam onder de Wpolr terug bij de activiteiten bewaren, de weigeringsgrond voor het verstrekken van informatie, het koppelen en het analyseren. Ondanks de in de praktijk bestaande problemen is deze voorwaarde onder de Wpolg onverkort gehandhaafd. Sterker nog, zoals gezien is bij de activiteit 'bewaren' de noodzakelijkheid als voorwaarde een sterkere rol gaan spelen.

Op zichzelf is het gebruik van noodzakelijkheid als voorwaarde niet per definitie problematisch. Gelet op de in de praktijk bestaande knelpunten had het echter wel op de weg van de wetgever gelegen om in de memorie van toelichting een uitgebreide verhandeling te geven over de toepassing van dit begrip in de verwerking van politiegegevens. Dit geldt temeer omdat nu onder de Wpolg de noodzakelijkheid als voorwaarde een sterkere positie krijgt dan onder de Wpolr. Nu de Wpolg niet voorziet in die verduidelijking van de het begrip noodzakelijkheid moet op dit punt worden geconstateerd dat de waarborgende werking van de Wpolg is verslechterd ten opzichte van de Wpolr.

Ook wat betreft de geconstateerde classificatieknelpunten moet worden geconstateerd dat er op dat punt vaagheid blijft bestaan. De Wpolg gaat nog steeds uit van de klassen (1) verdachten, (2) betrokkenen en (3) contacten zonder dat daarbij handvatten worden gegeven om het onderscheid daartussen te verduidelijken. Ook op dit punt zal de praktijk dus geconfronteerd blijven met de knelpunten die zich op dit punt onder de Wpolr voordeden.

Daarnaast heeft de Wpolg met de introductie van de themaverwerking een nieuwe verwerkingsgrond geïntroduceerd waarvan te verwachten is dat deze in de praktijk tot nieuwe afbakeningsproblemen zal leiden. Ook daar heeft de wetgever zich bediend van een vage terminologie en verzuimd iets van een afbakening te formuleren over de reikwijdte van de regeling als het gaat om de personen over wie op die grond gegevens mogen worden verwerkt.

Het onderzoek dat in de praktijk naar de uitwerking van de Wbp is gedaan, maakt duidelijk dat juist vage normen ook mogelijkheden bieden voor de praktijk om bevoegdheden flexibel in te zetten. Daarbij is dan wel een nadere interpretatie van die open en vage normen vereist en de invloed van een overkoepelende organisatie gewenst.

Ad(2) Oplossingen vooral instrumenteel

We hebben gezien dat de Wpolg ook een aantal prangende knelpunten heeft opgelost. Dit betrof echter vooral knelpunten vanuit een instrumenteel belang. We noemen het afbakeningsprobleem tussen het voorlopig register en het register zware criminaliteit. Het is echter de vraag of met de wijze waarop dit probleem is opgelost – het schrappen van het voorlopig register –

recht wordt gedaan aan de daarmee verbonden beschermingsbelangen. Vast staat dat op dit punt aan bescherming is ingeleverd. Gegevens, die onder de Wpolr onder de beperkte 'verwerkingsgronden' van het voorlopig register vielen, vallen nu direct onder het ruimere verwerkingsregime van de zwa-criververwerking. Daarmee is weliswaar het afbakeningsprobleem opgelost, maar is aan bescherming van die voorlopige gegevens ingeboet.

Het oplossen van knelpunten ten koste van het beschermingsniveau zagen we ook bij de te knellende bewaartermijn van 5 jaar, waarvan onder de Wpolg kan worden afgeweken. We noemen voorts de toegangsproblemen tot het informantenregister die zijn opgelost, evenals de verstrekkingmogelijkheden naar derden buiten de politieorganisatie. Daarnaast worden met de introductie van themaverwerkingen meer mogelijkheden geboden tot gegevensverwerking. De geboden mogelijkheden in het verwerken van politiegegevens zijn onder de Wpolg dan ook ontegenzeggelijk ruimer dan onder de Wpolr. De wetgever heeft – zoals reeds besproken – zelf ook aangegeven dat de Wpolg meer mogelijkheden biedt tot gegevensverwerking dan de Wpolr.

Ad(3) Meer mogelijkheden, sterkere waarborgen?

Tegenover deze ruimere instrumentele mogelijkheden staat volgens de wetgever ook een strenger systeem van waarborgen. Maar die extra bescherming kan echter niet van de eerste waarborg worden verwacht. Die eerste waarborg is het verwerkingsregime zelf en daarin zit wat betreft de bevoegdheden nu juist een aanzienlijke verruiming van de mogelijkheden.

In de toepassingsvoorwaarden blijft de vaagheid echter een grote factor van betekenis. Dit geldt ten eerste op punten waarvan reeds onder de Wpolr was geconstateerd dat deze tot toepassingsproblemen hebben geleid, maar ten tweede zien we dat de Wpolg ook nieuwe regelingen introduceert waarbij toepassingsproblemen te verwachten zijn (onder andere (1) themaverwerking en (2) de koppeling van de 5-jaar-bewaartermijn aan de noodzakelijkheid). Kort gezegd blijft daarmee onduidelijk wanneer de (ruimere) bevoegdheden door de politie mogen worden ingezet. Dit leidt tot de conclusie dat de Wpolg slechts op ondergeschikte deelpunten een oplossing biedt voor de onder de Wpolr geconstateerde knelpunten als het gaat om het verwerken van politiegegevens en het wettelijk kader. De Wpolg voorziet weliswaar in meer instrumentele mogelijkheden, maar brengt ook een toenemende vaagheid met zich mee in de toepassingsvoorwaarden van die bevoegdheden.

Op grond van het nieuwe verwerkingsregime moet worden geconstateerd dat het regime van de Wpolg aan waarborgende werking inboet. Dat vraagt dus, bij wijze van compensatie, meer van de overige twee waarborgen, die in de navolgende hoofdstukken aan bod komen.

5 Het kennisnemingsrecht in theorie en praktijk

Naast het wettelijk verwerkingsregime is de tweede waarborg het kennisnemingsrecht. De betrokkene, degene op wie de gegevens betrekking hebben, heeft in beginsel het recht om kennis te nemen van de gegevens die over hem door de politie zijn geregistreerd en om wijziging of verwijdering daarvan te verzoeken. In dit hoofdstuk behandelen we de tweede en derde onderzoeksvraag met betrekking tot het kennisnemingsrecht. Ov2 luidt: *“Welke knelpunten zijn er in de literatuur en de praktijk geconstateerd ten aanzien van de waarborgende werking van de Wet politieregisters?”* en Ov3 luidt: *“In hoeverre komt de Wet politiegegevens, mede in het licht van de ervaringen met de Wet bescherming persoonsgegevens, tegemoet aan deze knelpunten?”*. Het hoofdstuk is gebaseerd op drie wettelijke regelingen: de Wpolr, de Wpolg en de Wbp. Het gaat over de wijze waarop de Wpolr en Wpolg vorm geven aan het kennisnemingsrecht. We onderzoeken de knelpunten die zich in de uitvoering hiervan voordoen onder het regime van de Wpolr en de oplossingen die de Wpolg voor deze knelpunten biedt. Dit doen we in het licht van de ervaringen die met de Wbp zijn opgedaan.

In ons onderzoek houden wij op een wetenschappelijk verantwoorde wijze rekening met de verschillende doelstellingen en de wijze van regulering in de drie wettelijke regelingen (zoals beschreven in sectie 4.1 en 4.2). In sectie 5.1 behandelen we de wijze waarop het kennisnemingsverzoek onder de Wpolr is uitgewerkt. In sectie 5.2 bespreken we de controle en het toezicht op de uitvoering van een kennisnemingsverzoek. De wijze waarop het kennisnemingsrecht onder de Wpolg vorm heeft gekregen is onderwerp van sectie 5.3. Naar aanleiding van hetgeen is behandeld in de secties 5.1 tot en met 5.3 formuleren wij in sectie 5.4 een tussenconclusie om vervolgens in sectie 5.5 het kennisnemingsrecht als waarborg ter discussie te stellen. Ten slotte beantwoorden we in sectie 5.6 de tweede en derde onderzoeksvraag aangaande het kennisnemingsrecht en geven we een hoofdstukconclusie.

5.1 THEORETISCH KADER

In art. 20 Wpolr is bepaald dat iedereen een verzoek tot de beheerder van een politieregister kan richten of, en zo ja welke, gegevens betreffende zijn persoon in het register zijn opgenomen. Daarbij moeten ook inlichtingen worden verschaft over de herkomst van de gegevens en over degene aan wie de gegevens zijn verstrekt. De informatie wordt niet schriftelijk verschaft, maar het gaat blijkens art. 21, eerste lid, Wpolr om een medede-

ling.³³⁹ In art. 21 Wpolr is voorts de mogelijkheid opgenomen om het doen van een dergelijke mededeling te weigeren indien dit (a) noodzakelijk is voor de goede uitvoering van de politietaak of (b) indien gewichtige belangen van derden daartoe noodzaken. Weigering is niet mogelijk indien het gaat om antecedenten³⁴⁰ of om persoonsgegevens die op verzoek van de betrokkene zelf zijn opgenomen.³⁴¹

Ingevolge art. 21 lid 3 Wpolr wordt in de verschillende reglementen bepaald in hoeverre toepassing wordt gegeven aan de weigeringsmogelijkheid van de beheerder om aan een kennisnemingsverzoek te voldoen. Een kennisnemingsverzoek dat gericht is op informatie die is opgenomen in het zwacri-register,³⁴² het voorlopig register³⁴³ of het informantenregister³⁴⁴ kan blijkens de toepasselijke modelreglementen geweigerd worden indien daaruit onevenredige schade kan voortvloeien, hetzij voor het beheer van de informantgegevens, hetzij voor een onderdeel van de politietaak, hetzij in verband met gewichtige belangen van derden.

In het verlengde van het kennisnemingsverzoek kan de verzoeker de beheerder van het register schriftelijk verzoeken om de opgenomen gegevens te verbeteren, aan te vullen, te verwijderen of af te schermen. De gegevens moeten dan wel (1) feitelijk onjuist zijn, (2) voor het doel van het register onvolledig of niet ter zake dienend zijn, dan wel (3) in strijd met een wettelijk voorschrift in het register voorkomen. De beheerder dient binnen vier weken te berichten of hij aan het verzoek voldoet. Een weigering moet met redenen omkleed zijn. Als de beheerder niet aan het verzoek voldoet, kan de verzoeker zich tot de rechter wenden om dit alsnog te bewerkstelligen. Op de wijze van rechterlijke controle wordt in subsectie 5.2.3 nader ingegaan.

339 Met uitzondering van de mededeling van de beslissing tot (gedeeltelijke) weigering van een kennisnemingsverzoek CBP, 23 oktober 2002, Z2002-0616.

340 Art. 2 Bpolr bepaalt wat antecedenten zijn: "a. het feit dat een proces-verbaal is opgesteld van het verhoor van een bepaald persoon ter zake van een strafbaar feit waarvoor deze als verdachte is gehoord, daaronder begrepen de aanduiding van de aard van dat strafbare feit;

b. het feit of al dan niet een proces-verbaal als bedoeld onder a, is verzonden aan het openbaar ministerie, en zo ja, de datum van verzending en het nummer waarmee het proces-verbaal aldaar kan worden geïdentificeerd en

c. de beslissing van het openbaar ministerie of de rechter over de aangelegenheid waarop het proces-verbaal betrekking heeft."

341 Art. 21 lid 2 Wpolr.

342 Art. 15 lid 2 modelreglement register zware criminaliteit.

343 Art. 12 lid 2 modelreglement voorlopig register.

344 Art. 12 lid 2 modelreglement informantenregister.

5.1.1 Afhandeling van het kennisnemingsverzoek

Het kennisnemingsrecht is een lange tijd vrijwel niet gebruikt door geregistreerden. Vanaf het jaar 2000 is daarin een behoorlijke stijging waarneembaar. Zo zijn in 2000 voor de bijzondere politieregisters ongeveer 25 verzoeken gedaan, in het jaar 2001 is dit aantal gestegen tot 65 en over 2002 was wederom een stijging waarneembaar.³⁴⁵ In de jaren daarna, zo blijkt uit het WODC-evaluatieonderzoek uit 2005, is het aantal verzoeken bij de CIE beperkt gebleven tot enkele per jaar.³⁴⁶ Daarbij ging het vooral om verzoeken die vanuit de advocatuur gedaan werden namens geregistreerden. Deze verzoeken zorgden voor problemen binnen de politiepraktijk. Naar aanleiding daarvan is de Werkgroep Stroomlijning inzagerecht ingesteld die een handleiding (hierna: de handleiding) heeft geschreven voor de te volgen procedure bij de afwikkeling van de kennisnemingsverzoeken. Het rapport werd ten tijde van het WODC-evaluatieonderzoek algemeen gebruikt voor de afhandeling van kennisnemingsverzoeken.³⁴⁷

In de handleiding is een procedure opgenomen die gevolgd kan worden bij de afhandeling van kennisnemingsverzoeken. Daarbij wordt veel aandacht besteed aan de te behandelen formaliteiten bij het afhandelen van een kennisnemingsverzoek. Het gaat dan bijvoorbeeld om een coördinatiesysteem waarin de kennisnemingsverzoeken worden geregistreerd, zodat kan worden nagegaan of een verzoek al eerder is gedaan. Ook biedt een dergelijk coördinatiesysteem de mogelijkheid om meerdere afzonderlijke verzoeken te onderkennen, die in hun totaliteit wellicht te veel zicht geven op het kennisniveau van de CIE (en dus geweigerd dienen te worden). Deze formaliteiten worden blijkens het WODC-evaluatieonderzoek in het algemeen door de privacyfunctionaris afgehandeld. De inhoudelijke afweging over wat aan een verzoeker ter kennisneming wordt meegedeeld, ligt evenwel bij de CIE zelf. Vanwege de afschermingsbelangen die een rol kunnen spelen is in de handleiding opgenomen dat de CIE, die de informatie van een informant heeft ingewonnen, de enige is die kan bepalen of informatie aan de verzoeker kan worden verstrekt. Het kennisnemingsrecht dient derhalve bij de CIE gedaan te worden. Indien de informatie bij de CIE aanwezig is, dient de CIE intern af te stemmen of de betreffende informatie aan de verzoeker kan worden meegedeeld.³⁴⁸

Evenals het wettelijk systeem gaat de handleiding ervan uit dat de verzoeker die een kennisnemingsverzoek heeft ingediend kennis dient te krijgen van de gegevens die over hem geregistreerd zijn, tenzij een weigeringsgrond kan worden ingeroepen. Zoals hiervoor is behandeld kan een kennisnemingsverzoek worden geweigerd indien dit (a) noodzakelijk is voor de goede

345 *Rapport Procedure/handleiding omgang met inzageverzoeken*, werkgroep stroomlijning inzagerecht, rapport te downloaden op <<http://www.cbppweb.nl>>.

346 Schreuders e.a., 2005, p. 157.

347 Schreuders e.a., 2005, p. 157.

348 Handleiding, sectie 2.

uitvoering van de politietaak of (b) indien gewichtige belangen van derden daartoe noodzaken. De handleiding noemt als voorbeelden:

- het afschermen van informanten;
- het voorkomen van het opdrogen van informatiebronnen;
- het afschermen van opsporingsonderzoeken;
- het afschermen van opsporingsmethoden (tactisch en technisch);
- indien de veiligheid of gezondheid van personen in het geding is of indien direct gevaar voor de desbetreffende geregistreerde of voor derden dreigt.

Het register zware criminaliteit

Als het gaat om kennisnemingsverzoeken die gericht zijn op het register zware-criminaliteit zoekt de handleiding aansluiting bij de daar gebruikte afhandelingscodes, zoals uitgebreid door Koelewijn is beschreven.³⁴⁹ Wat de informatie betreft die in het register is opgeslagen onder de code 01 en 00 zal mededeling daarvan in beginsel geweigerd dienen te worden met verwijzing naar een algemene motivering, zoals hieronder is beschreven. Een zeer globale weergave van deze gegevens is onder omstandigheden mogelijk. Van informatie die is weggeschreven onder code 200 en 300 zal nooit mededeling gedaan worden. Alleen ten aanzien van de 11-informatie gaat de handleiding ervan uit dat mededeling daarvan mogelijk is, maar aangegeven wordt dat de beheerder zal moeten beslissen of, en zo ja in welke vorm, dat kan gebeuren.³⁵⁰ Zoals reeds in hoofdstuk 2 is behandeld, is de toekenning van een afhandelingscode aan de verkregen informatie typisch een taak van de CIE zelf.

Het voorlopig register

Ook wat het voorlopig register betreft gaat de handleiding uit van de mededelingsplicht, tenzij er een beroep op de weigeringsgrond mogelijk is. Het doel van het voorlopig register is informatie op te slaan die mogelijk voor registratie in het zwacri-register in aanmerking komt. Nu dit voor een periode van zes maanden is, stelt de handleiding dat gedurende deze maanden de geregistreerde personen in onderzoek zullen zijn juist om te proberen de verkregen informatie 'op te waarderen' naar het zwacri-register. Een kennisnemingsverzoek gericht op het voorlopig register zal onder verwijzing naar dat onderzoek veelal geweigerd kunnen worden in verband met de goede uitvoering van de politietaak.³⁵¹

Het informantenregister

Specifiek ten aanzien van het informantenregister stelt de handleiding dat het register onder het regime van de Wpolr een gewoon politieregister is.

349 Koelewijn, 2009, p. 109.

350 Handleiding, sectie 4.3.2.3.

351 *Idem*, sectie 4.3.2.2.

Voor de afhandeling van een kennisnemingsverzoek geldt dan in beginsel de hoofdregel dat informatie uit dit register wordt verstrekt, tenzij er sprake is van een weigeringsgrond. De handleiding vermeldt daarbij dat in de praktijk vaak van deze mogelijkheid gebruik zal kunnen worden gemaakt. Gezien het doel van het register zal het immers bijna altijd noodzakelijk zijn om de gegevens af te schermen ter bescherming van de belangen van derden: de informant.³⁵²

Uit de handleiding blijkt dat de CIE zich bij een verzoek tot kennisneming veelal op een weigeringsgrond zal kunnen beroepen. Samengevat komt het erop neer dat de informatie die is opgenomen in het informantenregister en het voorlopig register in beginsel niet voor mededeling aan de verzoeker in aanmerking komt. Van de informatie die is opgenomen in het zwacri-register komt in principe alleen de 11-informatie in aanmerking.

Een weigering van gegevensverstrekking dient gemotiveerd te worden. De weigering dient volgens de handleiding ook mondeling te worden toegelicht indien daarvoor aanleiding bestaat.³⁵³ Zoals reeds is aangegeven dient een weigeringsbeslissing schriftelijk te worden meegedeeld.

5.1.2 De wijze van kennisneming

Op het moment dat is bepaald of, en zo ja welke, informatie aan de verzoeker kan worden meegedeeld kan de beheerder van het register de verzoeker meedelen (a) dat hij niet in het betrokken politieregister voorkomt, (b) dat gegevens over hem voorkomen in het politieregister en hoe (een gedeelte van) de inhoud van die gegevens en de herkomst ervan verstrekt zullen worden, of (c) dat bij de controle van het register is gebleken dat de wettelijke bepalingen ten aanzien van de verzoeker zijn nageleefd. De handleiding vermeldt ten aanzien van de laatste mogelijkheid dat hiervan slechts gebruik dient te worden gemaakt indien er sprake is van een strategisch belang.

De wijze van kennisneming is volgens de Wpolr een mededeling. De wijze waarop deze mededeling moet worden gedaan is verder niet gereguleerd. De handleiding geeft daar een praktische invulling aan.³⁵⁴ Voorgeschreven is om een voor alle betrokkenen zo praktisch mogelijke invulling aan de mededelingsvorm te geven. Zo wordt in de handleiding beschreven dat een verzoek van een raadsman van een geregistreerde telefonisch kan worden afgedaan. Ook kan de verzoeker worden uitgenodigd om op het bureau van de geregistreerde gegevens kennis te nemen en mogelijk zelfs aantekeningen te maken. Als anonimiseren echter meer werk oplevert dan het voorlezen van de mee te delen passages dan kan volgens de handleiding met dit laatste wor-

352 *Idem*, sectie 4.3.2.1.

353 *Idem*, sectie 4.2.1.

354 *Idem*, sectie 4.1.

den volstaan. De verzoeker zal dan op het bureau worden uitgenodigd waar hij de betreffende passages krijgt voorgelezen. De handleiding adviseert dringend het maken van geluidsopnames daarvan niet toe te staan.

Over de mate van gedetailleerdheid van de mededeling die aan de verzoeker wordt gedaan vermeldt de handleiding dat in zijn algemeenheid het uitgangspunt is dat de in de registers opgenomen gegevens integraal worden weergegeven aan betrokkene. Als dit niet wenselijk is, kan worden volstaan met een zakelijke weergave van de opgenomen gegevens. Dit heeft blijkens de handleiding bij het weergeven van CIE-gegevens de voorkeur aangezien de verzoeker anders mogelijk te veel kennis krijgt van het kennisniveau van de CIE.³⁵⁵

5.2 DE KNELPUNTEN BESCHREVEN

Iedere CIE blijkt in de praktijk met het kennisnemingsrecht in aanraking te zijn gekomen. Het aantal verzoeken is echter beperkt. Ten tijde van het WODC-evaluatieonderzoek en het onderzoek van Kielman en Koelewijn betrof het enkele kennisnemingsverzoeken per jaar per CIE, met een maximum van zeven.³⁵⁶ Het onderzoek naar de uitwerking van het kennisnemingsrecht onder de Wbp laat een soortgelijk beeld zien. Ook daar wordt erg weinig gebruikt van gemaakt. De commissie-Brauer constateert dat het recht op inzage en correctie van persoonsgegevens een hoge drempel kent. Ook signaleert zij dat het recht op kennisneming nauwelijks bekend is bij burgers.³⁵⁷

Door de onderzoekers van het Wbp-evaluatieonderzoek wordt opgemerkt dat het privacygeschil meestal slechts een onderdeel is van een groter geschil zoals bijvoorbeeld een arbeidsconflict. Die constatering is hier relevant aangezien het de vraag opwerpt of de kennisnemingsverzoeken die gedaan worden echt uit privacy-overwegingen worden gedaan of dat wordt beoogd er in strafvordelijke zin voordeel mee te behalen.

In het onderzoek van Kielman en Koelewijn is verder naar voren gekomen dat onder de CIE-en in zijn algemeenheid een weerstand bestaat om aan de kennisnemingsverzoeken te voldoen. De omstandigheid dat een persoon, die onderwerp van onderzoek is, aan de politie kan vragen wat ze over hem geregistreerd hebben – en dus waar het onderzoek over gaat – bevreemdt de CIE-ers.

Een minderheid van de gedane kennisnemingsverzoeken betreft zogenaamde '*fishing expeditions*', waarbij een verzoek wordt gedaan zonder dat dit nader gemotiveerd is. Daarbij bestaat bij de CIE de indruk dat dergelijke verzoeken bedoeld zijn om de identiteit van een informant of de informatie-

355 *Idem*, sectie 4.3.4.

356 Schreuders e.a., 2005, p. 157.

357 Brauer-Korf e.a., 2009, p. 25.

positie van de CIE te achterhalen.³⁵⁸ Van Stratum geeft aan dat er daarnaast diverse strafvorderlijke belangen met het kennisnemingsrecht worden nagestreefd.³⁵⁹ Dergelijke verzoeken kosten de CIE vanzelfsprekend veel tijd, doordat alle gegevens die met betrekking tot die persoon geregistreerd zijn, moeten worden doorlopen om te bepalen of deze voor mededeling in aanmerking komen. Over de precieze belasting voor de CIE zijn geen cijfers bekend, maar over één subject kunnen duizenden gegevens geregistreerd zijn (denk aan bijvoorbeeld uitgewerkte telefoontaps). Ten aanzien van ieder afzonderlijk gegeven zal bepaald moeten worden of dat gegeven voor kennisneming in aanmerking komt. Dergelijke uitgebreide onderzoeken vormen daarbij een zware last die ten koste gaat van de capaciteit die de CIE heeft voor haar andere werkzaamheden. Deze tijdrovende bezigheden waren in het verleden voor Van der Pol reden om te constateren dat het eenvoudig is de politieorganisatie tijdelijk 'lam te leggen' door het doen van een kennisnemingsverzoek.³⁶⁰

In het evaluatieonderzoek werd geconstateerd dat er een vermindering van dergelijke uitgebreide kennisnemingsverzoeken waarneembaar was, maar werd tegelijk opgemerkt dat deze daling mogelijk slechts tijdelijk van aard was. Bij *fishing expeditions* werd over het algemeen na binnenkomst van een dergelijk verzoek contact met de verzoeker (of diens gemachtigde) opgenomen om te kijken of het verzoek gespecificeerd kon worden. Ook kwam het voor dat een CIE simpelweg een verzoek weigerde als het een *fishing expedition* betrof.³⁶¹ Dat laatste is met betrekking tot het CIE-register door de rechter goedgekeurd indien het verzoek een zeer algemeen karakter heeft.³⁶²

Over de wijze waarop het probleem van het gebruik van het kennisnemingsrecht als *fishing expediton* kan worden opgelost, bestaan binnen de politie verschillende gedachten. Er kan een oplossingsrichting worden gezocht waarbij de grond voor het weigeren van een verzoek wordt opgerekt, hetgeen volgens het WODC-evaluatieonderzoek het gevaar in zich draagt dat het kennisnemingsrecht een papieren tijger wordt. Daarnaast wordt gedacht aan een oplossing om kennisnemingsverzoeken te weigeren indien daar door de verzoeker een strafvorderlijk belang mee wordt nagestreefd in plaats van zijn privacy-belang. Er kan dan gedacht worden om een weigeringsgrond aan het huidige arsenaal toe te voegen, waarbij een verzoek kan worden geweigerd indien er nog een strafvorderlijk middel voorhanden is om toegang tot die gegevens te verkrijgen. De onderzoekers van het WODC-evaluatieonderzoek merken daarbij op dat het voor de politie lastig is te achterhalen wat de precieze motieven zijn voor het doen van een kennisnemingsverzoek.³⁶³

358 Schreuders e.a., 2005, p. 158.

359 Van Stratum, 2001, p. 178.

360 Van de Pol, 2002, p. 113.

361 Schreuders e.a., 2005, p. 159.

362 Rb 's-Gravenhage, 5 juni 2008 (niet gepubliceerd).

363 Schreuders e.a., 2005, p. 165.

Daarnaast ondervonden de CIE-en hinder van verzoeken die veel werk met zich meebrengen vanuit de advocatuur, waarbij direct werd gedreigd met alle mogelijke juridische stappen indien niet aan de wettelijke termijnen werd voldaan. Dit bemoeilijkt een weloverwogen beslissing over welke gegevens voor kennisneming in aanmerking komen als ook het nemen van de verantwoordelijkheid daarover.³⁶⁴

5.2.1 Het gehonoreerd krijgen van het verzoek

Na een verzoek tot kennisneming bij de CIE zelf, heeft de verzoeker twee mogelijkheden om de juistheid van de aan hem meegedeelde beslissing op zijn verzoek aan te kaarten. Ten eerste kan hij het CBP vragen om te bemiddelen. Daarnaast kan hij een verzoekschriftprocedure starten bij een arrondissementsrechtbank. Deze laatste weg staat ook nog open op het moment dat reeds door het CBP bemiddeld is.

Bemiddeling door het Cbp

Binnen de in art. 23 lid 2 Wpolr gestelde termijn kan een verzoeker, alvorens een verzoekschriftprocedure bij de rechtbank te starten, het CBP verzoeken te bemiddelen tussen hem en de beheerder van het register waar hij om kennisneming heeft verzocht. Het gaat om een bemiddeling, zodat het CBP geen bindende uitspraken kan doen. Wij hebben op de website van het CBP slechts één verslag van bemiddeling van het CBP gevonden. Daar is bemiddeld tussen een betrokkene en de Regiopolitie IJsselland.³⁶⁵ Naar aanleiding van een krantenbericht over banden tussen Turkse lokale en provinciale politici en de Turkse maffia had een Turks lid van de Provinciale Staten een kennisnemingsverzoek gedaan. Het verzoek werd door de politie geweigerd, waarop het CBP door het Statenlid werd ingeschakeld met het verzoek om te bemiddelen. Het CBP stelt in haar bemiddeling voorop dat het uitgaat van een marginale beoordeling of de weigering van het kennisnemingsverzoek terecht is. In casu had de politie (1) aangegeven dat er naar datgene waar de gegevens betrekking op hadden nog altijd een onderzoek liep en (2) mededeling geweigerd aan het Statenlid over het al dan niet geregistreerd zijn vanuit strategische (onderzoeks)belangen. Het CBP achtte het belang van de politie zwaar genoeg om het kennisnemingsverzoek te weigeren.

In de beschreven casus waarbij door het CBP is bemiddeld lijkt het CBP zelf geen kennis te hebben genomen van de betreffende gegevens. Dit was gelet op de voorliggende vraag ook niet noodzakelijk. Uit het WODC-evaluatieonderzoek blijkt dat kennisneming van de geweigerde gegevens door het CBP, ondanks de toezichthoudende taak en de daarmee gepaard gaande onderzoeksmogelijkheden, voor de politie gevoeliger ligt dan het

³⁶⁴ Schreuders e.a., 2005, p. 164.

³⁶⁵ CBP, 26 maart 2004, z2006-0440.

ter beschikking stellen van de gegevens aan de rechter.³⁶⁶ Een reden hiervoor wordt niet gegeven, maar kennelijk is er sprake van een minder hoog vertrouwensniveau bij de politie ten aanzien van het CBP dan ten aanzien van de rechterlijke macht. Ten aanzien van deze laatste categorie heeft de politie immers aangegeven dat kennisneming van de betreffende gegevens in de praktijk niet tot problemen leidt. In het evaluatieonderzoek is zelfs aangegeven dat korpsen weigerachtig zouden zijn bij het verlenen van kennisneming tot gegevens ten aanzien waarvan een kennisnemingsverzoek is gedaan. Het CBP zelf gaat er evenwel van uit dat zij kennis kan nemen van de betreffende gegevens op grond van het bepaalde in art. 26 Wpolr.³⁶⁷

Rechterlijke bemiddeling

Indien de beheerder niet aan het verzoek overeenkomstig art. 20 of 22 Wpolr voldoet, kan een verzoekschrift bij de arrondissementsrechtbank worden ingediend waarin wordt verzocht de beheerder van het registers te bevelen alsnog aan deze verplichting te voldoen. In lid 2 van art. 23 Wpolr is bepaald dat dit verzoek dient te worden gedaan binnen vier weken nadat de beslissing van de beheerder aan de verzoeker is meegedeeld. In de beoordeling van het verzoek kan de rechtbank ingevolge art. 23 lid 4 het CBP om advies vragen. Uit de openbare bronnen zijn slechts een aantal uitspraken te raadplegen die zien op een geschil dat is voortgekomen uit een kennisnemingsverzoek dat (onder meer) is gericht op een politieregister dat bij de CIE wordt gevoerd. Daaruit komt naar voren dat van de adviesmogelijkheid bij het CBP gebruik wordt gemaakt.

Voorts is door de Hoge Raad uitgemaakt dat de toetsing door de rechter in de verzoekschriftprocedure *ex nunc* dient plaats te vinden.³⁶⁸ Het is derhalve niet de vraag of de korpsbeheerder ten tijde van het kennisnemingsverzoek terecht heeft geweigerd, maar of er op het moment van beoordeling door de rechter nog sprake is van een toepasselijke weigeringsgrond.

5.2.2 Kennisneming van politiegegevens door de rechter

Uit de bestudeerde uitspraken komt één duidelijk knelpunt naar voren. De Wpolr kent geen verstrekkingsmogelijkheid waarbij gegevens aan een lid van de rechterlijke macht kunnen worden verstrekt. De enige gegevens waar de rechterlijke macht kennis van mag nemen zijn de antecedenten die overeenkomstig art. 16 Wpolr aan hun leden kunnen worden verstrekt.

De rechtbank Maastricht besteedt in haar uitspraak van 22 maart 1996³⁶⁹ uitgebreid aandacht aan de problematiek van het kennisnemen van politie-

366 Schreuders e.a., 2005, p. 163.

367 Schreuders e.a., 2005, p. 163.

368 HR 24 januari 1997, NJ 1998/398.

369 Rb Maastricht 31 oktober 1996, Rb Maastricht 20 februari 1997, NJ 1997/26, Rb Maastricht 13 november 1997, NJ 1997/103.

gegevens door de rechter in het kader van een verzoekschriftprocedure. Zij overweegt dat de Wpolr geen bepalingen bevat op grond waarvan politiegegevens aan de rechter verstrekt kunnen worden. Voorts lijkt ook de parlementaire geschiedenis op het niet bestaan van een dergelijke mogelijkheid te wijzen. Daartoe citeert de rechtbank de parlementaire geschiedenis aangaande de wijze waarop aan de verzoekschriftprocedure vorm is gegeven:

“Het lid van de PSP-fractie vroeg of indien geen recht op kennisneming kan worden verleend, er toegang tot de rechter is. Dit is inderdaad het geval. Art. 34, vierde lid, van de Wet persoonsregistraties, dat blijkens art. 23 van het onderhavige wetsvoorstel van overeenkomstige toepassing is, opent de mogelijkheid dat de rechter de Registratiekamer in dat geval om advies vraagt. De Registratiekamer kan alsdan de betreffende gegevens bezien en haar oordeel geven. De rechter kan dan ook toetsen of de beheerder terecht het verzoek om kennisneming heeft geweigerd.”³⁷⁰

De rechtbank overweegt vervolgens dat uit het citaat op te maken lijkt dat de rechter bij de beoordeling van het verzoekschrift dient te varen op het uitgebrachte advies van het CBP, hoewel dit niet expliciet door de wetgever is overwogen. Volgens de rechtbank is er sprake van een omissie in de regelgeving, nu er een speciale procedure bij de rechtbank in het leven is geroepen waarbij deze de beoordeling van het kennisnemingsverzoek moet toetsen. Het is volgens haar dan ook niet de bedoeling van de wetgever om kennisneming van de betreffende gegevens aan de rechtbank te onthouden. De rechtbank verzoekt de korpsbeheerder de betreffende gegevens over te leggen, waarbij zij opmerkt dat zij ingevolge art. 30 Wpolr (de geheimhoudingsbepaling), deze gegevens niet aan de verzoeker mag verstrekken. Deze gang van zaken is door het gerechtshof 's-Hertogenbosch bevestigd, waarbij het hof overigens uiteindelijk – na zelfstandige kennisneming van de betreffende gegevens – tot het oordeel is gekomen dat het kennisnemingsverzoek terecht was geweigerd.³⁷¹

Een zelfde koers lijkt het gerechtshof 's-Gravenhage (2008) te varen. Zonder veel woorden vuil te maken aan de hier aangesneden problematiek bepaalt zij dat de korpsbeheerder een afschrift van de in geschil zijnde persoonsgegevens aan het hof dient over te leggen, voorzien van een toelichting waarom kennisneming geweigerd dient te worden.³⁷² Ten slotte blijkt uit de uitspraak dat de verzoeker heeft ingestemd met de omstandigheid dat de rechter kennis heeft genomen van de betreffende gegevens zonder dat hij daar zelf kennis van heeft kunnen nemen. Dat de verzoeker in het kader van de verzoekschriftprocedure geen inzicht krijgt in de gegevens waarvan de kennisneming in geschil is, spreekt voor zichzelf, omdat anders het kennisnemingsrecht door het enkel instellen van een dergelijke procedure feitelijk zou kunnen worden afgedwongen.

³⁷⁰ *Kamerstukken II*, 1988/89, 19 589, nr. 11.

³⁷¹ Gerechtshof 's-Hertogenbosch, 8 mei 1998, gerechtshof 's-Hertogenbosch, 10 juni 1998, NJ 1999/706.

³⁷² Gerechtshof 's-Gravenhage, 19 juni 2008, LJN BD5187.

Eigenhandige kennisneming van de in geschil zijnde gegevens door de rechter die over het weigeringsbesluit moet oordelen is echter geen gemeengoed. De rechtbank Arnhem heeft in 2001³⁷³ namelijk geoordeeld dat kennisneming van de betreffende gegevens niet noodzakelijk is om een oordeel te geven over de rechtmatigheid van de weigering tot kennisneming door de verzoeker. Daartoe heeft de rechtbank overwogen dat het systeem van de wet met zich meebrengt dat zij in hoge mate moet afgaan op het advies van de Registratiekamer, die wel van de betreffende gegevens kennis kan nemen. Nu door verzoeker onvoldoende klemmende feiten en omstandigheden zijn gesteld waarom van dat advies zou moeten worden afgeweken, gaat de rechtbank mee in het oordeel van de Registratiekamer en wijst het verzoek tot kennisneming af.

Overigens blijkt dat de politie er in het algemeen geen probleem mee heeft om de rechters die over een dergelijke zaak moeten oordelen op het politiebureau inzage te geven in de betreffende gegevens.³⁷⁴

5.2.3 Verschil in procedures

Ten slotte wekt het in de praktijk verbazing dat bij de invoering van de Wbp de relevante bepalingen van de Algemene wet bestuursrecht (Awb) van toepassing zijn verklaard en dat in de Wpolr de verzoekschriftprocedure als beroepsmogelijkheid is blijven bestaan.³⁷⁵ Overigens wordt daarbij niet gesteld dat de ene procedure de voorkeur geniet boven de andere procedure. Voorts past de rechtbank, om zelf kennis te nemen van de betreffende gegevens, art. 8:29 Awb naar analogie toe.³⁷⁶ Het CBP heeft in 2003 er op aangedrongen dat de rechterlijk macht in dergelijke gevallen toegang dient te krijgen tot de gegevens waarop het verzoekschrift van de betrokkene betrekking heeft. Daarbij kan volgens het CBP aansluiting worden gezocht bij de regeling die in de Awb is opgenomen.³⁷⁷

WOB-verzoeken

In het verleden is diverse keren geprobeerd via de Wet openbaarheid van bestuur kennis te nemen van de gegevens die de politie geregistreerd heeft. Reeds in 1987, nog voor de invoering van de Wpolr, werd via die weg een inzagerecht voor de betrokkene afgedwongen.³⁷⁸ Nadien is ten aanzien van WOB-verzoeken bepaald dat daar waar de Wpolr van toepassing is de verzo-

373 Rechtbank Arnhem, 8 mei 2001, NJ 2001/503.

374 Schreuders e.a., 2005, p. 163.

375 Schreuders e.a., 2005, p. 163.

376 Rechtbank Maastricht 31 oktober 1996, rechtbank Maastricht 20 februari 1997 NJ 1997/26, Rechtbank Maastricht 13 november 1997 NJ 1997/103.

377 Cbp, 31 oktober 2003, z2003-1023.

378 ABRvS 30 september 1985, AB 1987/343.

ken op basis daarvan dienen te worden afgedaan en niet op basis van de bepaling uit de WOB, ook als de gegevens in één document zijn opgenomen.³⁷⁹

5.3 UITWERKING ONDER DE WPOLG

Het kennisnemingsrecht heeft onder de Wpolg zijn belangrijke positie gekregen en vervolgens als waarborg behouden. Daarbij is volgens de memorie van toelichting nauw aangesloten bij de regeling onder de Wet politieregisters.³⁸⁰ Hieronder beschrijven we in hoeverre de Wpolg tegemoet komt aan de knelpunten die onder het regime van de Wpolr zijn geconstateerd. Onder de Wpolg zijn naar onze mening geen nieuwe knelpunten te verwachten bij de uitvoering van het kennisnemingsrecht, zodat dit punt hier onbesproken blijft.

Oude knelpunten aangepakt

In art. 25 Wpolg is bepaald dat de korpschef binnen zes weken op een kennisnemingsverzoek dient te beslissen. Daarbij is tevens bepaald dat hij deze beslissing kan verdagen voor een termijn van vier weken en met een termijn van zes weken als er ook gegevens van andere korpsen bij betrokken zijn. De wetgever geeft aan dat met name de kennisnemingsverzoeken bij de CIE tijdrovend kunnen zijn, onder meer omdat veel gegevens over een persoon aanwezig kunnen zijn en omdat meerdere regio's bij een kennisnemingsverzoek betrokken kunnen zijn. De wetgever sluit zich dan ook aan bij het voorstel vanuit de handleiding om voor de coördinatie van de kennisnemingsverzoeken een gezamenlijk systeem op te zetten.³⁸¹ Hoewel de wetgever stelt geen inzicht te hebben in de kwalitatieve werkbelasting voor de CIE in de afwikkeling van de kennisnemingsverzoeken worden vanwege deze praktische zaken de beslissingstermijnen ten opzichte van zowel de Wpolr als de Wbp tegenwoordig iets ruimer gesteld. In het tweede lid van art. 25 Wpolg is bepaald dat in het besluit nadere regels kunnen worden gesteld over de wijze waarop het verzoek wordt gedaan en over het verzoek zelf. Het stellen van nadere regels is, met uitzondering van een regeling over de kosten van het verzoek, tot nu toe niet gedaan.

Naast bepalingen omtrent de bij de afwikkeling van het kennisnemingsverzoek in acht te nemen formaliteiten (vaststelling identiteit en dergelijke) bevat art. 27 Wpolg drie mogelijkheden tot weigering van het kennisnemingsverzoek. Het gaat om (1) de goede uitvoering van de politietaak, (2) de gewichtige belangen van derden, en (3) de veiligheid van de staat. Voor de uitleg van het begrip 'goede uitvoering van de politietaak' verwijst de wetgever naar hetgeen daarover in de Wpolr is bepaald. Daarbij wordt wel opgemerkt dat verzoeken die tot doel hebben de politieorganisatie 'te belas-

379 ABRvS 11 februari 2004, AB 2004/153, ABRvS 29 november 2006, AB 2007/24.

380 *Kamerstukken II*, 2005-06, 30 327, nr. 3, p. 83.

381 *Kamerstukken II*, 2005-06, 30 327, nr. 3, p. 84.

ten' ook op deze grond kunnen worden afgewezen. Met de weigeringsgrond 'de gewichtige belangen van derden' wordt volgens de memorie vooral gedoeld op de bescherming van informanten en infiltranten.³⁸²

De Wpolg heeft het besluit op een kennisnemingsverzoek van de betrokkene aangemerkt als een besluit in de zin van de Awb. Nu de bepalingen omtrent het bezwaar van afdeling 7.1 van de Awb zijn uitgesloten, staat tegen een beslissing beroep bij de bestuursrechter open. Praktisch gezien betekent het dat de verzoeker, indien hij het niet eens is met het besluit dat op zijn kennisnemingsverzoek is genomen, de bestuursrechter over zijn verzoek kan laten oordelen zoals dat onder de Wpolr door de burgerlijke rechter gebeurt. Daarmee is de procedure gelijkgetrokken met die onder de Wbp en is de wetgever tegemoet gekomen aan de daartoe strekkende geluiden vanuit de politiepraktijk, het CBP, en de rechter.

Daarnaast zijn de artt. 47 en 48 van de Wbp van overeenkomstige toepassing verklaard. Hierin is een regeling opgenomen over de mogelijkheid van bemiddeling zoals we die ook onder de Wpolr kenden.

5.4 TUSSENCONCLUSIE

Alvorens we onze tussenconclusie aangaande het kennisnemingsrecht formuleren, geven we schematisch weer (a) het aantal onder de Wpolr geconstateerde knelpunten, (b) de inhoud van die knelpunten, (c) de uitwerking daarvan onder de Wpolg, en (d) de (te verwachten) resultaten van de uitwerking onder de Wpolg.

Aantal	Knelpunten Wpolr	Wpolg	Resultaat
1	(Beperkt) aantal verzoeken	Geen veranderingen	'Knelpunt' niet opgelost
2	Capaciteitsproblemen in afwikkeling	Voor de weigering van verzoeken is aansluiting gezocht bij het systeem van de Wpolr	Knelpunt slechts gedeeltelijk opgelost doordat in belangrijke mate aansluiting is gezocht bij het systeem van de Wpolr
a	<i>Fishing expeditions</i>	(a) moeten afgewezen worden	
b	Korte beslistermijnen	(b) iets langere termijnen	
3	Geen verstrekking aan rechters mogelijk	Verstrekkingsmogelijkheid opgenomen	Knelpunt opgelost
4	Verskil in rechtsprocedure tussen verzoek op grond van Wbp en Wpolr	Rechtsprocedure Wpolr gelijk geworden met procedure onder Wbp	Knelpunt opgelost
5	Bemiddeling door CBP weinig gebruikt	Geen specifieke maatregel opgenomen	'Knelpunt' niet opgelost

Figuur 5.1 Schematisch weergave knelpunt 'kennisnemingsrecht'.

382 Kamerstukken II, 2005-06, 30 327, nr. 3, p. 85.

De geconstateerde knelpunten kunnen worden onderverdeeld in (1) knelpunten die de politie ervaart bij de afhandeling van kennisnemingsverzoeken en (2) knelpunten die bestaan bij de instanties die controle en toezicht daarop houden. We behandelen beide categorieën hieronder.

Ad (1) Knelpunten politie

Wat de knelpunten betreft die bij de CIE-en zijn geconstateerd in de afwikkeling van de kennisnemingsverzoeken gaat het om (a) het relatief geringe aantal verzoeken en (b) de hoeveelheid werk die de verzoeken met zich meebrengen. Wij hebben aangetoond dat beide knelpunten door de wetgeving niet zijn opgelost. Ook onder de Wpolg zullen de CIE-en zich geconfronteerd zien met kennisnemingsverzoeken die ze veel tijd zullen gaan kosten.

Ad (2) Knelpunten toezichthouders

Wat de geconstateerde knelpunten betreft blijft de Wpolg een verbetering aangaande de controle en het toezicht op de afhandeling van de kennisnemingsverzoeken. De twee knelpunten (3 en 4 in figuur 5.1) in de rechterlijke controle zijn beide opgelost. Er is voorzien in een verstrekkingsmogelijkheid voor de rechterlijke macht en daarnaast is in de systematiek van dit type controle aansluiting gezocht bij het systeem van de Wbp. Ten aanzien van het knelpunt dat bij de bemiddeling door het CBP is geconstateerd, biedt de Wpolg geen oplossing en daarmee is onze verwachting dat dit knelpunt zal blijven bestaan.

Het is al met al ook de vraag of de knelpunten die door de Wpolg niet zijn opgelost aan te pakken zijn met wetgeving of dat deze knelpunten inherent verbonden zijn aan het instrument van het kennisnemingsrecht. Het stellen van deze vraag leidt tot het discussiepunt of we in het systeem van waarborgen op het gebruik van persoonsgegevens een zodanige waarde aan het kennisnemingsrecht moeten toekennen als die daar thans aan gegeven wordt. In de navolgende sectie bespreken we dit verder.

5.5 HET KENNISNEMINGSRECHT TER DISCUSSIE

De in de vorige sectie geconstateerde knelpunten bevinden zich met name aan de uitvoeringskant bij de CIE-en. Het gaat om praktische problemen bij de uitvoering van het kennisnemingsrecht die voortkomen uit de volgende twee belangen: (1) de CIE probeert heimelijk informatie over personen en groepen te verzamelen en (2) de crimineel wil graag weten wat de politie over hem weet. Deze twee belangen die lijnrecht tegenover elkaar staan, maken dat niet zonder meer alle bij de CIE aanwezige informatie kan worden verstrekt aan de persoon die om inzage verzoekt. Daar moet, in verband met de goede uitvoering van de politietaak, eerst een selectie in gemaakt worden. Dit zorgt ervoor dat het recht op kennisneming van informatie uit

de CIE-databanken een vrijwel onmogelijke taak is. Dit is niet alleen een conclusie die volgt uit de praktijk van alle dag, maar ook een conclusie die naar voren komt uit de handleiding. Zoals gezien in sectie 5.2 komt alleen de 11-informatie in beginsel voor kennisneming in aanmerking. Dit uitgangspunt is bevestigd door de rechtbank 's-Gravenhage, die van oordeel is dat kennisneming van de in de CIE-registers geregistreerde gegevens in beginsel niet is toegestaan.³⁸³

Aan dit uitgangspunt ligt naar ons idee de volgende gedachte ten grondslag. Een gegeven mag zich alleen in een register bevinden indien dit noodzakelijk is voor de goede uitvoering van de politietaak. Als dit niet het geval is, moet het gegeven namelijk verwijderd worden overeenkomstig hetgeen in subsectie 4.6.3 is behandeld. De registratie is dus bij de CIE nodig om inzicht te verkrijgen in de zware criminaliteit en de rol van de geregistreerde daarbij. Door die betreffende persoon daarvan op de hoogte te stellen geeft de CIE informatie prijs die afbreuk doet aan haar eigen taak. De verzoeker weet op dat moment immers dat hij of zij geregistreerd staat bij de CIE en zal daar in zijn doen en laten rekening mee houden en daar mogelijk ook anderen van op de hoogte stellen. Daar is de informatiepositie van de CIE in beginsel niet mee gediend. De geregistreerde zal immers op zijn tellen passen en zich op zijn minst een keer extra bedenken voordat hij een derde (een mogelijke informant van de CIE) iets zal vertellen over zijn criminele activiteiten. Zo bezien doet elke verstrekking afbreuk aan de informatiepositie en derhalve ook aan de goede taakuitvoering door de CIE. Daarmee kan elk kennisnemingsverzoek worden geweigerd, met uitzondering van de reeds genoemde 11-informatie.

Het voorgaande is wellicht wat kort door de bocht, maar het maakt duidelijk dat het kennisnemingsrecht slechts toepasbaar is op een klein deel van de informatie die de CIE heeft. 11-informatie is veelal informatie die toch al bekend is of waarvan openbare bekendheid geen afbreukrisico met zich meebrengt. Het brengt de vraag met zich mee of het beperkte recht op kennisneming, afgezet tegen de inzet van politiemanuren, rendabel moet worden geacht. Met rendabel bedoelen we dat onderzocht moet worden of de rechtsbescherming die het kennisnemingsrecht op informatie in de CIE-databanken biedt door die inzet gerechtvaardigd wordt. Wij betogen hier van niet.

De inzage van een betrokkene beperkt is tot 11-informatie. Dit betekent dat de meeste informatie in de CIE-databanken te allen tijde voor hem gesloten blijft en kennisneming geweigerd zal worden. Daarmee is de volgende conclusie onvermijdelijk. Weliswaar wekt het kennisnemingsrecht de indruk een rechtsbeschermend middel te zijn, maar we moeten concluderen dat het dit effectief gezien niet is. Immers, een groot deel van de informatie blijft voor de betrokkene afgesloten.

383 Rechtbank 's-Gravenhage, 5 juni 2008 (niet gepubliceerd).

Daarin verschilt het recht op kennisneming op een essentieel punt van datzelfde recht onder de Wbp. Onder de Wbp gaat het om een gelijkwaardige situatie tussen beide partijen. Een goed voorbeeld is te zien in de relatie tussen patiënt en arts, waarbij de patiënt vrijwillig gegevens aan de arts verstrekt. De arts heeft – jegens die patiënt – geen enkele reden die gegevens geheim te houden. In deze situatie is een kennisnemingsrecht volstrekt logisch. Het gaat over de patiënt, deze kan alle gegevens zien en kan op basis daarvan met de arts in discussie of wat geregistreerd is ook terecht is geregistreerd.

Doordat in het geval van kennisneming bij de CIE een groot deel van de informatie geheim blijft, is het voeren van een discussie over het al dan niet terecht geregistreerd hebben van een deel van die informatie niet goed mogelijk. Bovendien is het, anders dan bij de patiënt – arts relatie, niet aan de geregistreerde om te bepalen wat wordt geregistreerd, of dat terecht is, of het mag en of hij zaken verwijderd wenst te zien. Juist bij de CIE is dat alles voortdurend onderwerp van onderzoek. Het is aan de professionaliteit van de CIE om te bepalen wat er geregistreerd dient te worden en waarvan inzage kan worden verleend bij een kennisnemingsverzoek.

5.5.1 Zelfreinigend vermogen

Alles overziend, kunnen we stellen dat het volgende overblijft: de CIE wordt gedwongen door een kennisnemingsverzoek alle aanwezige informatie (dus niet alleen 11-informatie) te doorlopen en te beoordelen of die informatie verstrekt kan worden. We kunnen stellen dat daarvan een zelfreinigend effect verwacht mag worden. Het is gelet op de houding van de CIE tegenover het kennisnemingsrecht echter de vraag of de CIE in die constellatie daar veel waarde aan zal toekennen. Bezien we dit samen met het relatief geringe aantal verzoeken dat wordt gedaan, dan rechtvaardigt dat naar onze mening de inzet van de mankracht van de CIE niet. Wat er van deze argumentatie overblijft als we het aantal verzoeken toeneemt is niet duidelijk. Dan zal naar andere (technische) mogelijkheden omgezien dienen te worden.

Op dit moment mogen we hier concluderen dat de waarborgende werking van het kennisnemingsrecht te wensen overlaat. Hoewel geldt dat de wijze waarop de inzageverzoeken worden afgehandeld door de CIE in overeenstemming met de toepasselijke regelgeving is, draagt het recht op inzage als gevolg van het geringe aantal en de wijze waarop die afgedaan worden naar ons idee slechts marginaal bij aan de waarborgende werking.

5.5.2 Mogelijke afschaffing?

Een mogelijke discussie over het bestaansrecht van het kennisnemingsrecht bij de CIE brengt de vraag met zich mee of er een verdragsrechtelijke verplichting bestaat tot het hebben van een dergelijk recht. De memorie spreekt

in dit verband over het in internationale verdragen neergelegde beginsel dat degene over wie persoonsgegevens worden verwerkt door de politie in de gelegenheid wordt gesteld tot kennisneming van die gegevens. Het leidt ertoe dat een ieder in beginsel in de gelegenheid moet zijn om na te kunnen gaan of zijn gegevens worden verwerkt en, zonodig, of deze verwerking in recht aan te vechten is, aldus de wetgever.³⁸⁴ Zoals in hoofdstuk 3 uitgebreid aan de orde is gekomen, kent Nederland geen verdragrechtelijke verplichting om specifieke wettelijke regelingen te hebben voor het verwerken van persoonsgegevens. Sterker nog, er is ons niet bekend dat een recht op kennisneming vanuit 'Europa' verplicht zou zijn.

5.6 BEANTWOORDING OV2 EN OV3 AANGAANDE HET KENNISNEMINGSRECHT

In dit hoofdstuk is de theorie en de praktijk van het kennisnemingsrecht bij de CIE besproken. Daarbij is een antwoord gegeven op OV2 en OV3 voor zover dit het kennisnemingsrecht als waarborg betreft. OV2 luidt: *"Welke knelpunten zijn er in de literatuur en de praktijk geconstateerd ten aanzien van de waarborgende werking van de Wet politieregisters?"* en OV3 luidt *"In hoeverre komt de Wet politiegegevens, mede in het licht van de ervaringen met de Wet bescherming persoonsgegevens, tegemoet aan deze knelpunten?"* In dit hoofdstuk hebben we beschreven op welke wijze de Wpolg tegemoet komt aan de onder de Wpolr geconstateerde knelpunten. In deze hoofdstukconclusie herhalen we niet alle geconstateerde individuele knelpunten, maar abstraheren we deze tot een hoger niveau, waarbij de discussie over het bestaansrecht van het kennisnemingsrecht leidend is.

We hebben laten zien dat de Wpolg niet aan alle knelpunten tegemoet komt en dat dit zijn oorzaak vindt in een fundamentele botsing tussen het recht op kennisneming enerzijds en de taakuitvoering van de CIE anderzijds. Dit is een knelpunt dat door nieuwe wetgeving niet op te lossen is. Wel heeft de Wpolg een aantal procedurele knelpunten weggenomen en vormt het daarmee zeker een verbetering ten opzichte van de Wpolr. Op grond van onze analyse mogen wij het volgende concluderen. In de waarborgende werking die van de wetgeving uit dient te gaan moet echter – zo stellen wij – ook onder de Wpolg niet veel van het kennisnemingsrecht worden verwacht. In ieder geval moet aan het kennisnemingsrecht niet de waarde worden toegekend die de wetgever daaraan geeft door het één van de drie waarborgen te maken die de politietaak en de vrijheid van gegevens moeten beschermen.

Net als bij de eerste waarborg, het wettelijk systeem zoals dat in hoofdstuk 4 is behandeld, leidt het gebrek aan waarborgende werking van het kennisnemingsrecht tot de conclusie dat daardoor meer moet worden verwacht van de derde en laatste waarborg, controle en toezicht.

384 Kamerstukken II, 2005/06, 30 327, nr. 3, p. 83.

De derde en laatste waarborg is controle en toezicht op politieke gegevensverwerking. Er zijn verschillende personen en instanties die belast zijn met controle en toezicht op de wijze waarop de CIE persoonsgegevens verwerkt. In dit hoofdstuk behandelen we de tweede en derde onderzoeksvraag met betrekking tot controle en toezicht. OV2 luidt: *“Welke knelpunten zijn er in de literatuur en de praktijk geconstateerd ten aanzien van de waarborgende werking van de Wet politieregisters?”* en OV3 luidt: *“In hoeverre komt de Wet politiegegevens, mede in het licht van de ervaringen met de Wet bescherming persoonsgegevens, tegemoet aan deze knelpunten?”* Dit hoofdstuk is gebaseerd op drie wettelijke regelingen: de Wpolr, de Wpolg, en de Wbp. Het gaat over de wijze waarop de Wpolr en Wpolg vorm geven aan de waarborg controle en toezicht. We onderzoeken de knelpunten die zich in de uitvoering hiervan voordoen onder het regime van de Wpolr en de oplossingen die de Wpolg voor deze knelpunten biedt. Dit doen we in het licht van de ervaringen die met de Wbp zijn opgedaan.

In ons onderzoek houden wij op een wetenschappelijk verantwoorde wijze rekening met de verschillende doelstellingen en de wijze van regulering in de drie wettelijke regelingen (zoals beschreven in sectie 4.1 en 4.2). In sectie 6.1 behandelen we de controle en toezichtmechanismen die in de wet zijn opgenomen en die uit de rechtsstatelijke verhouding tussen partijen voortvloeien. In sectie 6.2 beschrijven wij het theoretische kader. Het gaat daar om (1) de verantwoordelijke, (2) de privacyfunctionaris, (3) het CBP, (4) protocollering en auditing, (5) de CIE-officier van justitie en (6) de strafrechter. In de secties 6.3 tot en met 6.7 behandelen we elk van deze mechanismen afzonderlijk. Naar aanleiding hiervan beantwoorden wij in sectie 6.8 OV2 en OV3 aangaande controle en toezicht en geven we een hoofdstukconclusie.

6.1 CONTROLE- EN TOEZICHTMECHANISMEN UIT DE WPOLR

In de Wpolg zijn een aantal bepalingen opgenomen die de controle en het toezicht op de verwerking van persoonsgegevens door de CIE reguleren. Het

385 Een deel van dit hoofdstuk is reeds gepubliceerd: Kielman en Koelewijn, 2006. De auteur bedankt hierbij zijn co-auteur en de uitgever van het tijdschrift Privacy en Informatie voor hun toestemming om relevante gedeelten van het artikel in dit proefschrift te mogen hergebruiken.

aantal en soort mechanismen die hiervoor zijn ingesteld zijn goed vergelijkbaar met het relevante regime onder de Wpolr. Wel zijn onder de Wpolg in de wijze waarop deze mechanismen kunnen worden ingezet, of in sommige gevallen zelfs móeten worden ingezet, veranderingen doorgevoerd. De controle- en toezichtsmechanismen die in de Wpolg (en in de Wpolr) en de daaronder liggende lagere regelingen³⁸⁶ expliciet zijn opgenomen, duiden we aan met wettelijke controle- en toezichtsmechanismen. Wij duiden vier van deze mechanismen. Het gaat achtereenvolgens om (1) de verantwoordelijke, (2) de privacyfunctionaris, (3) het CBP en (4) protocollering en auditing.

Daarnaast zijn er twee mechanismen van controle en toezicht die niet expliciet in de wet zijn opgenomen, maar die voortvloeien uit de wijze waarop we de politieorganisatie als uitvoerende macht hebben ingekleed als een van de drie machten van de trias politica. De andere twee machten zijn de wetgevende en de rechtsprekende. De wetgevende macht is in hoofdstuk 4, waar de wet als waarborg is behandeld, uitgebreid aan de orde gekomen. De rol van de rechtsprekende macht is dat – met uitzondering van haar rol bij de uitvoering van het kennisnemingsrecht in hoofdstuk 5 – echter nog niet. In de verhouding van de trias politica is het bij uitstek de rol van de rechtsprekende macht om de uitvoerende macht te controleren in de wijze waarop zij de wet uitvoert. De rol van de rechtsprekende macht kan in dit hoofdstuk dan ook niet ontbreken. Als onderdeel van de rechtsprekende macht merken we hier aan (1) de officier van justitie en (2) de strafrechter.

Ad (1) controle door de officier van justitie

Ten aanzien van de rol van de officier van justitie merken we op dat het Nederlandse systeem aangaande de rechterlijke macht zo ingericht is dat ook de officier van justitie daar onderdeel van uitmaakt. Dat brengt met zich mee dat de officier van justitie een magistraat is en vanuit die rol dus ook een controlerende taak heeft op de wijze waarop de politie met haar bevoegdheden omgaat. In ons onderzoek zal de nadruk liggen op de CIE-officier van justitie.

Ad (2) strafrechterlijke controle

Wat betreft de strafrechter behoeft het geen betoog dat deze middels het strafproces, waar individuele zaken worden behandeld, toezicht houdt op de wijze waarop de politie omgaat met haar bevoegdheden. De bestuursrechter en civiele rechter worden hier buiten beschouwing gelaten, omdat zij zich, behoudens de gevallen inzake het kennisnemingsrecht, niet over het verwerken van politiegegevens uitlaten.

In dit hoofdstuk behandelen we elk van bovenstaande controle- en toezichtmechanismen achtereenvolgens. Het gaat dan om de wettelijke mechanismen zoals die voortvloeien uit de rechtsstatelijke verhouding tussen de ver-

386 Denk daarbij bijvoorbeeld aan het Besluit politiegegevens en aan de modelreglementen zoals deze onder de Wpolr golden.

schillende betrokkenen. Dit zijn achtereenvolgens: (1) de verantwoordelijke, (2) de privacyfunctionaris, (3) het CBP, (4) protocollering en auditing, (5) de CIE-officier van justitie en (6) de strafrechter. Deze mechanismen zijn onderwerp van respectievelijk de subsecties 6.2, 6.3, 6.4, 6.5, 6.6 en 6.7.

6.2 DE BEHEERDER

De eerst aangewezen om controle en toezicht te houden op gegevensverwerking door de CIE is degene die daar onder de Wpolg ook verantwoordelijk voor is gesteld. In het gegevensbeschermingsrecht wordt dit aangeduid met 'de verantwoordelijke'. Het gaat dan blijkens art. 1 onder f van de Wpolg om:

- bij een regionaal politiekorps: de korpsbeheerder, zijnde de burgemeester;
- bij het Korps landelijke politiediensten: onze minister van Binnenlandse Zaken en Koninkrijksrelaties;
- bij de rijksrecherche: het College van procureurs-generaal;
- bij de Koninklijke marechaussee: onze minister van Defensie.

Onder de werking van de Wpolr was deze indeling hetzelfde, maar werd gesproken over een beheerder in plaats van een verantwoordelijke.³⁸⁷

We bespreken achtereenvolgens het theoretisch kader dat hierop van toepassing is onder de Wpolr (subsectie 6.2.1), de daarbij geconstateerde knelpunten (subsectie 6.2.2.), de uitwerking van de rol van de verantwoordelijke onder de Wpolg (subsectie 6.2.3) en eindigen met een tussenconclusie (subsectie 6.2.4).

6.2.1 Theoretisch kader

In de Wpolr zijn tal van verplichtingen aan de beheerder van de politieregisters toebedeeld. Kort gezegd had de beheerder de algehele verplichting om te zorgen dat de politieregisters in zijn regio overeenkomstig de daarop van toepassing zijnde regelingen werden gevoerd. Gelet op de hoeveelheid politieregisters die bij een gemiddeld politiekorps gebruikt werden, was dat een verantwoordelijkheid die veel werk met zich meebracht. Het ging onder de Wpolr om vrij algemene bevoegdheden en verplichtingen die over het algemeen niet concreet waren uitgewerkt.

Als hoofdverplichting was in art. 4, derde lid Wpolr neergelegd dat de beheerder de nodige voorzieningen treft ter bevordering van de juistheid en de volledigheid van de opgenomen persoonsgegevens. Deze verplichting was vervolgens uitgewerkt in art. 7 van de Wpolr waar in het tweede lid was bepaald dat hij zorg draagt voor de nodige voorzieningen van technische en

387 Art. 1 lid 1 onder f Wpolr.

organisatorische aard ter beveiliging van het register tegen verlies of aantasting van de gegevens en tegen onbevoegde kennisneming, wijziging of verstrekking daarvan. In het eerste lid van art. 7 Wpolr was voorts bepaald dat hij zorg draagt voor de juiste werking van het register en dat hem daartoe alle inlichtingen worden verstrekt die hij nodig heeft.

Een van de weinige concrete verplichtingen van de beheerder was de in art. 9 Wpolr neergelegde verplichting voor ieder register een reglement op te stellen en een afschrift daarvan aan het CBP te zenden. Ook in verband met het kennisnemingsrecht had de beheerder een aantal concrete verplichtingen, zoals we in hoofdstuk 5 hebben beschreven.

De beheerder was voorts civielrechtelijk aansprakelijk voor de schade die een derde leed als gevolg van een overtreding van de regels en normen uit de Wpolr. Deze verantwoordelijkheid is neergelegd in de artt. 49, eerste tot en met derde lid, en art. 50, eerste lid, van de Wet bescherming persoonsgegevens. Deze artikelliden uit de Wbp waren van overeenkomstige toepassing verklaard op de beheerder van een politieregister. Art. 50 lid 1 Wbp bepaalt dat de rechter de beheerder bepaald gedrag kon verbieden en hem kon bevelen maatregelen te treffen tot herstel van de gevolgen van dat gedrag.

Naast de wettelijke regeling werd in de circulaire Toezicht op beheer bijzondere politieregisters een handreiking gegeven aan de beheerders van de registers bij de CIE-en om adequaat toezicht te houden op de kwaliteit van de gegevensverwerking.³⁸⁸ De circulaire, die op 14 maart 2002 voor een periode van vier jaar in werking was getreden, had betrekking op een zelfevaluatie middels een bijgevoegde vragenlijst en een besprekingsverslag daarvan met de korpsleiding en de CIE-officier van justitie. De zelfevaluatie diende overeenkomstig de circulaire iedere twee jaar plaats te vinden.

6.2.2 De knelpunten beschreven

Uit de hoeveelheid registers waarover de beheerder van een politieregio verantwoordelijkheid had was reeds duidelijk dat deze verantwoordelijkheid niet de dagelijkse controle verrichte en toezicht had. Daartoe werd gebruik gemaakt van mandatering, wat inhield dat in geval van de CIE het hoofd CIE deze taken voor de beheerder waarnam, namens die beheerder. Dat betekende wel dat formeel gezien de verantwoordelijkheid bij de beheerder bleef liggen. Ook voornoemde circulaire ging van een dergelijke mandatering uit.

In de uitoefening van deze taken was het hoofd van de CIE dagelijks verantwoordelijke voor de wijze waarop informatie door de CIE werd verwerkt. Dat gebeurde in de praktijk intensief, zowel bij de opslag van de bruto-informatie (het gespreksverslag van het gesprek met de informant) als bij de overheveling van de bruto-informatie naar het zwacri-register, waarin de netto-informatie werd opgenomen. De verstrekkingen die naar buiten de CIE

388 Circulaire Toezicht op beheer bijzondere politieregisters, *Stcrt*, 13 maart 2002, nr. 51, p. 10.

gingen werden blijkens het onderzoek van Kielman en Koelewijn inderdaad allemaal langs het hoofd van de CIE geleid. Dat maakte dat het hoofd van de CIE bij iedere belangrijke stap in het informatieproces binnen de CIE zijn invloed kon laten voelen. Uit het WODC-evaluatieonderzoek bleek evenwel dat capaciteitsgebrek het grootste gebrek opleverde in de uitvoering van deze taken.³⁸⁹ Een gebrek aan tijd zorgde ervoor dat CIE-en niet in staat waren de in de registers opgenomen informatie op hun rechtmatigheid te beoordelen. Ongeveer de helft van de CIE-en heeft aangegeven bij de vertaling van de informatie van bruto naar netto (praktisch gezien van het informantenregister naar het zwacri-register) niet in staat te zijn controle op deze informatie uit te voeren. Pas op het moment dat de informatie uit het zwacri-register moest worden verstrekt werd deze controle alsnog gedaan. Een derde van de CIE-en heeft aangegeven dat ook bij de opslag van de bruto-informatie de capaciteit eraan in de weg staat de controle op rechtmatigheid uit te voeren. Daarnaast verdient ook hier opmerking dat, zoals reeds in hoofdstuk 4 uitgebreid aan de orde is gekomen, de toepasselijke regelgeving als complex wordt ervaren en het hoofd van de CIE de toepassing daarvan lastig vindt.

Het hoofd van de CIE is verantwoording aan de beheerder verschuldigd voor de wijze waarop namens hem het beheer van de registers wordt gevoerd. Dat gebeurt in de meerderheid van de regio's door het opstellen van periodiek verslag door het hoofd van de CIE. In de helft van de gevallen was de inhoud van de rapportage beperkt tot een kwantitatieve verantwoording over de hoeveelheid verstrekte processen-verbaal en de uitbetaalde tipgelden. De andere helft bevatte ook een meer kwalitatieve verantwoording op het gebied van de wijze waarop de CIE informatie verwerkt. Op deze wijze kan de beheerder dus indirect zijn invloed laten voelen. Ook in het zogenaamde driehoeksoverleg (overleg tussen de burgemeester, politie en openbaar ministerie) worden deze jaarverslagen besproken. We kunnen hier echter constateren dat deze wijze van verantwoording afleggen aan de leidinggevende organen nog niet optimaal gebeurt. Voor een beheerder is die verantwoording vanzelfsprekend onontbeerlijk om zijn rol als formeel verantwoordelijke waar te kunnen maken. Dat dit in sommige gevallen helemaal niet gebeurt of slechts op kwantitatief niveau is om die reden aan te merken als knelpunt.

Ten aanzien van de civielrechtelijke aansprakelijkheid van de verantwoordelijke is ons niet bekend dat daar in de praktijk al een keer vorm aan gegeven is door een aansprakelijkheidsstelling van een verantwoordelijke door een derde.

Als het gaat om de bij circulaire voorgeschreven zelfevaluatie is ons alleen uit het WODC-evaluatieonderzoek bekend dat deze in de periode van maart 2002 tot maart 2003 uitgevoerd zijn door de CIE-en. De uitkomsten daarvan waren echter alleen bedoeld voor intern gebruik, maar zijn in geanonimiseer-

389 Schreuders e.a., 2005, p. 144-145.

de vorm wel gebruikt voor het WODC-evaluatieonderzoek.³⁹⁰ Blijkens het evaluatieonderzoek heeft de zelfevaluatie bijgedragen aan het zelfbewustzijn, doordat dit heeft geresulteerd in de oprichting van de ABRIO-werkgroep die zich op bovenregionaal niveau heeft beziggehouden met de stroomlijning van de werkprocessen bij de CIE. Of de zelfevaluatie na 2003 nog een keer is uitgevoerd, is bij ons niet bekend. De circulaire Toezicht op beheer bijzondere politieregisters is in ieder geval in februari 2006 van rechtswege vervallen en ons is niet van een verlenging of vervanging bekend. De zelfevaluatie lijkt daarmee een stille dood gestorven.

6.2.3 Uitwerking onder de Wpolg

Onder de Wpolg is de beheerder omgedoopt tot de verantwoordelijke. Inhoudelijk treden er niet veel verschillen op in de rol die hij wettelijk gezien vervult ten aanzien van de wijze waarop informatie door de CIE wordt verwerkt. We behandelen hier dan ook alleen de verschillen die in de Wpolg optreden ten opzichte van de Wpolr.

Onder art. 4 van de Wpolg is voor de verantwoordelijke de verplichting opgenomen om ervoor zorg te dragen dat de politiegegevens die verwerkt worden (1) juist en nauwkeurig zijn, (2) op tijd verwijderd worden, en (3) passend beveiligd worden.³⁹¹ Voorts is onder de Wpolg eveneens bepaald dat de verantwoordelijke civielrechtelijk de verantwoordelijkheid draagt voor het voldoen aan de in de Wpolg gestelde eisen.

Daarnaast heeft de verantwoordelijke de verplichting onder de Wpolg om zorg te dragen voor het systeem van autorisaties dat met de komst van de Wpolg is ingevoerd. Art. 6 Wpolg bepaalt dat de verantwoordelijke het systeem van autorisaties onderhoudt naar de eisen van zorgvuldigheid en evenredigheid. Ook de verplichting tot het protocolleren is nieuw onder de Wpolg. We komen daar nader over te spreken in sectie 6.5, waar we het hebben over protocollering en auditing.

Ten slotte verschilt de rol van de verantwoordelijke onder de Wpolg van zijn rol onder de Wpolr doordat de meerderheid van de verstrekkingmogelijkheden van politiegegevens direct aan de verantwoordelijke zijn opgedragen. Dat wil zeggen dat in de Wpolg expliciet is opgenomen dat de verantwoordelijke gegevens verstrekt. Daarmee heeft hij onder de Wpolg niet alleen de algemene verantwoordelijkheid voor – kort gezegd – zorgvuldig gegevensbeheer, maar ook heel specifiek voor iedere afzonderlijke verstrekking. Zijn civielrechtelijke aansprakelijkheid is daarmee dus ook uitgebreid.

³⁹⁰ Schreuders e.a., 2005, p. 53.

³⁹¹ Zie respectievelijk de leden 1, 2 en 3 van art. 4 Wpolg.

6.2.4 Tussenconclusie aangaande de beheerder

Alvorens we onze tussenconclusie aangaande het mechanisme van de controle en het toezicht door de verantwoordelijke formuleren, geven we schematisch weer (a) het aantal onder de Wpolr geconstateerde knelpunten, (b) de inhoud van die knelpunten, (c) de uitwerking daarvan onder de Wpolg en (d) de (te verwachten) resultaten van de uitwerking onder de Wpolg.

Aantal	Knelpunten Wpolr	Wpolg	Resultaat
1	Capaciteitsgebrek in uitvoering controle	–	Knelpunt niet opgelost
2	Schriftelijke verantwoording aan verantwoordelijke schiet tekort	–	Knelpunt niet opgelost

Figuur 6.1 Schematische weergave knelpunten beheerder.

De verplichtingen die aan de verantwoordelijke zijn opgelegd zijn een vrij formele aangelegenheid, aangezien de daadwerkelijke werkzaamheden grotendeels door middel van gemandateerde ondergeschikten worden uitgevoerd. In de uitvoering daarvan zien we dat het hoofd CIE een belangrijke rol vervult, maar de tijd hem eenvoudigweg ontbreekt om daar op zodanige wijze vorm aan te geven zoals van hem verwacht zou mogen worden. Dat is een knelpunt dat niet door de Wpolg wordt opgelost, maar dat kan ook niet van een wettelijke regeling verwacht worden. Het knelpunt is het gevolg van het feit dat de CIE meer informatie verwerkt dan waartoe zij feitelijk is ingericht. Dat is een beleidsmatige keuze, waarvoor de verantwoordelijke uiteindelijk verantwoordelijk is en daar ook op aangesproken kan worden.

Om die beleidsmatige keuze echter gefundeerd te kunnen maken is de verantwoordelijke afhankelijk van de informatie die hij van de CIE ontvangt. En ook daar schiet de praktijk tekort. Soms gebeurt die verantwoording helemaal niet, soms slechts gedeeltelijk. Ook daarvoor biedt de Wpolg geen oplossing en daarmee laat ze een belangrijke mogelijkheid liggen. Doordat de verantwoording van het hoofd CIE niet formeel is vastgelegd, wordt de verantwoordelijke de mogelijkheid ontnomen om feitelijk toezicht te houden. Daarin heeft hij zelf natuurlijk ook een verantwoordelijkheid aangezien hij de verslaglegging ook zelf kan afdwingen bij zijn hoofd-CIE. Dit gebeurt in de praktijk echter kennelijk niet. Een wettelijke plicht daartoe is dan juist de aangewezen manier om zulks te bewerkstelligen.

6.3 DE PRIVACYFUNCTIONARIS

In de politiepraktijk bestaat de functie van privacyfunctionaris. In de praktijk wordt deze persoon ook wel *privacy officer* genoemd. Kort gezegd is dit een persoon binnen de politieorganisatie die een controlerende, toezichthoudende als ook een adviserende rol vervult binnen de eigen politieorganisatie.

We bespreken achtereenvolgens het theoretisch kader van de privacyfunctionaris onder de Wpolr (subsectie 6.3.1), de daarbij geconstateerde knelpunten (subsectie 6.3.2.), de uitwerking van de rol van de privacyfunctionaris onder de Wpolg (subsectie 6.3.3), en eindigen met een tussenconclusie (subsectie 6.3.4).

6.3.1 Theoretisch kader

In de Wpolr waren geen specifieke bepalingen opgenomen over de rol en bevoegdheden van de privacyfunctionaris. Dat geldt evenzeer voor het besluit politieregisters en de verschillende modelreglementen die op de registers bij de CIE van toepassing waren onder het regime van de Wpolr.

6.3.2 De knelpunten beschreven

Opvallend is dat er geen regeling voor de privacyfunctionaris bestaat, terwijl zijn functie er in de praktijk wel is. Dat maakt dus ook dat de invulling van de rol van de privacyfunctionaris niet vastligt en de invulling daarvan per regio verschilt.³⁹² In het algemeen kan gezegd worden dat de privacyfunctionaris in de praktijk één politie-ambtenaar is, die deze functie in zijn takenpakket heeft en daar (een deel van) zijn tijd aan besteedt. Het gaat in veel gevallen niet om een fulltime-functie. Daarnaast is de privacyfunctionaris er natuurlijk niet alleen voor de CIE, maar bedient hij het hele politiekorps waartoe hij behoort. Daaronder vallen ook de gegevensverwerkingen van een politiekorps die onder de werking van de Wbp vallen. De privacyfunctionaris bedient derhalve een zeer breed publiek. Dat beperkt ook zijn mogelijkheden. Illustratief voor de knelpunten die hierdoor veroorzaakt worden is wat ons betreft de uitkomst van een recent onderzoek van het CBP bij infodesks van drie politieregio's.³⁹³ Daaruit bleek onder meer dat de privacyfunctionaris zijn werk onvoldoende invulling gaf, één regio had zelfs helemaal geen privacyfunctionaris.

Vanwege het gebrek van een regeling rond de privacyfunctionaris is de invulling van zijn rol per regio verschillend. In het algemeen kunnen drie taken onderscheiden worden, te weten (1) adviserend, (2) controlerend en (3) administratief. Als het gaat om de adviserende rol moet gedacht worden

392 Schreuders e.a., 2005, p. 147.

393 Het onderzoek van het Cbp betrof infodesk, dat geen onderdeel van de CIE uitmaakt. De uitkomsten van het onderzoek zijn echter illustratief voor de problemen die wij ook ten aanzien van controle en toezicht op de gegevensverwerkingen bij de CIE signaleren. *Verwerking persoonsgegevens door regionale politiekorpsen. Vervolgonderzoek CBP naar functioneren politie infodesks bij het Regionaal politiekorps Brabant Noord, Regionaal politiekorps Amsterdam-Amstelland en Regionaal politiekorps Drenthe*, juli 2009, te downloaden op <http://www.cbweb.nl>.

aan voorlichting over de werking van privacy-wetgeving en de beantwoording van vragen die bij de verschillende ambtenaren van de politie (daaronder dus ook de CIE-ers begrepen) leven. Wat de controlerende functie betreft gaat het om een meer zelfstandige handeling van een privacyfunctionaris die ongevraagd bekijkt of de verwerking van persoonsgegevens in 'zijn' politieregio in overeenstemming met de regelgeving gebeurt. De administratieve functie van de privacyfunctionaris bestaat voornamelijk uit het doen van de verplichte meldingen van gegevensverwerkingen aan het CBP en het afhandelen van inzageverzoeken.

Vanuit de CIE bestaat er weerstand tegen de functie van de privacyfunctionaris. Veel CIE-ers zijn de mening toegedaan dat het werk van de privacyfunctionaris prima gedaan kan worden door de CIE zelf (populair gezegd: de CIE heeft geen pottenkijkers nodig). Vanwege de in hoofdstuk 2 genoemde afbreukrisico's zijn de CIE-ers dan ook vaak niet bereid de voor zijn taakuitoefening benodigde informatie aan een privacyfunctionaris te verschaffen.³⁹⁴ Kenmerkend is de uitspraak van één van de geïnterviewde CIE-ers:

*"Aan hem (privacyfunctionaris – HHK) wordt geen informatie verstrekt, dat is in zijn eigen belang. Kennis van de inhoud kan hem toch alleen maar belasten."*³⁹⁵

De privacyfunctionaris vervult, zoals gezegd, een adviserende en administratieve rol. Daarbij vermijdt de CIE zoveel mogelijk inhoudelijke beslissingen en kennisname van gegevens. Maar er zijn ons ook gevallen bekend waar de privacyfunctionaris niet binnen de vertrekken van de CIE welkom was. Een veel gehoorde reden voor de weerstand is dat de CIE al beschikt over een speciale CIE-ovj die een adviserende rol heeft, ook op het gebied van de verwerking van persoonsgegevens. De toegevoegde waarde van de privacyfunctionaris wordt om deze reden niet gevoeld.³⁹⁶

6.3.3 Uitwerking onder de Wpolg

De taken van de privacyfunctionaris zijn in de Wpolg neergelegd in art. 34 Wpolg. Daarbij is nauwe aansluiting gezocht bij de rol die de privacyfunctionarissen reeds in de praktijk vervulden. In lid 1 van art. 34 Wpolg is de controlerende taak van de privacyfunctionaris neergelegd en is bepaald dat de privacyfunctionaris namens de verantwoordelijke (de korpsbeheerder) toeziet op de verwerking van politiegegevens. Daarnaast voert de privacyfunctionaris volgens die bepaling een aantal administratieve taken uit, zoals het opstellen van een jaarverslag. Het belang van de privacyfunctionaris is, zo

³⁹⁴ Schreuders e.a., 2005, p. 147.

³⁹⁵ Koelewijn, 2009, p. 128.

³⁹⁶ Schreuders e.a., 2005, p. 147.

blijkt uit de memorie van toelichting, in zijn bijzondere deskundigheid op het gebied van het privacyrecht gelegen.³⁹⁷

Over het toezicht dat op deze wijze van de verantwoordelijke gedelegeerd is aan de privacyfunctionaris stelt de wetgever in de memorie van toelichting dat de privacyfunctionaris een belangrijke rol kan vervullen bij het uitvoeren van controle en toezicht. De verantwoordelijkheid daarvoor ligt in eerste instantie bij de korpsbeheerder. De privacyfunctionaris kan volgens de memorie van toelichting daarbij een ondersteunende taak vervullen. Op grond van art. 4 Wpolg dient de verantwoordelijke de nodige maatregelen te treffen om de verwerking van persoonsgegevens in overeenstemming met de wet te laten gebeuren. Hierdoor heeft de privacyfunctionaris toegang tot de voor de uitvoering van zijn taak benodigde gegevensverwerkingen.

Door de wetgever is in de memorie van toelichting expliciet overwogen dat de privacyfunctionaris geen toezichthouder is in de zin van art. 5:11 Awb, maar dat het CBP de toezichthouder is.³⁹⁸ Om die reden heeft de privacyfunctionaris ook geen eigen bevoegdheden gekregen om controle en toezicht uit te voeren op politieke gegevensverwerkingen.

De functionaris gegevensbescherming

De functionaris gegevensbescherming is een nieuw mechanisme in het veld van politieke gegevensverwerking. Naast de verplichte instelling van de privacyfunctionaris kent de Wpolg de mogelijkheid aan iedere politieregio toe om een functionaris gegevensbescherming in te stellen. Deze mogelijkheid is neergelegd in art. 36 Wpolg. Ook is het mogelijk dat alle korpsbeheerders samen één functionaris gegevensbescherming benoemen. Dit artikel bepaalt dat een korpsbeheerder een dergelijke functionaris kan benoemen en dat de artt. 63 en 64 van de Wbp van overeenkomstige toepassing zijn. De functionaris gegevensbescherming is onder de Wbp een reeds bestaande figuur. In de artt. 63 en 64 Wbp is bepaald dat de functionaris gegevensbescherming onafhankelijk van de korpsbeheerder en de politieregio functioneert en daartoe ook in de gelegenheid moet worden gesteld. Om de onafhankelijke positie te waarborgen geniet de functionaris ook een vorm van ontslagbescherming die te vergelijken is met die van een lid van de ondernemingsraad. De functionaris ziet toe op de gegevensverwerkingen die onder verantwoordelijkheid plaatsvinden van de korpsbeheerder die hem heeft benoemd.³⁹⁹ Van zijn bevindingen stelt de functionaris een jaarverslag op en hij kan aanbevelingen doen aan de korpsbeheerder die strekken tot een betere bescherming van de persoonsgegevens. In het laatste geval kan de functionaris, indien er bij hem sprake is van twijfel, overleggen met het CBP.

Ter uitoefening van zijn functie heeft de functionaris gegevensbescherming een aantal bevoegdheden nodig die het houden van toezicht mogelijk

³⁹⁷ *Kamerstukken II*, 1985/86, 19 589, nr. 3, p. 67.

³⁹⁸ *Kamerstukken II*, 2005/06, 30 327, nr. 3, p. 91.

³⁹⁹ Art. 64 lid 1 Wbp.

maken. Daartoe is in art. 64 lid 3 Wbp bepaald dat de functionaris van de korpsbeheerder de beschikking krijgt over bevoegdheden die gelijkwaardig zijn aan de bevoegdheden van een toezichthouder zoals bedoeld in art. 5:11 Awb. Deze bevoegdheden zijn neergelegd in afdeling 5.2 van de Awb. Let wel, daarbij gaat het dus om de bevoegdheden waar die van de functionaris gelijkwaardig aan moeten zijn. Er is dus niet voorgeschreven dat hij dient te beschikken over de bevoegdheden zoals daar voorgeschreven. Kort gezegd komt het erop neer dat de functionaris gegevensbescherming, in het geval van zijn functie bij een politieregio, toegang moet krijgen tot de voor zijn functie benodigde vertrekken en gegevensverzamelingen. Dit betekent met betrekking tot de CIE precies hetzelfde, namelijk dat de functionaris gegevensbescherming toegang dient te krijgen tot de vertrekken van de CIE en de gegevensverzamelingen die zij voeren. In art. 4 lid 5 Wpolg is in ieder geval neergelegd dat alle toezichthouders, dus ook de functionaris gegevensbescherming toegang dienen te krijgen tot de gegevens die zij nodig hebben voor de uitvoering van hun taak.

6.3.4 Tussenconclusie aangaande de privacyfunctionaris

Alvorens we onze tussenconclusie aangaande het controle en toezicht door de privacyfunctionaris formuleren, geven we schematisch weer (a) het aantal onder de Wpolr geconstateerde knelpunten, (b) de inhoud van die knelpunten, (c) de uitwerking daarvan onder de Wpolg, en (d) de (te verwachten) resultaten van de uitwerking onder de Wpolg

Aantal	Knelpunten Wpolr	Wpolg	Resultaat
1	Geen regeling: taakinfilling privacy-functionaris onduidelijk	Functie wettelijk vastgelegd	Knelpunt opgelost
2	Functie voornamelijk administratief	Voor controlerende taak functie van functionaris gegevensbescherming geïntroduceerd	Knelpunt opgelost
3	CIE-en laten privacy-functionaris niet toe	–	Niet opgelost
4		Functionaris gegevensbescherming facultatief	
5		Reikwijdte bevoegdheden functionaris gegevensbescherming onduidelijk	Nieuw knelpunt te verwachten

Figuur 6.2 Schematische weergave knelpunten 'privacyfunctionaris'.

Onder de Wpolg heeft de privacyfunctionaris een wettelijke basis gekregen. Dat is een verbetering ten opzichte van de situatie onder de Wpolr aangezien daarmee ook de precieze taakinfilling van de privacyfunctionaris vast staat. Kort gezegd komt het erop neer dat hij een administratieve en onder-

steunende taak heeft en tevens een onderdeel van de organisatie zelf is. We zagen onder de Wpolr echter al dat juist deze adviserende rol van de privacyfunctionaris er een is waar de CIE geen behoefte aan heeft in verband met het bestaan van de CIE-officier van justitie. De CIE-officier van justitie heeft immers eveneens uitgebreide kennis van het privacyrecht en vormt, anders dan de privacyfunctionaris, een geringer afbreukrisico.

Een tweede verbetering is erin gelegen dat het instellen van een privacyfunctionaris onder de Wpolg verplicht is, zodat ook iedere politieregio over zo een functionaris beschikt. Een privacyfunctionaris is ook onder de Wpolg echter geen onafhankelijke functie in een politieregio. Hij is ondergeschikt aan de korpsbeheerder en hij is daarmee dus niet onafhankelijk en voert ook niet zelfstandig controlerende en toezichthoudende taken uit. Controlerende taken vanuit een onafhankelijke positie liggen bij het CBP (het onderwerp van de navolgende sectie) en bij de functionaris gegevensbescherming.

Met de invoering van de functionaris gegevensbescherming vormt de Wpolg een aanzienlijke uitbreiding op de Wpolr. De nieuwe regeling brengt echter ook een hoop onduidelijkheden met zich mee, met name in de reikwijdte van de geheimhoudingsplicht en daarmee de vraag of de CIE zichzelf van de werking van de functionaris gegevensverwerking kan uitsluiten. Daarnaast vragen wij ons af of de instelling van een functionaris gegevensbescherming door de korpsbeheerder ook kan plaatsvinden, wanneer hij aan deze zijn bevoegdheden slechts voor bepaalde onderdelen van zijn korps toekent. Ten slotte blijkt uit de verplichte meldingen van de ingestelde functionarissen gegevensbescherming bij het CBP dat thans (september 2009) nog maar in drie politieregio's een dergelijke functionaris is ingesteld. Overigens is dat wel een zeer behoorlijk percentage, afgezet tegen de private sector waar slechts 0,3 promille van de bedrijven en instelling een functionaris gegevensbescherming heeft ingesteld.⁴⁰⁰ De functionarissen gegevensbescherming die onder de Wbp ingesteld zijn, lijken een positieve bijdrage aan de gegevensverwerkingen te leveren.⁴⁰¹ Door deze functionaris onder de Wpolg slechts facultatief te maken is volgens ons een in potentie krachtig toezichtmechanisme thans nog onvoldoende benut. In dit verband willen wij ook wijzen op de mogelijkheid, die in de memorie van toelichting expliciet is aangehaald, waarbij alle korpsbeheerders tezamen één functionaris gegevensbescherming benoemen. Wij hebben dan een ombudsman voor politieke gegevensverwerking voor ogen, die over de regio's heen zicht houdt op de verwerking van politiegegevens. Niet alleen kan deze een krachtig kenniscentrum worden voor de politie dat bijdraagt aan de eenheid en gelijke wet-suitleg bij de verwerking van politiegegevens, maar ook kan deze in de controle en het toezicht vanuit een centrale positie krachtiger optreden. Op die manier worden de controle en toezicht op de politieke gegevensverwerking geüniformeerd. In hoofdstuk 7 komen we hier op terug.

400 Zwenne e.a., 2007, p. 157.

401 *Idem.*

6.4 HET COLLEGE BESCHERMING PERSOONSGEGEVENS

De formele toezichthouder op de verwerking van persoonsgegevens is het College bescherming persoonsgegevens, het CBP. Dit college is wettelijk met het toezicht op de verwerking van politieke gegevens belast. Daartoe heeft zij ook een aantal (onderzoeks)bevoegdheden gekregen die in respectievelijk de Wpolr en de Wpolg zijn neergelegd. De wijze waarop het CBP invulling geeft aan zijn controlerende en toezichthoudende taken zijn onderwerp van deze sectie.

We bespreken achtereenvolgens het theoretisch kader van de taakuitoefening door het CBP onder de Wpolr (subsectie 6.4.1), de daarbij geconstateerde knelpunten (subsectie 6.4.2), de uitwerking van de rol van het College bescherming persoonsgegevens onder de Wpolg (subsectie 6.4.3), en we eindigen met een tussenconclusie (subsectie 6.4.4).

6.4.1 Theoretisch kader

Ingevolge het bepaalde in art. 26 Wpolr ziet het CBP toe op de werking van de politieregisters krachtens het door de Wpolr bepaalde. Voor een preciezere taakomschrijving verwijst de Wpolr naar de artt. 51, tweede lid, en 60 tot en met 64 Wbp. We behandelen deze achtereenvolgens.

In het tweede lid van art. 51 is bepaald dat het CBP om advies gevraagd wordt bij voorstellen van wet en algemene maatregelen van bestuur die in overwegende mate zien op de verwerking van persoonsgegevens. Van deze adviserende functie maakt het CBP ook gebruik. We hebben reeds gezien dat het CBP heeft geadviseerd ten aanzien van de Wpolg en Bpolg. Ook over een veelheid van andere regelingen, die (zijdelings) zien op de verwerking van persoonsgegevens door de politie, is door het CBP geadviseerd.⁴⁰²

Art. 60 Wbp bepaalt dat het CBP ambtshalve en op verzoek van een belanghebbende onderzoek kan instellen naar de wijze waarop gegevens door, voor zover hier relevant, de CIE worden verwerkt. Ter uitoefening van deze toezichthoudende taak heeft het CBP in art. 61 Wbp een aantal bevoegdheden gekregen. Zo is in lid 4 van art. 61 Wbp bepaald dat de daartoe aangewezen personen van het CBP bestuursdwang mogen toepassen om een persoon te verplichten mee te werken aan een onderzoek naar de wijze waarop gegevens door hem worden verwerkt. In het vijfde lid van dat artikel is vervolgens bepaald dat die persoon zich daarbij niet op een geheimhoudingsplicht kan beroepen. Daarmee onderscheidt het CBP zich van de privacy-functionaris en de functionaris gegevensbescherming doordat het CBP met deze bevoegdheden een formele toezichthouder is, dat wil zeggen een toezichthouder in de zin van titel 5.1 van de Awb.

402 Zie uitgebreid voor bijvoorbeeld 2008: <http://www.cbppweb.nl/indexen/ind_publ_adv_datum_2008.stm?refer=true&theme=purple>.

Onder de Wbp heeft het CBP ook de mogelijkheid tot het opleggen van bestuurlijke boeten en het toepassen van bestuursdwang ter handhaving van de wettelijke bepalingen. Die bevoegdheden had het CBP onder de Wpolr niet. Onder Wpolr kon het CBP slechts medewerking aan een onderzoek afdwingen, maar bij een geconstateerde overtreding van de bepalingen in de Wpolr kon het CBP daarover vervolgens alleen adviseren aan de betrokken personen en daarover bijvoorbeeld verslag uitbrengen. Onder de Wpolr had het college geen bevoegdheden om de ongedaanmaking van een geconstateerde overtreding af te dwingen. Deze bevoegdheden heeft het CBP onder de Wpolg wel gekregen. Bestuursdwang brengt bijvoorbeeld met zich mee dat het CBP een last onder dwangsom kan opleggen, waarbij de last ziet op een ongedaanmaking van een overtreding van de Wpolg. Het CBP heeft op basis van de Wbp beleid gemaakt over de toepassing van bestuurlijke boeten en bestuursdwang.

Het CBP heeft in de afgelopen jaren twee maal onderzoek gedaan bij de CIE-en naar de wijze waarop zij gegevens verwerken. Het eerste onderzoek stamt uit 2003/2004 en is uitgevoerd bij acht CIE-en bij regionale politiekorpsen.⁴⁰³ Het CBP heeft 18 korpsen aangeschreven en heeft op basis daarvan een selectie gemaakt van acht korpsen waarbij het op één dag een onderzoek heeft uitgevoerd naar de bij die CIE aanwezige registraties en de manier waarop ze gegevens verwerkten. Dit onderzoek is door het CBP van tevoren schriftelijk aangekondigd en had volgens het CBP het karakter van een steekproef. Het aantal onderzochte gespreksverslagen en mutaties betrof slechts een gering aantal. Het tweede onderzoek is in 2005/2006 uitgevoerd bij twee CIE-en, die van de FIOD-ECD en de VROM-IOD.⁴⁰⁴ Het CBP heeft een aantal mutaties uit de gevoerde registers inhoudelijk onderzocht en daarnaast ook aandacht besteed aan de daarmee samenhangende technische en organisatorische aspecten.

6.4.2 De knelpunten beschreven

Er zijn drie knelpunten. Een eerste knelpunt dat zich voor lijkt te doen in de controle en toezichtspraktijk van het CBP is het feit dat het college alleen bevoegdheden heeft om het onderzoek te verrichten en zonodig af te dwingen. Het CBP heeft geen bevoegdheden om een wetsconforme verwerking van de verwerking van persoonsgegevens af te dwingen indien dat nodig is.

403 *Algemene bevindingen naar aanleiding van de onderzoeken door het CBP naar de bijzondere politieregisters van Criminele Inlichtingen Eenheden in 2003/2004*, 8 september 2004, te raadplegen via <http://www.cbweb.nl>.

404 *Verwerking persoonsgegevens in registers zware criminaliteit en informantregisters*, CBP-onderzoek naar politieregisters bij de Criminele Inlichtingen Eenheden van twee Bijzondere Opsporingsdiensten z2005-0988 en z2005-0989, april 2007, te raadplegen via <http://www.cbweb.nl>.

Hierbij dient te worden opgemerkt dat het CBP deze mogelijkheid – die het in de private sector wel heeft – slechts in zeer uitzonderlijke gevallen inzet.

Wat toezichthoudende en adviserende taak betreft, is opvallend dat het CBP reeds in 2004 zelf heeft aangegeven als gevolg van beperkte capaciteit zich meer wil gaan toeleggen op haar toezichthoudende taak en minder op advisering en het verstrekken van informatie.⁴⁰⁵

Het capaciteitsgebrek is als het gaat om politieke gegevensverwerking het tweede knelpunt dat wij signaleren. Het CBP heeft de afgelopen jaren tal van onderzoeken uitgevoerd in het veld van politie en justitie. Enkele bekende voorbeelden zijn onderzoeken naar het vastleggen van DNA-profielen, het vastleggen van tap-verslagen van gesprekken tussen verdachten en advocaten, en het vastleggen van verkeersgegevens.⁴⁰⁶ Als we echter bekijken wat de bemoeienis van het CBP ten aanzien van CIE is, dan zien we dat het college sinds haar instelling in 2001 slechts tweemaal onderzoek heeft gedaan naar de wijze waarop persoonsgegevens bij deze eenheden worden verwerkt.

Daarnaast wordt in de literatuur ook aangegeven dat de samenloop van de verschillende taken van het CBP onwenselijk is. Het gaat dan om (ook onder de Wbp) het adviseren over wetgeving, toetsing van gedragscodes en reglementen, voorlichting, bemiddeling, klachtbehandeling en internationale taken. Zoals de commissie-Brauer stelt, is de slagvaardigheid van het externe toezicht erbij gebaat wanneer de externe toezichthouder geen bemoeienis met dergelijke activiteiten heeft.⁴⁰⁷

Ook het eerste onderzoek, bij acht regionale CIE-en, is alweer zes jaar geleden uitgevoerd en droeg bovendien het karakter van – in de eigen woorden van het CBP – een steekproef. De normerende waarde die zich daarvan thans nog laat voelen kan als nihil worden bestempeld. Het tweede door het CBP uitgevoerde onderzoek dateert van 2005/2006 en ziet slechts op twee CIE-en. Dit betekent dat de meerderheid van de CIE-en die dagelijks opereren weinig tot niets van de controlerende en toezichthoudende taak van het CBP hebben gemerkt. De reden is eenvoudigweg dat het CBP niet bij hen is langsgeweest om toezicht te houden en controle uit te voeren op de wijze waarop zij persoonsgegevens verwerken. Dit alleen al vormt aanleiding voor ons om vraagstekens te plaatsen bij de bijdrage van het CBP, vanuit zijn positie als toezichthouder en controleur, aan een zorgvuldige gegevensverwerking bij CIE-en. Deze constatering leidt als het ware vanzelfsprekend tot het derde knelpunt.

Het voorgaande beeld wordt versterkt als we kijken naar de impact van dergelijke onderzoeken op het gedrag van de CIE-en. Dit is het derde knelpunt. In het door Kielman en Koelewijn uitgevoerde veldonderzoek werd over het bezoek van de CIE het volgende opgemerkt:

405 Uitgangspunten en beleidsregels werkwijze Cbp, *Stcrt* 2004, nr. 190, p. 11.

406 Zie voor de verschillende rapporten <http://www.cbweb.nl/>.

407 Brauer e.a., 2009, p. 53-54.

*“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.”*⁴⁰⁸

Het citaat maakt duidelijk dat de waarde die aan de door het CBP uitgevoerde onderzoeken kan worden toegekend sterk afhankelijk is van de gegevensverwerkingen waarop de onderzoeken zijn gebaseerd. Het voorgaande citaat geeft op z’n minst het vermoeden dat die basis niet zo representatief is dat van een deugdelijk onderzoek kan worden gesproken. Natuurlijk kan ook niet betoogd worden dat voornoemd citaat een representatief beeld geeft. Wij herhalen echter dat het wel de aanleiding vormt om aan de deugdelijkheid van de basis waarop die onderzoeken gebaseerd te twijfelen. Ook de verslaglegging van de onderzoeken van het CBP zelf vermelden niets over de wijze waarop de gegevens die zijn onderzocht zijn geselecteerd uit de gegevensverzamelingen van de CIE.

Afgezien van al deze beschouwingen geeft voornoemd citaat inzicht in de wijze waarop vanuit de CIE-praktijk wordt aangekeken tegen de rol die het CBP speelt. Vanuit het onderzoek dat door Kielman en Koelewijn is uitgevoerd kan worden gezegd dat dit beeld een breed gedragen beeld is onder de CIE-en die in dat onderzoek zijn gesproken. De zeer lage frequentie van de uitvoering van de controlerende en toezichthoudende taken van het CBP is daarbij een belangrijke factor.

6.4.3 Uitwerking onder de Wpolg

De taak van het CBP is onder de Wpolg hetzelfde gebleven als onder de Wpolr. Het CBP blijft de toezichthouder als het gaat om de controle en het toezicht op de wijze waarop gegevens door de CIE-en worden verwerkt. Wel komt de Wpolg tegemoet aan het eerste knelpunt dat het CBP niet over middelen beschikt om verwerking van persoonsgegevens in overeenstemming met het wettelijk regime af te dwingen. De Wpolg verklaart ook art. 65 Wbp van overeenkomstige toepassing. In dat artikel is bepaald dat het CBP bestuursdwang kan toepassen en op die manier de naleving van de regels tot gegevensverwerking kan afdwingen. Het opleggen van een bestuurlijke boete is gedeeltelijk van toepassing verklaard als het gaat om politieke gegevensverwerking. Een boete kan alleen worden opgelegd bij een schending van de protocolplicht, waarover we in sectie 6.5 komen te spreken. Indien een korpsbeheerder niet aan die protocolplicht voldoet, kan het CBP overgaan tot boeteoplegging. Het moge duidelijk zijn dat de Wpolg daarmee in hoge mate tegemoet komt aan het feit dat het CBP onder het oude regime van de Wpolr op papier de kracht van een tandeloze tijger had.

408 Koelewijn, 2009, p. 128.

Wat het tweede knelpunt betreft, stellen we vast dat de Wpolg geen verandering brengt in de situatie dat het CBP naast zijn toezichthoudende taak ook tal van adviserende taken heeft. Het knelpunt in de samenloop van de verschillende taken zal dus blijven bestaan.

Ook ten aanzien van het derde knelpunt biedt de Wpolg geen oplossing. De hoeveelheid door het CBP uitgevoerde onderzoeken wordt door de nieuwe wet niet nader aangeduid. Ook onder de nieuwe wet wordt verwezen naar art. 60 Wbp, waar in het eerste lid is bepaald dat het CBP ambtshalve of op verzoek van een belanghebbende onderzoek kan instellen. De frequentie waarmee onderzoek wordt gedaan door het CBP staat dus ook onder de nieuwe wet open. Er is geen reden om aan te nemen dat deze frequentie in de toekomst verhoogd wordt.

Hetzelfde geldt voor de houding van de CIE-en tegenover het CBP. Daarover bepaalt de Wpolg niets. Dit is wat ons betreft ook vanzelfsprekend. Een houding tegenover een toezichthouder is niet in een wet te bepalen. De houding zal grotendeels bepaald worden door (1) de frequentie van de door het CBP uit te voeren onderzoeken, (2) de intensiteit daarvan en (3) de maatregelen die nadien door het CBP zullen worden genomen om de geconstateerde overschrijdingen van wet- en regelgeving ongedaan te maken.

6.4.4 Tussenconclusie aangaande het College bescherming persoonsgegevens

Alvorens we onze tussenconclusie aangaande de controle en het toezicht door het CBP formuleren, geven we schematisch weer (a) het aantal onder de Wpolr geconstateerde knelpunten, (b) de inhoud van die knelpunten, (c) de uitwerking daarvan onder de Wpolg, en (d) de (te verwachten) resultaten van de uitwerking onder de Wpolg.

Aantal	Knelpunten Wpolr	Wpolg	Resultaat
1	Geen bevoegdheden tot afdwingen wetsconforme gegevensverwerking	Kent bevoegdheden toe tot (1) bestuursdwang en (2) bestuurlijke boete ingeval van protocolplicht	'Knelpunt' opgelost door bevoegdheidstoekenning
2	Samenloop van taken	Geen verandering in takenpakket	Niet opgelost
3	Beperkte onderzoekscapaciteit	–	Niet opgelost
4	Weinig normerende werking van onderzoeken CBP	–	Niet opgelost

Figuur 6.3 Schematische weergave knelpunt 'CBP'.

De Wpolg biedt een duidelijke oplossing voor het tandeloze-tijgergehalte van het CBP onder de Wpolr. De wet kent het CBP duidelijke bevoegdheden toe waarmee het college zo nodig effectief de CIE-en kan dwingen in over-

eenstemming met de wet gegevens te verwerken. Daarmee is het knelpunt opgelost zoals dat hierboven is geconstateerd. Het is vervolgens natuurlijk de vraag of het CBP daar in de praktijk gebruik van gaat maken. Het CBP heeft deze bevoegdheid al sinds 2001 voor de private sector onder de Wbp, maar de praktijk leert dat de drempel voor het CBP om dit middel in te zetten hoog ligt. Ons is slechts één geval bekend waar daadwerkelijk een boete/bestuursdwang werd opgelegd en dat ging om een flagrante schending van de bepalingen van de Wbp. Wij vragen ons sterk af of het CBP in geval van een voor de politiepraktijk zo'n belangrijk instituut als de CIE de gegevensverwerkingen zou stoppen als het erop aankomt. Dit staat los van de vraag of het stoppen, gelet op de belangen die daar spelen als het gaat om de veiligheid van informanten en dergelijke, eigenlijk wel te rechtvaardigen valt. Het zal er naar ons idee in de praktijk toe leiden dat het CBP in het geval van de CIE van deze bevoegdheden geen gebruik zal maken.

De sterkere wettelijke controle- en toezichtsmogelijkheden van het CBP maken wel dat het college in staat is om zijn positie bij de CIE-en te verstevigen. Daarbij wordt het wel gehinderd door de samenloop van de verschillende taken die het heeft en die elkaar in de weg zitten. Dit knelpunt is onder de Wpolg niet opgelost.

Het derde en vierde knelpunt zijn evenmin door de Wpolg opgelost, maar deze knelpunten kunnen ook niet door wetgeving opgelost worden. De bal ligt wat deze punten betreft bij het CBP zelf. Het college heeft de wettelijke mogelijkheden om haar toezichthoudende en controlerende taak handen en voeten aan te geven. Tot nu toe is daar echter geen direct gevolg aan gegeven. De constatering blijft dat het domein van politie en justitie slechts een van de vele gebieden is waar het CBP zijn toezichthoudende taak heeft. Dat maakt ook dat van het CBP in redelijkheid niet kan worden verwacht dat zij haar taken erg op dat gebied van de CIE intensificeert. Dat zou onvermijdelijk ten koste gaan van andere gebieden waar het haar rol als toezichthouder vervult. De wetgever heeft op dit gebied ook in de memorie van toelichting niet aangegeven hoe het CBP hiermee om zou kunnen gaan. Ook is niet aangegeven dat er ruimte aan het CBP zal worden geboden om haar controlerende en toezichthoudende taken te intensiveren.

In conclusie mogen we stellen dat controle en toezicht door het CBP tekortschieten, niet alleen als gevolg van een gebrek aan bevoegdheden, maar vooral als gevolg van capaciteitsgebrek en gebrek aan vertrouwen onder de CIE-en. Dit maakt dat dé toezichthouder feitelijk niet in staat is om deze rol naar behoren te vervullen.

6.5 PROTOCOLLERING EN AUDITING

Een van de mogelijkheden voor realisatie van controle en toezicht is het vastleggen van de diverse handelingen die met politiegegevens worden uitgevoerd. In vaktermen wordt dan gesproken over 'protocollering'. Achteraf is dan in de protocolbestanden terug te zien wat er met een bepaald gegeven

is gebeurd, bijvoorbeeld wanneer het is opgeslagen, aan wie het is verstrekt en wanneer het is verwijderd. Als we het vervolgens hebben over controle en toezicht op grond van deze protocolbestanden, dan spreken we van 'auditing'.

We bespreken achtereenvolgens het theoretisch kader van de protocollering onder de Wpolr (subsectie 6.5.1), de daarbij geconstateerde knelpunten (subsectie 6.5.2), de uitwerking van protocollering en auditing onder de Wpolg (subsectie 6.5.3) en eindigen met een tussenconclusie (subsectie 6.5.4).

6.5.1 Theoretisch kader

Een verstrekking vanuit het register zware criminaliteit wordt vastgelegd, tenzij het een verstrekking is aan vaste gebruikers overeenkomstig het doel van het register. Verstrekkingen aan de inlichtingen- en veiligheidsdiensten dienen niet te worden vastgelegd.⁴⁰⁹ Dit laatste geldt ook voor verstrekkingen uit het voorlopig register. In het algemeen dienen verstrekkingen uit het voorlopig register te worden vastgelegd en voor één jaar te worden bewaard, met uitzondering van, zoals gezegd, de verstrekkingen aan de inlichtingen- en veiligheidsdiensten.⁴¹⁰

In het modelreglement informantenregisters is voorts bepaald dat van iedere verstrekking uit het informantenregister een aantekening wordt gemaakt.⁴¹¹ In ieder geval dienen blijkens het tweede lid van art. 10 van het modelreglement de identiteit van degene aan wie verstrekt is, de datum, het precieze doel van de verstrekking, en een omschrijving van de verstrekte gegevens te worden aangetekend. Deze gegevens mogen pas worden verwijderd indien de registratie zelf ook uit het informantenregister verwijderd wordt.

Onder de Wpolr en de daarbij behorende lagere regelgeving zijn verder geen bepalingen opgenomen wat met de voornoemde protocollering dient te gebeuren. Het ligt voor de hand dat de verschillende toezichthouders toegang hebben tot de protocolbestanden om hun controlerende en toezichthoudende taken uit te voeren.

In de regeling Toezicht op beheer bijzondere politieregisters wordt voorts aangestipt dat door CIE-en ook een onafhankelijke audit dient te worden uitgevoerd. Dat is echter in de toelichting van die regeling vermeld. In een aparte regeling zou dit op een later moment worden ingevuld.⁴¹² Dit is echter niet gebeurd. Mogelijk omdat enige tijd na de invoering van voornoemde circulaire het ontwikkelingstraject van de Wpolg is ingezet. Wij hebben echter niet kunnen nagaan dat aan het mechanisme van auditing onder de Wpolr op enige wijze invulling is gegeven.

409 Art. 13a lid 6 en 7 Wpolr.

410 Art. 13b lid 4 Wpolr.

411 Art. 10 lid 1 modelreglement informantenregister.

412 Toezicht op beheer bijzondere politieregisters, *Stcrt.*, 13 maart 2002, nr. 51, p. 10.

6.5.2 De knelpunten beschreven

Het belangrijkste knelpunt in de uitvoering van de onder de Wpolr opgenomen regeling betreft de omstandigheid dat de ICT-infrastructuur van de politie niet in staat is om aan de protocolverplichting van de Wpolr te voldoen. Bij sommige systemen bestaat de mogelijkheid tot protocollering gewoonweg niet. Wanneer die mogelijkheid wel bestaat, is een veelgehoord geluid dat het aanzetten van het loggen het systeem dusdanig vertraagt dat het onwerkbaar wordt. Overigens gaven de CIE-en aan dat het ook geen zin had om de protocol-functie aan te zetten, omdat noch zij noch de gegevens-beheerders tijd hebben om aan de controle daarvan toe te komen.⁴¹³ Daarnaast bleek in elk van de drie gevallen de protocollering dusdanig te geschieden dat deze niet meer beschikbaar was op het moment van de wettelijk voorgeschreven auditing.⁴¹⁴ Voorts zag het onderzoek van het CBP maar op drie regio's, hetgeen geleet op de frequentie van dergelijk onderzoek door het CBP de 'pakkans' erg klein maakt.

Voorts merken wij als knelpunt aan dat in de regelingen niet is opgenomen wat er met de protocolgegevens dient te gebeuren, zodat de regeling onder de Wpolr niet als zelfstandig controle- en toezichtmechanisme functioneert, maar uitsluitend ten dienste staat van de overige controle- en toezichtsmechanismen. Dit heeft tot gevolg gehad dat bij het evaluatieonderzoek in 2005 werd geconcludeerd dat het onduidelijk was in hoeverre de protocolgegevens werden gebruikt bij het uitvoeren van controle- en toezichtswerkzaamheden.

6.5.3 Uitwerking onder de Wpolg

Onder de Wpolg is in art. 32 de protocolverplichting onder vergelijkbare voorwaarden gehandhaafd. Het gaat dan met name om de verstrekkingen die zijn gedaan uit de verschillende gegevensverzamelingen. De enige uitzondering die daarop bestaat is het verstrekken aan de AIVD, zoals dat ook onder oude regeling het geval was. Daarnaast is de protocollering van de verstrekte autorisaties verplicht voorgeschreven, evenals een automatische vergelijking van gegevens zoals bedoeld in art. 11, vijfde lid Wpolg. Ten slotte is ingevolge art. 32 lid 1 onder e Wpolg ook de protocollering verplicht van verwerkingen ten aanzien waarvan aanwijzingen bestaan dat zij door onbevoegden of anderszins op onrechtmatige wijze zijn verricht. Daarmee is de protollering onder de Wpolg iets omvangrijker dan onder de Wpolr, waar deze alleen verstrekkingen betrof.

Wat de bewaarplicht van de protocolleringsgegevens betreft is in art. 32 lid 3 Wpolg bepaald dat dit dient te gebeuren zolang de verantwoordelijke

⁴¹³ Schreuders e.a., 2005, p. 115.

⁴¹⁴ De problemen daarbij liepen van helemaal geen loggegevens opslaan tot de opgeslagen gegevens te kort bewaren.

de gegevens nodig heeft in verband met zijn verplichting uit hoofde van het eerste lid van art. 30. Dit artikel bepaalt dat de verantwoordelijke mededeling doet van een wijziging in gegevens aan iedereen aan wie de gegevens zijn verstrekt, indien de wijziging het gevolg is van een verzoek daartoe van een belanghebbende (in de regel een persoon die een kennisnemingsverzoek heeft gedaan). Het gaat dan alleen om de verstrekking(en) in het jaar voor de betreffende wijziging. Daarnaast dienen de gegevens bewaard te worden, kort gezegd, zolang deze nodig zijn voor de onder de Wpolg verplichte audit.

Daarmee komen we op een belangrijk wijziging in de Wpolg ten opzichte van de Wpolr. Onder de Wpolg is het houden van zogenaamde audits verplicht. In art. 33 Wpolg is bepaald dat de verantwoordelijke daartoe verplicht is. In art. 6:5 lid 1 Bpolg is vervolgens bepaald dat dit iedere twee jaar dient te gebeuren op een door de minister te bepalen wijze. Blijkens het tweede lid van art. 6:5 Bpolg gaat het bij de audits om (1) de wijze waarop het verwerken van politiegegevens is georganiseerd, (2) de maatregelen en procedures die daarop van toepassing zijn en (3) de werking van deze maatregelen en procedures. Indien de verantwoordelijke niet aan het in de wet bepaalde voldoet, is hij volgens lid 3 van datzelfde artikel verplicht binnen een jaar opnieuw een audit te laten uitvoeren. In de regeling periodieke audit politiegegevens,⁴¹⁵ die per 1 januari 2009 van kracht is geworden, zijn nadere regels neergelegd over de wijze waarop deze audit vorm moet worden gegeven. De regeling ziet echter niet op de inhoud van de audit doch stelt alleen eisen aan de auditeur en bepaalt dat het onderzoek melding moet maken van de wijze waarop het verwerken van politiegegevens is georganiseerd, alsmede van de maatregelen en procedures die daarop van toepassing zijn als ook van de werking van deze maatregelen en procedures. In de regeling is voorts bepaald dat van de resultaten van een audit een rapport wordt opgesteld dat aan de verantwoordelijke wordt gepresenteerd en ook aan het CBP. Indien daarin geconstateerd wordt dat bepaalde delen van de gegevensverwerking niet in overeenstemming met de wet- en regelgeving is, dient de verantwoordelijke hier maatregelen te nemen en na een jaar opnieuw een audit uit te laten voeren, net zo lang totdat de gegevensverwerking wel in overeenstemming met wet- en regelgeving is.

6.5.4 Tussenconclusie aangaande protocollering en auditing

Alvorens we onze tussenconclusie aangaande de controle en het toezicht door protocollering en auditing formuleren, geven we schematisch weer (a) het aantal onder de Wpolr geconstateerde knelpunten, (b) de inhoud van die knelpunten, (c) de uitwerking daarvan onder de Wpolg, en (d) de (te verwachten) resultaten van de uitwerking onder de Wpolg.

415 Regeling periodieke audits politiegegevens, *Stcrt* 30 december 2008, nr. 252.

Aantal	Knelpunten Wpolr	Wpolg	Resultaat
1	Protocollering technisch en door fte-capaciteit onwerkbaar	–	Niet opgelost
2	Doel protocollering onduidelijk	–	Niet opgelost
3		Veel onduidelijkheden rond auditing-regeling	Knelpunt geïntroduceerd

Figuur 6.4 Schematische weergave knelpunten 'protocollering en auditing'.

De protocollering is onder de Wpolg gehandhaafd, maar er is geen oplossing geboden voor de kennelijke onmogelijkheid van de ICT-systemen om de protocollering uit te voeren. Daarover is ook niets opgemerkt in bijvoorbeeld de memorie van toelichting. Evenmin is er aandacht besteed aan de in de praktijk geconstateerde capaciteitsproblemen bij een mogelijke rol die de protocolleringsgegevens bij het uitvoeren van controle en toezicht zouden kunnen spelen. Nog los van de vraag of wetgeving de aangewezen weg is om deze problemen op te lossen, had het wel op de weg van de wetgever gelegen om daar duidelijkheid over te verschaffen. Dit zou zeker zo moeten zijn omdat onder de Wpolg aan de verantwoordelijke zelfs boetes kunnen worden opgelegd als hij zich niet aan de protocolleringsverplichting houdt. Onder de Wpolg is aan de verantwoordelijke daarmee een verplichting opgelegd, waarvan we uit de praktijk weten dat hij die niet kan nakomen. Deze constatering is zorgelijk.

Voorts is de verhouding tussen protocollering en auditing onduidelijk. Zo is het onduidelijk of de protocolgegevens bij de uit te voeren audit gebruikt dienen te worden. Dat lijkt enerzijds wel te kunnen worden opge maakt uit de wettelijke bepaling omtrent de bewaartermijn van deze gegevens. Daarin is immers opgenomen dat deze gegevens bewaard dienen te worden totdat de wettelijk voorgeschreven audit in zijn geheel is uitgevoerd. Anderzijds kan hieruit niet direct een verplichting worden gelezen om deze gegevens ook direct bij een audit te betrekken. In de wettelijke bepalingen over de uit te voeren audit, alsmede die in het Bpolg en de regeling periodieke audits politiegegevens, is daarover iets opgenomen. Daarin is alleen vermeld dat het audit-onderzoek onder meer een beschrijving van de onderzoeksmethoden bevat. In geen van de genoemde regelingen is voorgeschreven dat de protocolleringsgegevens bij het doen van de audit dienen te worden betrokken.

Van een wat grotere afstand bekeken hebben wij meer vraagtekens bij de wijze waarop de audits uitgevoerd dienen te worden. Voorop is gesteld dat met het voorschrijven van een EDP-auditeur er een effectieve waarborg is gecreëerd voor de deskundigheid van de auditeur. Over de inhoud van de audit is wat ons betreft meer onduidelijkheid. Zo vragen wij ons af in hoeverre de audit ziet op procedures en in hoeverre er daadwerkelijk wordt onderzocht of de gegevensverzamelingen zelf ook aan de wettelijke eisen

voldoen. In de regeling is weliswaar opgenomen dat 'de werking van deze maatregelen en procedures' onderdeel van de audit dienen te zijn, maar dat kan ook resulteren in een formalistische benadering of de op papier gezette procedures worden gevolgd, zonder daarbij daadwerkelijk een gegevensverzameling te openen en te bekijken. Dat deze vrees niet geheel ongegrond is, blijkt uit de uitwerking van de circulaire toezicht op beheer bijzondere politieregisters, die tot stand is gekomen in 2002. Op grond van deze circulaire is rond 2003 een zelfevaluatie met een besprekingsverslag uitgevoerd door de CIE-en. Deze zag echter hoofdzakelijk op de organisatie van het beheer. In het kader van het besprekingsverslag werd kennelijk geen kennis genomen van de inhoud van de gegevensverzamelingen.⁴¹⁶ Het had ook hier op de weg van de wetgever gelegen om strakker voor te schrijven hoe inhoudelijk aan de audit vorm dient te worden gegeven.

Ten slotte is opvallend dat er geen sanctie is gesteld op de eventuele constatering van een auditeur dat in strijd met de wet gegevens worden verwerkt. De verantwoordelijke heeft dan wel de verplichting om die strijdigheid op te lossen en na een jaar opnieuw een audit te laten uitvoeren, net zo lang totdat het probleem is opgelost. Noch op het verzuim daarvan noch op het verzuim om niet tijdig een audit te laten uitvoeren is de boeteclausule van toepassing verklaard. Dat was wat ons betreft, net als bij de protocolleringsplicht, wel de aangewezen weg geweest. Opgemerkt zij dat het CBP bij een geconstateerde overtreding wel bestuursdwang kan toepassen, waardoor actie van een verantwoordelijke door middel van een dwangsom kan worden afgedwongen.

In conclusie kunnen we stellen dat met de invoering van het systeem van auditing een nieuwe wijze van toezicht houden aan het wettelijk stelsel is toegevoegd. De regeling waarbij dit middel is uitgewerkt bevat wat ons betreft evenwel te veel gaten om op voorhand van een effectief middel te kunnen spreken.

6.6 DE CIE-OFFICIER VAN JUSTITIE

Zoals beschreven in sectie 6.1 worden controle en toezicht niet alleen uitgevoerd door personen en instanties die in de Wpolg genoemd zijn, maar ook door instanties die dat vanuit hun rechtsstatelijke positie doen. Eén daarvan is de officier van justitie. Vanuit zijn positie heeft hij de leiding over het opsporingsonderzoek en dus ook de leiding over de politie.

We bespreken achtereenvolgens het theoretisch kader van de CIE-ovj onder de Wpolr (subsectie 6.6.1), de daarbij geconstateerde knelpunten (subsectie 6.6.2), de uitwerking van de rol van de CIE-ovj onder de Wpolg (subsectie 6.6.3), en eindigen met een tussenconclusie (subsectie 6.6.4).

⁴¹⁶ *Algemene bevindingen CIE-onderzoeken*, College bescherming persoonsgegevens, september 2004, p. 5.

6.6.1 Theoretisch kader

De CIE-ovj is een positie die niet expliciet in de Wpolr voorkomt. De enige verwijzing die in de Wpolr naar de CIE-ovj is te vinden is de verwijzing naar 'het bevoegd gezag', dat in sommige gevallen is aangewezen als het orgaan dat bepaalt of een bevoegdheid mag worden ingezet. De officier van justitie is ingevolge art. 148 Sv leider van het opsporingsonderzoek en uit dien hoofde bevoegd gezag over de politie. Hij voert die taken uit naast de taken van de korpsbeheerder, die als verantwoordelijke is aangemerkt. De wetgever gaat er vanuit dat hun positie als het gaat om de verwerking van gegevens bij de CIE gelijkwaardig is.⁴¹⁷ Over de wijze waarop de CIE-ovj met zijn toezichthoudende taken dient om te gaan, zijn echter geen bepalingen opgenomen in de Wpolr of het Bpolr. Alleen uit de CIE-regeling blijkt dat er een officier van justitie aangewezen is die verantwoordelijk is voor de taakuitoefening van de CIE. Dit is zo bepaald in art. 1 onder g CIE-regeling. Deze regeling bepaalt echter evenmin hoe de CIE-ovj hier invulling aan dient te geven.

In een door het College van procureurs-generaal opgestelde instructie CIE-officier van justitie⁴¹⁸ wordt nader uitgewerkt op welke wijze de CIE-ovj aan zijn verantwoordelijkheid op grond van de Wpolr vorm dient te geven. De instructie stelt voorop dat de taak van de CIE erin gelegen is het recherche-proces te ondersteunen. Dit dient dus ook voor de rol van de CIE-ovj te gelden; hij verleent volgens de instructie ondersteuning aan de tactische recherche en aan zaaks-officieren van justitie.⁴¹⁹ Meer specifiek bepaalt artikel 1.1 van de instructie dat de CIE-ovj het gezag uitoefent over alle werkzaamheden die de onder hem ressorterende CIE verricht. Daartoe is in het tweede artikel onder meer bepaald dat hij structureel contact met de CIE dient te onderhouden en daarvan een journaal dient bij te houden. Voorts schrijft de instructie in de artikelen 3 en 4 voor hoe de CIE-ovj dient om te gaan met respectievelijk (1) het inwinnen van informatie en (2) het verwerken (dit is opslaan, bewaren, verstrekken, koppelen, en analyseren) van informatie. Gelet op de beperkingen van dit onderzoek behandelen we alleen de rol van de CIE-ovj bij de verwerking van politiegegevens.

Wat het informantenregister betreft bepaalt de CIE-ovj of een informant definitief mag worden ingeschreven in het informantenregister en daarbij toetst hij de kwaliteit van de informant en bepaalt hij ook de duur van de inschrijving. De CIE-ovj draagt, naast de korpsbeheerder, de verantwoordelijkheid voor onder meer de juistheid en volledigheid van de gegevens, alsmede voor het gebruik en de verwijdering van die gegevens. Deze laatste verantwoordelijkheid geldt ook voor de gegevens die opgenomen zijn in het zwacri- en het voorlopig register. Van de verstrekking van 00-informatie is in

417 *Kamerstukken II*, 1996/97, 25 398, nr. 3, p. 11.

418 Instructie CIE-officier van justitie (2006I002), niet gepubliceerd. De instructies zijn ook beschreven in Van der Bel e.a., 2007, p. 70-72.

419 *Idem*.

de instructie opgenomen dat deze uitsluitend met toestemming van de CIE-ovj buiten de CIE-structuur wordt uitgegeven.

Op grond van artikel 5 van de instructie is de CIE-ovj gehouden medewerking te verlenen aan zelfevaluaties en te houden externe audits bij de CIE indien dit door de minister van Binnenlandse zaken en Koninkrijksrelaties bij voorschrift is bepaald. Ook is in dat artikel bepaald dat de CIE-ovj het informantenregister, het voorlopig register en het register zware-criminaliteit controleert overeenkomstig de Instructie CIE-Registercontrole⁴²⁰.

De Instructie CIE-Registercontrole bepaalt dat de CIE-ovj twee keer per jaar controle uitvoert op het informantenregister, het voorlopig register en het register zware-criminaliteit. Daarbij beoordeelt hij ondermeer de rechtmatigheid van de verkrijging en het opslaan van gegevens, de noodzakelijkheid van de noodzaak van de registratie, de juistheid van de in het register opgenomen gegevens en de volledigheid daarvan. Ten slotte is bepaald dat de CIE-ovj er op toe dient te zien dat de eventueel geconstateerde gebreken worden hersteld. In de instructie is vastgelegd dat de CIE-ovj regelmatig overleg voert met de CIE-chef en kennis neemt van processen-verbaal, journaals, gespreksverslagen en andere stukken van de CIE. De CIE-chef legt zijn bevindingen vast in een verslag, dat eenmaal per jaar aan de hoofdofficier van justitie wordt verstrekt.

Naast de instructies voor de CIE-ovj is er een landelijk overleg van CIE-officieren tot stand gekomen. Dit Landelijk Platform CIE-officieren (LPC) houdt zich met name bezig met de vraag op welke wijze de informatieofficier gezag zou moeten uitoefenen over het informatieproces. Deze ontwikkelingen hebben er volgens de een aantal officieren zelf toe geleid dat de CIE-ovj steeds meer verantwoordelijk wordt voor de informatiestromen rond de CIE.⁴²¹

6.6.2 De knelpunten beschreven

Vooropgesteld dient te worden dat de controle en het toezicht door de CIE-ovj intensief zijn. Uit het WODC-evaluatieonderzoek blijkt dat een CIE-ovj gemiddeld een keer per week of twee weken overleg pleegt met de CIE-chef. Daarnaast is er een grote betrokkenheid van hem bij de dagelijkse werkzaamheden, wordt het overleg van de CIE-runners bijgewoond en voert hij zelfstandig controle uit op de in de registers opgenomen gegevens.⁴²² Ook uit het onderzoek van Kielman en Koelewijn is naar voren gekomen dat het toezicht door de CIE-ovj door de CIE-en als intensief wordt ervaren.

420 Instructie CIE registercontrole (2007I003), niet gepubliceerd.

421 Van der Bel e.a., 2007, p. 98.

422 Schreuders e.a., 2005, p. 146. *Opportuun*, 2002.

Het gebrek aan enige wettelijke regeling rond de CIE-ovj merken wij aan als eerste knelpunt. Juist vanwege het feit dat de CIE-ovj in de praktijk een grote rol speelt bij de het proces van politieke informatieverwerking zou een wettelijke rol als toezichthouder of controleur verwacht worden. Niets is echter minder waar. Zoals reeds aangehaald heeft de wetgever het alleen in de memorie van toelichting bij de Wet bijzondere politieregisters over de positie van de CIE-ovj ten opzichte van de korpsbeheerder en blijkt uit de CIE-regeling het bestaan van de CIE-ovj. Er zijn echter nergens in de regelingen bepalingen opgenomen over de wijze waarop de CIE-ovj invulling moet geven aan zijn verantwoordelijkheid die uit art. 148 Sv voortvloeit. Dat heeft geresulteerd in de instructie van het College van Procureurs-generaal. Deze instructie functioneert in de praktijk goed. Opname van deze controlerende en toezichthoudende taken in een formele (wettelijke) regeling lijkt dan ook aangewezen.

In de praktijk worden de taken van de CIE-ovj nog wel eens feitelijk uitgevoerd door gespecialiseerde parketsecretarissen. Het CBP heeft daarover gezegd dat er in de toepasselijke instructie geen basis voor gegeven was.⁴²³ Op grond van de regelingen onder de Wpolr was geen mandatering van de bevoegdheden van de CIE-ovj mogelijk. Dit merken wij aan als tweede knelpunt.

6.6.3 Uitwerking onder de Wpolg

Over de controlerende en toezichthoudende taak van de CIE-ovj is in de Wpolg niets opgenomen. In het Bpolg is dat evenmin het geval, wel is op een aantal momenten van gegevensverwerking opgenomen dat de instemming van de officier van justitie vereist is, met name op het gebied van gegevensverstrekkingen naar het buitenland.

Onder de Wpolg is vastgehouden aan het systeem zoals we dat onder de Wpolr kennen. In twee instructies van het College van Procureurs-generaal is aan de CIE-ovj's aangegeven hoe zij hun controlerende en toezichthoudende taak vorm dienen te geven. Net als onder de Wpolr is daarbij gekozen voor een Instructie CIE-officier van justitie⁴²⁴ en een Instructie controle CIE-gegevensverwerking⁴²⁵. Deze beide instructies omvatten feitelijk exact dezelfde regelingen als onder de Instructie CIE-officier van justitie en de Instructie CIE-Registercontrole, zoals deze onder de Wpolr golden. Vanzelfsprekend zijn wel wetstechnische aspecten in de beide instructies verwerkt als gevolg van het vervallen van het registerbegrip onder de Wpolg en het

423 *Verwerking persoonsgegevens in registers zware criminaliteit en informantenregisters* CBP-onderzoek naar politieregisters bij de Criminele Inlichtingen Eenheden van twee Bijzondere Opsporingsdiensten z2005-0988 en z2005-0989, april 2007.

424 Instructie CIE-officier van justitie (2009I004), niet gepubliceerd.

425 Instructie controle CIE-gegevensverwerking (2009I003), niet gepubliceerd.

voorlopige register als verwerkingsgrond. Omdat de instructies materieel bezien geen wijzigingen bevatten ten opzichte van de instructies zoals deze in subsectie 6.6.1 zijn besproken verwijzen we korthedshalve naar hetgeen we daar hebben vermeld.

De Instructie CIE-gegevensverwerking bevat daarnaast één toevoeging. Dit betreft een mandateringsbevoegdheid voor de CIE-ovj om bepaalde taken te mandateren aan een specialistische parketsecretaris (artikel 7.1). Het gaat daarbij kort gezegd om de algemene controle op de standaard gegevensverwerking door de CIE en de controle over een nieuw subject (n.b. niet de beslissing en opname daarvan) (artikel 7.2).

6.6.4 Tussenconclusie aangaande de CIE-officier van justitie

Alvorens we onze tussenconclusie aangaande het controle en toezicht door de CIE-ovj formuleren, geven we schematisch weer (a) het aantal onder de Wpolr geconstateerde knelpunten, (b) de inhoud van die knelpunten, (c) de uitwerking daarvan onder de Wpolg, en (d) de (te verwachten) resultaten van de uitwerking onder de Wpolg.

Aantal	Knelpunten Wpolr	Wpolg	Resultaat
1	Geen wettelijke invulling taken en bevoegdheden	–	Knelpunt niet opgelost
2	Geen mandatering mogelijk	Mandatering opgenomen in instructie	Knelpunt opgelost

Figuur 6.5 Schematische weergave knelpunten 'de CIE-ovj'.

De Wpolg heeft in het systeem van controle en toezicht door de CIE-ovj vrijwel geen wijzigingen doorgevoerd. Dat is gelet op de sterke positie die de CIE-ovj van nature heeft vanuit het wetboek van strafvordering en het succes van zijn controlerende en toezichthoudende taken in de praktijk begrijpelijk. Juist vanwege het succes van de wijze waarop hij controle en toezicht uitvoert, had het ons inziens echter in de lijn der verwachting gelegen als de CIE-ovj een formeel wettelijke positie in de Wpolg had gekregen. Dat had de positie van de CIE-ovj verder kunnen verstevigen.

Wel komt de Wpolg tegemoet aan het knelpunt dat niet is voorzien in een mogelijkheid om de bevoegdheden van de CIE-ovj te mandateren aan een specialistische parketsecretaris. Daarmee komt de Wpolg tegemoet aan een wens die in de praktijk leeft, maar waarvoor de instructies onder de Wpolr geen ruimte boden.

Voorts merken wij hier op dat de controle en het toezicht van de CIE-ovj zich aan het gezichtsveld van de burger lijkt te onttrekken. Vanzelfsprekend kan hij niet te veel uitweiden over hetgeen bij de CIE wordt verwerkt, maar van de bevindingen van de CIE-ovj wordt geen verslag gemaakt dat openbaar wordt. Ook als hij een normschending constateert die zich al jaren voordoe, komt dat in beginsel niet naar buiten. Dit is het geval omdat bij het

moment waarop de officier van justitie verantwoording aflegt over zijn handelen, het strafproces, de verwerking van politiegegevens geen rol van betekenis speelt. We behandelen dit in sectie 6.7.

6.7 DE STRAFRECHTER

Naast de CIE-ovj als rechtsstatelijk controle- en toezichtsmechanisme kennen we vanzelfsprekend de strafrechter als controleur van politieke werkzaamheden. Kort gezegd heeft de strafrechter een controlerende taak op het moment dat een strafzaak voorkomt, waarbij de wijze waarop de politie het opsporingsonderzoek heeft gedaan ook onderwerp van onderzoek is.

We bespreken achtereenvolgens het theoretisch kader van de controlerende taak van de strafrechter onder de Wpolr (subsectie 6.6.1), de daarbij geconstateerde knelpunten (subsectie 6.6.2), de uitwerking van de rol van de strafrechter onder de Wpolg (subsectie 6.6.3), en eindigen met een tussenconclusie (subsectie 6.6.4).

6.7.1 Theoretisch kader

De gevolgen die in de strafrechtpraktijk worden toegekend aan een normschending volgens de Wpolr worden in sterke mate beïnvloed door het feit dat de wet haar grondslag vond in de privacybenadering. De Hoge Raad stelde zich namelijk op het standpunt dat de normen uit de Wpolr niet strekken tot de bescherming van het strafvorderlijk belang van de verdachte.⁴²⁶ Schending van de normen uit de Wpolr resulteren in een strafprocedure in beginsel dus niet in bewijsuitsluiting of niet-ontvankelijkheid van het OM.⁴²⁷ Dat is in lijn met de Europese rechtspraak over de doorwerking van privacyschendingen in het strafproces. Het is vaste rechtspraak van het EHRM dat schendingen van het recht op privacy (art. 8 EVRM) niet direct leidt tot een schending van het 'fair trial' beginsel (art. 6 EVRM). Daarvoor moet volgens het EHRM worden gekeken naar het strafproces als geheel.⁴²⁸

De Hoge Raad laat op soortgelijke wijze de achterdeur openstaan. Onder omstandigheden kunnen schendingen van de normen uit de Wpolr namelijk niet meer verenigbaar zijn met een eerlijke procesvoering.⁴²⁹ Thans moet een dergelijke exceptiemogelijkheid bekeken worden in het licht van de Wet vormverzuimen, die na het aangehaalde arrest van de Hoge Raad in werking is getreden en ook thans onder het regime van de Wpolg nog van kracht

⁴²⁶ HR 7 februari 1995, NJ 1995, nr. 308.

⁴²⁷ HR 7 februari 1995, NJ 1995, nr. 308 r.o. 5.7. Zie ook Van der Bel e.a., 2007, p. 63-64.

⁴²⁸ EHRM 12 juli 1988 (Schenk). Uitgebreid herhaald in EHRM 12 mei 2000 (Khan), NJCM-bulletin 2000, p. 1255-1261.

⁴²⁹ HR 7 februari 1995, NJ 1995, nr. 308. Bespreking arrest: Goos, 1995, p. 132-133.

is.⁴³⁰ Schending van de normen uit de Wpolr wordt in strafrechtelijke zin geduid als het verzuim van vormen. Indien een vormverzuim niet meer hersteld kan worden, heeft de rechter de bevoegdheid de straf te verminderen, de resultaten van het betreffende onderzoek te laten uitsluiten van bewijs of het OM niet-ontvankelijk te verklaren.⁴³¹ Tevens kan de rechter alleen constateren dat vormen zijn verzuimd, zonder daaraan een direct gevolg te verbinden.⁴³² De rechter behoeft een dergelijk onderzoek niet ambtshalve uit te voeren. Het ligt op de weg van de verdediging om, aan de hand van het beoordelingskader dat in lid 2 van art. 359a Sv is gegeven, aan te tonen dat vormen zijn verzuimd en welke sanctie aan dat verzuim dient te worden verbonden.⁴³³ Daarbij moet rekening worden gehouden met 'het belang dat het geschonden voorschrift dient', 'de ernst van het verzuim' en het 'daardoor veroorzaakte nadeel'.⁴³⁴ Hier is met name de eerste wegingsfactor interessant. In lijn met de aangehaalde uitspraak van de Hoge Raad ligt het voor de hand te veronderstellen dat aan een schending van de normen uit de Wpolr geen sanctie zal worden verbonden. Immers, de normen uit de Wpolr beschermen niet het strafvorderlijk belang van de verdachte. In die redenering is de conventie dat 'het belang dat het geschonden voorschrift dient' niet strafprocesrechtelijk is.

6.7.2 De knelpunten beschreven

Wij vragen ons af of deze conventie onder invloed van technologische en maatschappelijke ontwikkelingen niet achterhaald is. Thans worden de gevolgen van de toenemende druk op de grondrechten uitsluitend vanuit privacyperspectief benaderd. De besproken ruimere grondslagen tonen aan dat die benadering te beperkt is. Ten eerste doet het gebruik van persoonsgegevens door de politie afbreuk aan het gehele scala aan grondrechten en niet alleen aan de privacy. Ten tweede neemt het beschermingsdoel aan belang af en komt de nadruk steeds meer op de bevoegdheidstoedeling te liggen. Deze onterechte beperking merken we als knelpunt aan.

De onterechte beperking tot privacy heeft gevolgen voor de strafprocesrechtelijke consequenties die aan een normschending uit de Wpolr verbonden zijn. Zoals beschreven, wordt onder verwijzing naar de privacygrondslag van de Wpolr, het strafvorderlijk belang voor de verdachte ontkend en zijn er tot op heden geen strafvorderlijke consequenties aan dergelijke normschendingen verbonden. Die redenering is naar onze mening achterhaald. Het beschermingsobject betreft immers niet alleen privacy.

430 Wet van 14 september 1995, *Stb.* 441, tot wijziging van het Wetboek van Strafvordering (Wet vormverzuimen).

431 Art. 359a lid 1 onder respectievelijk a, b, c Sv

432 zie bijvoorbeeld gerechtshof 's-Gravenhage, 23 april 2004, *LJN* AO9376..

433 HR 30 maart 2004, *LJN* AM2533.

434 Art. 359a lid 2 Sv.

6.7.3 Uitwerking onder de Wpolg

De wetgever heeft over dit onderwerp niets in de Wpolg opgenomen en daaraan ook geen aandacht besteed in de memorie van toelichting. De Wpolg is naar onze mening echter wel een stille getuige van het feit dat informatie mede onder invloed van maatschappelijke en technologische ontwikkelingen een steeds prominentere rol gaat spelen in de opsporing. We hebben de ontwikkeling van deze technieken reeds in subsectie 3.2.4 besproken. We hebben de toepassing van die technieken (zoals *datamining* en *machine learning*) daar geduid met de term *informatieele opsporingsmethoden*. We wijzen in dit verband nogmaals op de onderzoeken die door Koelewijn en bijvoorbeeld VanderLooy zijn uitgevoerd over de toepassing van geavanceerde ICT-technieken om verbanden te ontdekken die anders verborgen zouden blijven.⁴³⁵ Dit brengt met zich mee dat de bevoegdheden die het gebruik van die informatie reguleren (de Wpolg) steeds meer het strafvorderlijk belang van de verdachte gaan dienen.

6.7.4 Tussenconclusie aangaande de strafrechter

Alvorens we onze tussenconclusie aangaande de controle en het toezicht door de strafrechter formuleren, geven we schematisch weer (a) het aantal onder de Wpolr geconstateerde knelpunten, (b) de inhoud van die knelpunten, (c) de uitwerking daarvan onder de Wpolg, en (d) de (te verwachten) resultaten van de uitwerking onder de Wpolg.

Aantal	Knelpunten Wpolr	Wpolg	Resultaat
1	Geen strafvorderlijk belang	–	Knelpunt niet opgelost

Figuur 6.6 Schematische weergave knelpunten ‘de strafrechter’.

De informatiemaatschappij heeft zich inmiddels zo ver ontwikkeld dat de stelling van de Hoge Raad, dat bij de verwerking van politiegegevens geen strafvorderlijke belangen in het geding zijn, naar onze mening is achterhaald. De normen uit de Wpolg kunnen wel degelijk het strafvorderlijk belang van de verdachte dienen. Met die constatering rijst de vraag welke consequenties dan wel aan normschendingen zouden moeten worden verbonden.

Om tot een dergelijke bepaling te komen maken we een vergelijking met soortgelijke bevoegdheden: de bijzondere opsporingsbevoegdheden. De overeenkomst daarmee vloeit voort uit het feit dat daaraan eenzelfde afweging ten grondslag ligt. Door beide regelingen wordt bescherming geboden aan het gehele scala van grondrechten tegen een te verre gaande inmenging daarin door de politie. Laten we eerst vaststellen dat inmengingen belang-

⁴³⁵ Koelewijn, 2009. VanderLooy, 2009.

rijke instrumenten zijn voor de opsporing en daarom hun grondslag vinden in het Wetboek van Strafvordering. Ook in de mate van ingrijpendheid zijn er overeenkomsten tussen de bevoegdheden uit de Wbob en de bevoegdheden uit de Wpolg. Zo is de in de vorige subsectie beschreven gerichte datamining een zwaar middel waarvoor, net als met de toepassing van een bijzondere opsporingsbevoegdheid, de toestemming van een officier van justitie vereist is. Die toestemming is gewenst omdat het gaat om een ingrijpende opsporingsbevoegdheid die inbreuken maakt op de grondrechten van de verdachte. Daarnaast is *gerichte datamining*, net als bijvoorbeeld een telefoontap, niet ondersteunend. Beide opsporingsbevoegdheden hebben namelijk tot doel nieuwe kennis te verkrijgen. Dit kan tot een verregaande inmenging leiden.

Vreemd genoeg worden aan normschendingen uit de Wbob in beginsel wel sancties verbonden.⁴³⁶ De Wbob-normen beschermen dus wel het strafvorderlijk belang van de verdachte, terwijl de normen uit de Wet politieregisters dat niet doen. Dat verschil wordt echter op geen enkele wijze gerechtvaardigd. De in het geding zijnde belangen zijn immers hetzelfde. Om de opmerkelijkheid daarvan te laten zien, draaien we de redenering om: bij een onrechtmatige huiszoeking wordt ook niet gesteld dat de verdachte daardoor wel in zijn privacy is getroffen, maar dat de vrucht van die huiszoeking vervolgens toch gebruikt mag worden in de strafprocedure.⁴³⁷ Die redenering wordt met betrekking tot de normen uit de Wpolg wel gehanteerd. Ondanks dat de grondslagen van de Wpolg daarvoor geen enkele aanleiding geven, worden ze daarvoor wel als doorslaggevend argument gebruikt. Het privacyrecht wordt dan misbruikt om niet in de rechtmatigheidsbeoordeling van een gegevensverwerking te behoeven treden.

6.8 BEANTWOORDING OV₂ EN OV₃ AANGAANDE CONTROLE EN TOEZICHT

In dit hoofdstuk zijn de controle en het toezicht op de informatieverwerking door de CIE-en besproken. Daarbij is een antwoord gegeven op OV₂ en OV₃ voor zover het controle en toezicht als waarborg betreft. Ov₂ luidt: *“Welke knelpunten zijn er in de literatuur en de praktijk geconstateerd ten aanzien van de waarborgende werking van de Wet politieregisters?”* en Ov₃ luidt: *“In hoeverre komt de Wet politiegegevens, mede in het licht van de ervaringen met de Wet bescherming persoonsgegevens, tegemoet aan deze knelpunten?”* In het hoofdstuk hebben we beschreven op welke wijze de Wpolg tegemoet komt aan de onder de Wpolr geconstateerde knelpunten als het gaat om controle en toezicht door (1) de verantwoordelijke, (2) de privacyfunctionaris, (3) het CBP, (4) protocollering en auditing, (5) de CIE-ovj, en (6) de strafrechter.

⁴³⁶ Corstens, 2008, p. 704-716.

⁴³⁷ Zie bijvoorbeeld: HR 21 oktober 2003, LJN AH9998.

In deze hoofdstukconclusie herhalen we niet alle geconstateerde individuele knelpunten, maar abstraheren we ze tot een hoger niveau. Het gaat ons inziens dan over één punt, namelijk een te grote versnippering van de verantwoordelijkheid voor de controle en het toezicht.

Versnippering

Er zijn zes personen en instanties die controle en toezicht uitvoeren op de verwerking van persoonsgegevens. Het knelpunt dat bij vrijwel bij elke persoon en instantie terugkeert is het feit dat er een capaciteitsgebrek is. We zagen bij de chef CIE, die namens de verantwoordelijke toezicht houdt op de verwerking van persoonsgegevens, dat hij tijd tekortkomt om controle en toezicht op een adequaat niveau te kunnen uitvoeren. Hetzelfde geldt feitelijk voor de privacyfunctionaris, de functionaris gegevensbescherming, en het CBP. Deze instanties hebben het gehele politieveld als werkgebied en de CIE is daar slechts een klein onderdeel van. Het is voor hun eenvoudigweg praktisch onmogelijk om op regelmatige basis hun werk bij de CIE uit te voeren. Hetzelfde lijkt in zekere zin (zij het in mindere mate) te gelden voor de CIE-ovj die zijn taken moet delegeren aan een gespecialiseerde parketsecretaris. Bovendien blijft het resultaat van zijn werk voor ons verborgen, omdat de strafrechter zijn ogen wenst te sluiten voor wat er zich bij de CIE heeft afgespeeld met de persoonsgegevens van de verdachte. Ten slotte lijkt het systeem van protocollering en daarmee ook het systeem van auditing gehinderd door de automatisering die het opslaan van de informatie lastig maakt.

Al met al zijn er in potentie een aantal zeer sterke controle- en toezicht-mechanismen. Het succes daarvan lijkt in elk van de gevallen echter in te moeten boeten door een gebrek aan capaciteit. De manier waarop de controle en het toezicht op de verwerking van politiegegevens bij de CIE thans is vormgegeven, is naar onze mening te versnipperd. De Wpolg lost voor de individuele controle- en toezichtmechanismen weliswaar een aantal praktische knelpunten op, maar niet op het punt van de capaciteit. Integendeel, het systeem onder de Wpolg raakt door de invoering van de functionaris gegevensbescherming en de verplichte auditing meer versnipperd dan onder de Wpolr.

Geen van de genoemde personen en instanties is in staat om inhoudelijk, bij iedere regio en op regelmatige basis, toezicht te kunnen houden. Er is te gemakkelijk een aantal mechanismen in de wet opgenomen, zonder dat specifiek voor de CIE wordt bepaald of die in de praktijk ook effect zullen hebben. Wij begrijpen niet dat voor toezicht binnen de politie maar liefst een privacyfunctionaris, een functionaris gegevensbescherming, het CBP, een onafhankelijke EDP-audit, en een CIE-ovj nodig zijn om effectief toezicht te kunnen houden. Zeker nu capaciteitsgebrek bij de meerderheid van deze personen en instanties een knellend probleem blijkt te zijn waar de Wpolg geen oplossing voor biedt, is aanpassing van deze mechanismen aangewezen. Dat moet wat ons betreft gezocht worden in kwantitatieve versobering enerzijds en kwalitatieve investering anderzijds. Met andere woorden, minder mensen, maar wel mensen die meer tijd hebben voor de CIE specifiek. We komen hier in onze conclusies en aanbevelingen nader op terug.

Dit hoofdstuk beoogt aan de hand van drie onderzoeksvragen een antwoord te formuleren op de probleemstelling die centraal staat in dit onderzoek. De probleemstelling luidde als volgt.

In hoeverre waarborgt de Wet politiegegevens de goede uitvoering van de politietaak en de grondrechten van de burger effectiever dan de Wet politieregisters?

Wij beginnen de beantwoording van de probleemstelling door allereerst in sectie 7.1 de eerste onderzoeksvraag (OV1) te beantwoorden. Daarmee werd beoogd inzicht te geven in de belangen die betrokken zijn bij het verwerken van politiegegevens door de CIE-en. Voorts beantwoorden wij in sectie 7.2 de tweede onderzoeksvraag (OV2), die zag op de in de praktijk en in de literatuur geconstateerde knelpunten ten aanzien van de waarborgende werking van de Wet politieregisters. In sectie 7.3 wordt vervolgens antwoord gegeven op de vraag in hoeverre de Wet politiegegevens aan de geconstateerde knelpunten tegemoet komt. Daarbij worden voor zover mogelijk de ervaringen die reeds met de Wet bescherming persoonsgegevens zijn opgedaan betrokken.

De inhoud van de secties 7.1 tot en met 7.3 geeft ons voldoende inzicht om een antwoord, of een aanzet daartoe, te kunnen geven op de centrale probleemstelling.

7.1 DE BELANGEN BIJ POLITIËLE GEGEVENSVERWERKING

Onze eerste onderzoeksvraag luidde als volgt.

Op welke wijze zijn de politietaak en de grondrechten van de burger betrokken bij het verwerken van politiegegevens?

Bij het eerste betrokken belang, de goede uitvoering van de politietaak, hebben we een toenemende instrumentalistische benadering gesignaleerd. Daarbij hebben we geconstateerd dat de politiële gegevensverwerking bij een goede uitvoering van de politietaak de administratieve en ondersteunende functie inmiddels is ontstegen en als zelfstandig opsporingsmiddel dient te worden aangemerkt. Verstrekkende bevoegdheden tot het verwerken van gegevens dienen in sommige gevallen zelfs te worden aangemerkt als *informatieele opsporingsmethoden*. Dat brengt ook met zich mee dat de inzet van deze bevoegdheden met de gebruikelijke strafvorderlijke waarbor-

gen omkleed dient te worden. Dat is onder de Wpolg feitelijk al deels al het geval, aangezien voor de inzet van enkele van deze informationele opsporingsmethoden de voorafgaande toestemming van de CIE-ovj vereist is. Hiermee ontdoet de Wpolg zich van zijn privacyjas en krijgt de politieke gegevensverwerking dus een expliciete strafvorderlijke betekenis. Deze constatering heeft tot gevolg dat het tegenwicht dat het tweede betrokken belang, het beschermingsbelang, tegen de instrumentele functie van de Wpolg moet leveren om een adequaat niveau van rechtsbescherming te bieden onder de Wpolg ook groter dient te zijn dan onder de oude Wpolr.

We hebben laten zien dat het beschermingsbelang van het gegevensbeschermingsrecht ten tijde van de Wpolr vrijwel uitsluitend vanuit het privacyperspectief werd benaderd. Met de komst van de ontwikkelingen op het gebied van informatie- en communicatietechnologie heeft daarin een verschuiving plaatsgevonden. Deze ontwikkelingen hebben tot gevolg dat het gegevensbeschermingsrecht zich steeds meer de status van een zelfstandig grondrecht is gaan aanmeten. De belangen die op het spel staan bij de verwerking van persoonsgegevens zijn immers niet alleen privacybelangen, maar beslaan een breder scala aan grondrechten. Het heeft ertoe geleid dat wij hebben moeten concluderen dat vanuit beschermingsoogpunt het gegevensbeschermingsrecht een zorgvuldige gegevensverwerking vereist. Het gaat om meer dan privacy alleen. Mede om die reden is de privacyjas van het gegevensbeschermingsrecht te klemmend. Het gaat mogelijk zelfs om een nieuw grondrecht: *het recht op vrijheid van gegevens*.

Voorts hebben we beschreven dat voor beide belangen de sturende rol van de technologiegestuurde ontwikkeling leidend is. Technologische ontwikkelingen geven meer instrumentele mogelijkheden. Daarom kunnen gegevens (bijna) optimaal voor de uitvoering van de politietaken ingezet worden. Tegelijkertijd stelt de samenleving hogere eisen aan de maatregelen die de vrijheid van gegevens moet waarborgen. De technologische ontwikkeling vormt geen zelfstandig belang dat gediend dient te worden door wetgeving als de Wpolg, maar zij is wel een afgeleid belang doordat het zo'n belangrijke sturende werking heeft in het denken over de betrokken belangen bij de inzet van gegevensverwerkingen. Bij de ontwikkeling van (1) de wijze waarop uitvoering wordt gegeven aan de politietaken en (2) de wijze waarop het recht van vrijheid van gegevens zich ontwikkelt, hebben we gezien dat de stand van de techniek daarin bepalend is. Dit brengt ons tot de conclusie dat vanuit die achtergrond gekeken moet worden naar de maatregelen die de belangen die met de Wpolg gediend worden, te beschermen.

Zodoende kunnen we bepalen of in het huidige tijdsgewricht met de drie bestaande waarborgen (de wet, het kennisnemingsrecht, en controle en toezicht) kan worden volstaan of dat het tempo van de technologische ontwikkelingen verschuiving of uitbreiding van die waarborgen noodzakelijk maken.

7.2 KNELPUNTEN AANGAANDE DE WAARBORGENDE WERKING VAN DE WPOLR

Onze tweede onderzoeksvraag luidde als volgt:

Welke knelpunten zijn er in de literatuur en de praktijk geconstateerd ten aanzien van de waarborgende werking van de Wet politieregisters?

In de hoofdstukken 4, 5 en 6 zijn de onder de werking van de Wpolr geconstateerde knelpunten behandeld. Hier herhalen we niet alle geconstateerde individuele knelpunten, maar abstraheren we ze tot een hoger niveau. Het gaat dan om (1) instrumentele knelpunten, (2) vaagheid in de regelgeving (3) capaciteitstekort en (4) versnippering. We behandelen deze achtereenvolgens in de subsecties 7.2.1 tot en met 7.2.4.

7.2.1 Instrumentele knelpunten

Een van de redenen om tot vervanging van de Wpolr over te gaan was het feit dat de wet niet meer aansloot op de wensen van de politiepraktijk. We hebben gezien dat dit op een aantal punten het geval was. Zonder volledigheid na te willen streven noemen we hier (1) het onderscheid tussen het voorlopig register en het zwacri-register, (2) de knellende bewaartermijnen, (3) de beperkte toegang tot het informantenregister, (4) het gebrek aan enige regeling rond het analyseren, en (5) de gebrekkige regeling rond het koppelen van gegevens.

Wat de laatste twee knelpunten betreft, geldt dat deze ook als zodanig voor de bescherming van de vrijheid van gegevens aangemerkt dienen te worden. Nu niet duidelijk is bepaald wat de CIE-en in dit kader met hun gegevens mogen doen, is het voor degenen wiens gegevens daarbij worden betrokken ook niet te voorzien wat er met hun gegevens gaat gebeuren. De knelpunten doen daarmee afbreuk aan hun rechtszekerheid.

7.2.2 Vaagheid in de regelgeving

Als veruit het belangrijkste knelpunt in het verwerkingsregime onder de Wpolr is de vaagheid van de regeling naar voren gekomen. Dit werd vooral veroorzaakt door het gebruik van het begrip 'noodzakelijkheid' als voorwaarde voor de toepassing van bepaalde bevoegdheden in het verwerken van politiegegevens. Noodzakelijkheid als voorwaarde kwam onder de Wpolr terug bij de activiteiten bewaren, de weigeringsgrond voor het verstrekken van informatie, het koppelen, en het analyseren. Ook bij de het opslaan zagen we dat er zich in de praktijk problemen voordoen bij de interpretatie van de wettelijk bepaalde categorieën. Bij de vraag wanneer een verzoek om kennisneming geweigerd kon worden, zagen we eveneens het probleem van de vage normen.

Vaagheid in een regeling is om een veelheid van redenen onwenselijk. Het heeft het gevaar in zich dat door verschillende vormen van toepassing rechtsongelijkheid wordt gecreëerd en normen worden toegepast op een manier die op dat moment het beste resultaat oplevert, het gaat dan juridisch gesproken over willekeur.

Aan de andere kant hebben we in onze korte uitstap naar de Wbp gezien dat daar vanuit de praktijk de vaagheid in de toepassingsvoorwaarden van de Wbp als noodzakelijk werd gezien. Het maakt een flexibele toepassing van de wet mogelijk en geeft de ruimte om in te springen op nieuwe technologieën. Dat maakt het gebruik van bijvoorbeeld de noodzakelijkheid als voorwaarde niet per definitie problematisch. Het vraagt echter wel meer van de praktijk om zelf invulling te geven aan die vage normen. Om daarbij zoveel mogelijk tegemoet te komen aan de nadelen die kleven aan een dergelijke systematiek heeft het onze grote voorkeur om dit op een gezamenlijk niveau te doen, zodat niet iedere gegevensverwerker zich moet buigen over de invulling van die normen.

7.2.3 Capaciteitstekort

In de toepassing van de normen uit de Wpolr hebben we gezien dat vanwege de vaagheid in de normen van de Wpolr de werkdruk tot problemen leidt. Er is bij de CIE niet genoeg capaciteit aanwezig om alle gegevens individueel op noodzakelijkheid te toetsen als het bijvoorbeeld gaat om vaststelling van de bewaartermijn. Dit brengt met zich mee dat er keuzes gemaakt dienen te worden door de CIE aan welke van haar werkzaamheden prioriteit gegeven dient te worden. De grondslag voor die keuze is een beleidsmatige en politieke en gaat buiten de reikwijdte van dit onderzoek. In onze context volstaat het om vast te stellen dat de vaagheid in het verwerkingsregime van de Wpolr dusdanig veel tijd kost dat de CIE-en erdoor in de problemen komen.

Hetzelfde knelpunt komen we tegen bij de uitvoering van het kennisnemingsrecht. Daar hebben we gezien dat er slechts een bescheiden aantal verzoeken per jaar wordt gedaan bij de afzonderlijke CIE-en. De verzoeken die evenwel gedaan worden, zorgen voor een aanzienlijke personele belasting. Dit zorgt er vanzelfsprekend voor dat de tijd die een CIE aan de afwikkeling van een dergelijk verzoek besteedt niet voor andere werkzaamheden ingezet kunnen worden.

Ook bij de uitwerking van de verschillende controle- en toezichtmechanismen hebben we gezien dat het gebrek aan capaciteit een terugkerend knelpunt was. Niet alleen de CIE zelf, maar ook de externe toezichthouders hebben niet voldoende menskracht om op structurele basis hun controlerende en toezichthoudende taken uit te voeren. Daarbij speelt de werkdruk van de CIE een rol, maar ook het feit dat de verwerking van politiegegevens door de CIE slechts een van de vele politieke gegevensverwerkingen is en de menskracht van de diverse toezichthouders buiten de CIE daarover verdeeld dient te worden.

7.2.4 Versnippering

Als derde algemene knelpunt onder de Wpolr kunnen we constateren dat er sprake is van versnippering in (1) de uitvoering van de taken door de CIE en (2) de wijze waarop de controle en het toezicht zijn vormgegeven.

Ten eerste zijn er vanwege de opgezette politiestructuur in totaal 33 CIE-en in Nederland, die allemaal dezelfde registers voeren. Elk van deze CIE-en loopt daarbij tegen dezelfde problemen aan, onder meer op het gebied van interpretatie van de normen uit de Wpolr. Die regionale structuur draagt eraan bij dat de vaagheid van de normen tot een capaciteitsgebrek leidt. Iedere CIE is zelf bezig de normen in de praktijk toe te passen, zonder dat daarbij op een structurele wijze is voorzien in een manier om de in de praktijk opgedane kennis over de toepassing van het regelgevend kader met elkaar te delen.

Als het gaat om de uitvoering van controle en toezicht op de gegevensverwerking door de CIE-en zien we dat daarmee onder de Wpolr vier personen en instanties zijn belast. Het gaat dan om de korpsbeheerder (als verantwoordelijke), de privacyfunctionaris, het CBP, en de CIE-ovj. Geen van deze is als gevolg van voornoemde capaciteitsproblemen in staat om ook daadwerkelijk effectief toezicht te houden. De CIE-ovj lijkt daarbij het dichtste in de buurt te komen, maar ten aanzien daarvan hebben we gezien dat ook hij gedwongen is zijn taken te mandateren en dat hij daarnaast geen verantwoording naar buiten toe aflegt over de resultaten van zijn controlerende werkzaamheden. De versnippering van de controle- en toezichtwerkzaamheden draagt naar onze overtuiging bij aan deze situatie. Doordat er vier personen en instanties zijn die elk een eigen rol en invalshoek hebben bij het uitvoeren van die werkzaamheden, heeft geen van die personen en instanties het overzicht over de algemene problemen die zich bij de gegevensverwerking door de CIE-en in Nederland voordoen. Ook heeft geen van de genoemde personen en instanties een overkoepelende rol toebedeeld gekregen.

7.3 TEGEMOETKOMINGEN IN DE WPOLG

Onze derde onderzoeksvraag luidde als volgt:

In hoeverre komt de Wet politiegegevens, mede in het licht van de ervaringen met de Wet bescherming persoonsgegevens, tegemoet aan de geconstateerde knelpunten?

In deze sectie beantwoorden we de vraag of en zo ja op welke manier de Wpolg aan de in de vorige sectie omschreven knelpunten tegemoetkomt. Ook hier gaan we uit van (1) instrumentele knelpunten, (2) vaagheid in de regelgeving, (3) capaciteitstekort, en (4) de versnipperde controle- en toezichtmechanismen. We behandelen deze achtereenvolgens in de subsecties 7.3.1 tot en met 7.3.4.

7.3.1 Instrumentele knelpunten

De onder de Wpolr geconstateerde knelpunten deden zich met name voor in het verwerkingsregime (hoofdstuk 4) en enkele bij de controle- en toezichtmechanismen. De Wpolg biedt daarvoor goeddeels een aanvullende of gewijzigde regeling. De wijzigingen in de Wpolg bestaan uit (1) het verwijderen van een bepaalde verwerkingsgrond, (2) het wijzigen van een verwerkingsregeling, en (3) een toevoeging aan het verwerkingsregime.

Bij het verwijderen van een verwerkingsgrond denken we met name aan de verwijdering van het voorlopig register (of een soortgelijke verwerkingsgrond) uit het verwerkingsregime. De praktijk had problemen met de afbakening tussen dat register en het zwacri-register. Onder de Wpolg valt elk van deze gegevensverwerkingen onder het regime van de zwacri-verwerking.

Als het gaat om het wijzigen van het verwerkingsregime dan gaat het veelal om knelpunten die met een wetstechnische wijziging van het bestaande verwerkingsregime konden worden opgelost. We noemen het wijzigen van de bewaartermijnen, die door de praktijk als te knellend werden ervaren. Daarnaast is bij het horizontale verstrekkingsregime de zogenaamde *free flow* explicieter in de regeling opgenomen. Ten slotte noemen we de toegenomen bevoegdheden van het CBP in de uitoefening van haar controle- en toezichtwerkzaamheden.

Wat de toevoegingen aan het verwerkingsregime betreft kunnen we wijzen op de regeling rond het informantenregister en de regeling voor het analyseren van gegevens. Deze verwerkingsgronden werden onder de Wpolr gemist. Ter compensatie waren evenwel juridische noodverbanden aangelegd. Daarnaast kent de Wpolg ook de toevoeging van een aantal nieuwe verwerkingsgronden die niet zozeer uit een knelpunt van de Wpolr voortkwamen, maar die nodig werden geacht om in de toekomst voldoende tegemoet te kunnen komen aan de instrumentele belangen van de politieke gegevensverwerking. We denken dan met name aan de in de Wpolg opgenomen themaverwerking.

Met deze verwijderingen, wijzigingen en toevoegingen in het verwerkingsregime komt de Wpolg aan een aantal prangende knelpunten uit de politiepraktijk tegemoet (zie hoofdstuk 6).

7.3.2 Vaagheid in de regelgeving

Naast de instrumentele knelpunten zagen we onder de Wpolr een meer fundamenteel knelpunt dat de vaagheid van de toepassingsvoorwaarden in het verwerkingsregime betrof. Onder de Wpolg blijft de vaagheid in de normering van de gegevensverwerking door de CIE evenwel bestaan. De wetgever heeft zich wederom bediend van begrippen zoals noodzakelijkheid. Bovendien blijft het onderscheid tussen verdachten, betrokkenen, en contacten net zo vaag als het was. Al met al blijft in de toepassingsvoorwaarden de vaag-

heid een grote factor van betekenis. Dit geldt ten eerste op punten waarvan reeds onder de Wpolr was geconstateerd dat deze tot toepassingsproblemen hebben geleid, maar ten tweede zien we dat de Wpolg ook nieuwe regelingen introduceert waarbij toepassingsproblemen te verwachten zijn (onder andere (1) themaverwerking en (2) de koppeling van de 5-jaar-bewaartermijn aan de noodzakelijkheid). Kort gezegd blijft daarmee onduidelijk wanneer de (ruimere) bevoegdheden door de politie mogen worden ingezet. Hetzelfde geldt voor de weigeringsgrond bij de afwikkeling van kennisnemingsverzoeken, ook daarin blijft de Wpolg vasthouden aan dezelfde vage criteria als onder de Wpolr.

Op zichzelf hoeft het hanteren van vage termen geen probleem te zijn. Het onderzoek dat in de praktijk naar de uitwerking van de Wbp is gedaan maakt duidelijk dat juist het gebruik van vage normen ook mogelijkheden biedt voor de praktijk om die bevoegdheden flexibel in te zetten. Daarbij is dan wel een nadere interpretatie van die open en vage normen vereist en de invloed van een overkoepelende organisatie gewenst. Op die manier kunnen vage normen in de praktijk nader worden ingevuld aan de hand van bijvoorbeeld *'best practices'* en worden aan de praktijk handvatten geboden voor de toepassing van die vage normen. Die handvatten geeft de wetgever in het geval van de Wpolg niet of nauwelijks. Zoals het nu beschreven is, wordt in de memorie of lagere regelgeving nauwelijks ingegaan op de manier waarop deze vage termen moeten worden toegepast. Dat betekent dat de uitleg van de vage normen aankomt op de praktijk. Het gaat dan om de CIE-praktijk en de personen en instanties die daarop toezicht houden, hetgeen capaciteit zal kosten. In hun samenwerking zal immers de uitleg van die vage normen tot stand dienen te komen.

Als het gaat om vaagheid in toepassingsvoorwaarden zien we dat de Wpolg een oplossing heeft geboden voor de lastige afbakening tussen het voorlopige register en het register zware criminaliteit. Dat heeft zij echter gedaan door afschaffing van het voorlopig register, zodat van een fundamentele oplossing, die ook bij andere vaagheidsknelpunten gebruikt kan worden, niet gesproken kan worden.

Resumerend kan op het gebied van de vaagheid van regelgeving worden geconcludeerd dat de Wpolg geen effectievere waarborgen biedt dan de Wpolr. Integendeel, de Wpolg bedient zich op meer plekken dan de Wpolr van begrippen waarvan onder de Wpolr reeds was gebleken dat de praktijk moeite heeft met de toepassing daarvan.

7.3.3 Capaciteitstekort

Met aanvullende wetgeving wordt vanzelfsprekend niet het capaciteitsprobleem bij de CIE-en en de toezichthouders opgelost. Dat is een kwestie van beleid en van de politiek, die de budgetten mogen vaststellen. Het is duidelijk dat de budgetten die daarvoor beschikbaar zijn niet onbeperkt kunnen zijn.

Op het gebied van wetgeving is de uitdaging er dan ook in gelegen om zorg te dragen voor een systeem van waarborgen, waarbij de beschikbare capaciteit zo efficiënt mogelijk wordt ingezet. Daar besteedt de Wpolg geen aandacht aan. Als we kijken naar de toepassingsvoorwaarden dan zien we dat de interpretatie daarvan juist meer capaciteit zal gaan kosten dan vroeger het geval was. Voorts zien we ook bij de uitwerking van het kennisnemingsrecht niet dat daar onder de Wpolg effectiever met de beschikbare capaciteit wordt omgegaan dan onder de Wpolr; ook niet nu daar feitelijk niets is veranderd. Als het gaat om de uitwerking van controle en toezicht zijn er geen grote sprongen vooruit te verwachten als het gaat om de capaciteitsinzet. Wel kan in dat verband de mandaatmogelijkheid voor de CIE-ovj worden genoemd, maar zijn taken worden ook geïntensiveerd onder de Wpolg. Verder voorziet de Wpolg alleen maar in meer controle en toezicht, zodat het meer capaciteit zal gaan kosten. We noemen in dit verband de verplichte protocollering en auditing, alsmede de functionaris gegevensbescherming.

Als het gaat om de inzet van capaciteit zal de Wpolg dan ook niet in staat zijn de knelpunten op te lossen die onder de Wpolr zijn geconstateerd. Het zal onder de werking van de Wpolg naar verwachting juist meer aan capaciteit kosten om aan de voorwaarden van de wet te voldoen. Zolang die capaciteit niet geboden wordt of gaat worden, betekent dit voor zowel het belang van de uitvoering van de politietaak als de bescherming van de vrijheid van gegevens een minder effectieve waarborging dan onder de Wpolr.

7.3.4 Versnippering

Als het gaat om de versnipperde opzet van de CIE-en door het land dan constateren we dat de Wpolg daar geen verandering in biedt. Dat is ook niet te verwachten, aangezien deze opzet het gevolg is van de Politiewet 1993 en aanpassing daarvan naar een landelijke organisatie reeds een lang discussietraject is. In dit verband is het interessant op te merken dat de Wpolg begonnen is als wettelijke begeleider van de nieuwe uniforme landelijke informatiehuishouding, die er uiteindelijk nooit gekomen is. In zoverre kan gezegd worden dat met de invoering van de Wpolg is getracht de versnippering tegen te gaan, maar dat dit uiteindelijk niet gelukt is.

Aangaande de versnippering van de controle- en toezichtmechanismen moeten we constateren dat deze onder de Wpolg juist in aantal toeneemt. Naast de vier personen en instanties die we onder de Wpolr kennen als toezichthouders (de beheerder, de privacyfunctionaris, het CBP en de CIE-ovj) zijn ook de functionaris gegevensbescherming en het systeem van protocollering en auditing ingevoerd. Elk van deze mechanismen is in potentie sterk, maar zoals we gezien hebben, zijn ze ook vrijwel allemaal beperkt door capaciteitsgebrek. Het invoeren van extra middelen is naar onze stellige overtuiging niet de manier om hier aan tegemoet te komen. Hierdoor wordt de beschikbare capaciteit juist nog meer verdeeld over de verschillende mechanisme, waardoor – zonder extra investeringen – uiteindelijk per

mechanismen minder capaciteit resteert en daarmee samenhangend ook een minder stringente controle en toezicht.

De Wpolg heeft tot gevolg dat de versnipperde CIE-organisatie in stand blijft en dat de manier waarop de controle en het toezicht wordt uitgevoerd zelfs verder versnipperd raakt. De nieuwe wet boekt ook op dit punt dus geen winst, maar zelfs verlies ten opzichte van de oude wet.

7.4 BEANTWOORDING PROBLEEMSTELLING

De resultaten van ons onderzoek zoals weergegeven in dit proefschrift en de abstrahering daarvan die we in dit hoofdstuk hebben gemaakt bieden voldoende basis om een gefundeerd antwoord te geven op de in hoofdstuk 1 geformuleerde probleemstelling, luidende:

In hoeverre waarborgt de Wet politiegegevens de goede uitvoering van de politietaak en de grondrechten van de burger effectiever dan de Wet politieregisters?

We behandelen achtereenvolgens de vraag of de Wpolg de politietaak effectiever waarborgt dan de Wpolr (subsectie 7.4.1), daarna dezelfde vraag aangaande de grondrechten van de burger (subsectie 7.4.2) en ronden af met conclusies (subsectie 7.4.3).

7.4.1 De politietaak

De Wpolg heeft een andere wijze van reguleren dan de Wpolr. Het wettelijk uitgangspunt is immers het verwerken van gegevens in plaats van politieregisters. De voorwaarden waaronder gegevens mogen worden verwerkt blijven echter grotendeels gelijk aan de voorwaarden zoals die onder de Wpolr golden. De CIE zal in haar dagelijkse praktijk dan ook niet veel verandering merken in de wijze waarop zij de gegevens verwerkt.

De Wpolg lost voor de politiepraktijk een aantal prangende knelpunten op door het verwerkingsregime op een aantal punten te wijzigen. De wijzigingen zijn echter vooral wijzigingen op detailniveau en bevatten geen fundamentele wijzigingen in de wijze waarop politiegegevens dienen te worden verwerkt. Alleen voor deze knelpunten was geen nieuwe wet nodig geweest. De knelpunten hadden met een aanpassing van de Wpolr kunnen worden doorgevoerd, zoals ook is gebeurd met de invoering van de Wbpolr.

De zingeving van nieuwe wetgeving is erin gelegen dat juist de meer fundamentele knelpunten worden aangepakt. We bedoelen met fundamentele knelpunten de knelpunten die voortkomen uit de wijze van regulering of de opzet van de regulering. We hebben aangetoond dat aangaande de verwerking van politiegegevens er zich drie van deze fundamentele knelpunten voordoen. We hebben het dan over de vaagheid in toepassingsvoorwaarden, het capaciteitsgebrek, en de geconstateerde versnippering. Met de

komst van de Wpolg hadden deze knelpunten aangepakt moeten worden, waarbij we opmerken dat aanpakken niet gelijk te stellen is met ook daadwerkelijk oplossen. We zien echter dat de Wpolg deze drie punten ongemoeid laat. De toepassingsvoorwaarden en de opzet van de regeling van waaruit de problemen voortkomen blijven in stand en de wetgever doet ook geen poging deze te verduidelijken. We zagen zelfs dat op sommige punten te verwachten is dat de geconstateerde knelpunten zich in verhevigde vorm zullen voordoen. Dit betekent dat de CIE zich in de praktijk geconfronteerd zal blijven zien met dezelfde of soortgelijke knelpunten.

7.4.2 De grondrechten van de burger

Het staat buiten kijf dat de Wpolg aan de CIE-en meer mogelijkheden biedt tot het verwerken van gegevens. Meer gegevens mogen worden opgeslagen, er mag meer met die gegevens worden gedaan en de gegevens mogen langer worden bewaard. Daarmee wordt de inbreuk op de vrijheid van de gegevens ook groter. Tegenover deze ruimere instrumentele mogelijkheden staat volgens de wetgever ook een strenger systeem van waarborgen. Echter, op grond van het nieuwe verwerkingsregime moet worden geconstateerd dat het verwerkingsregime van de Wpolg aan waarborgende werking afneemt als het gaat om de bescherming van de grondrechten van de burger of zo men wil het recht op vrijheid van gegevens. Dat vraagt dus, bij wijze van compensatie, meer van de overige twee waarborgen, het kennisnemingsrecht en de controle- en toezichtmechanismen.

Het belangrijkste geconstateerde knelpunt aangaande het kennisnemingsrecht komt voort uit de onverenigbaarheid tussen het recht op kennisneming enerzijds en de taakuitvoering van de CIE anderzijds. Dat knelpunt is door wetgeving niet op te lossen en derhalve is dat door de Wpolg dan ook niet gebeurd. Wel heeft de Wpolg een aantal procedurele knelpunten weggenomen en vormt daarmee een verbetering ten opzichte van de Wpolr. Van de waarborgende werking die van het kennisnemingsrecht uit zou moeten gaan, moet ook onder de Wpolg niet veel worden verwacht. Het recht werd onder de Wpolr immers weinig gebruikt en de invulling van die verzoeken die werden gedaan was dusdanig dat daarvan vrijwel geen waarborgende werking uitging. De wijziging in de regeling rond het kennisnemingsrecht in de Wpolg leiden niet tot de verwachting dat hierin een wijziging zal optreden. Onder de Wpolg zal er, net als onder de Wpolr, dan ook een weinig waarborgende werking uitgaan van het kennisnemingsrecht. De Wpolg zet dit middel in ieder geval niet effectiever in de Wpolr.

Dit maakt dat de noodzakelijke extra waarborgende werking door de controle- en toezichtmechanismen geboden moet worden. De Wpolg tracht dit te doen door de invoering van een aantal extra controle- en toezichtmechanismen. We hebben op dit punt echter gezien dat daarmee de knelpunten op het gebied van controle en toezicht – capaciteit en versnippering – worden versterkt in plaats van afgezwakt. Met de invoering van extra controle-

en toezichtmechanismen is het dus sterk de vraag of de effectiviteit van die controle en dat toezicht groter wordt dan onder de Wpolr. Zonder extra maatregelen, waarvan tot nu toe niet is gebleken, moet worden geconcludeerd dat dit niet het geval is.

Ten slotte is een belangrijk fundamenteel probleem dat het beschermingsbelang door de Wpolg uitsluitend vanuit privacyperspectief wordt benaderd, terwijl met de verwerking van politiegegevens meer grondrechten in het geding zijn.

7.4.3 Conclusies

In de bovenstaande twee subsecties hebben we laten zien dat de Wpolg weliswaar meer mogelijkheden biedt voor de verwerking van politiegegevens, maar dat deze ruimere mogelijkheden vooral gepaard gaan met het oplossen van praktische knelpunten. In conclusie kunnen we vaststellen dat de Wpolg de praktijk enerzijds meer mogelijkheden biedt tot het verwerken van politiegegevens. Daarmee is de politietaak gediend. Anderzijds maken die ruimere instrumentele mogelijkheden echter niet dat de politietaak daarmee effectiever gewaarborgd wordt. De Wpolg laat de mogelijkheid onbenut om de meer fundamentele knelpunten waarmee de CIE-en zich geconfronteerd zien aan te pakken en geeft daarmee uiteindelijk geen effectievere waarborging aan de uitvoering van de politietaak door CIE-en dan de Wpolr.

Als het gaat om de waarborging van de grondrechten van de burger hebben we laten zien dat zich daar soortgelijke problemen voordoen. In plaats van de fundamentele knelpunten (het bestaansrecht van het kennisnemingsrecht, alsmede versnippering van de controle en het toezicht en het daarmee gepaard gaande capaciteitstekort) aan te pakken, introduceert de Wpolg extra controle- en toezichtsmechanismen. Hierdoor zullen de knelpunten rond versnippering en capaciteit, zonder nadere maatregelen, worden versterkt.

Het voorgaande leidt tot de conclusie dat de Wpolg niet in staat is gebleken om de vrijheid van gegevens effectiever te waarborgen dan de Wpolr. Daarmee komt de Wpolg de door de wetgever gemaakte beloften niet na.

7.5 DISCUSSIE

De door ons geformuleerde antwoorden op de probleemstelling en de daarbij behorende onderzoeksvragen roepen de vraag op hoe met de onopgeloste knelpunten omgegaan zou moeten worden. Het gaat dan om (1) de vaagheid in de regelgeving, (2) het capaciteitstekort, en (3) de versnippering. In deze sectie geven we een aanzet voor een discussie over de vraag hoe de geconstateerde knelpunten kunnen worden opgelost. We gaan hieronder in de subsecties 7.5.1 tot en met 7.5.3 nader op de genoemde knelpunten.

7.5.1 Vaagheid in de regelgeving

Het eerste onopgeloste knelpunt betreft de vaagheid in de regelgeving aangaande de verwerking van politiegegevens door de CIE-en. Wij nemen de stelling in dat dit knelpunt in de wetgeving niet op te lossen is. Inherent aan het gegevensbeschermingsrecht in het domein van de CIE is dat er ruimte moet blijven voor individuele afwegingen in de op dat moment betrokken belangen bij de gegevensverwerking. Deze belangen zijn zo specifiek en afhankelijk van de omstandigheden van het geval dat dit niet vooraf in wetgeving vast te leggen is. Dat wetgeving op dit gebied vaagheden bevat, is naar onze mening een gegeven en dient geaccepteerd te worden.

Dat wetgeving op het gebied van politieke gegevensverwerking vaag is en wat ons betreft ook vaag zal blijven laat onverlet dat er voorzieningen kunnen worden getroffen die aan de bezwaren van vage wetgeving tegemoet kunnen komen. We denken aan een systeem dat voor invulling van de vage normen zorg draagt. De wijze waarop een dergelijk systeem vorm zou kunnen worden gegeven was onderwerp van onderzoek binnen het ANITA-project. Koelewijn heeft in zijn onderzoek aangetoond dat moderne ICT-technieken bij de invulling van die vage normen een belangrijke rol kunnen spelen.⁴³⁸ We hebben ook reeds gewezen op de andere onderzoeken uit het ANITA-project van Teepe⁴³⁹, Aldewereld⁴⁴⁰, en Dijkstra⁴⁴¹, waarmee de bevindingen van Koelewijn vanuit de informatica kunnen worden onderschreven.

Daarnaast dient een instantie op nationaal niveau te worden opgericht die, gevoed door problemen uit de praktijk, nadere invulling geeft aan de open normen. De CIE-en kunnen in hun dagelijkse praktijk vervolgens aansluiting zoeken bij deze nadere invulling. Over de vormgeving van die nationale instantie die voor nadere invulling van de normen zorg draagt zal een discussie op gang moeten worden gebracht. Noodzakelijk is wat ons betreft in ieder geval een nauwe betrokkenheid van CIE-en, aangezien zij de input zullen moeten leveren over de belangen die spelen bij de invulling van de betreffende vage normen. Betrokkenheid van het CBP, ter zekering dat voldoende rekening wordt gehouden met de implicaties van gegevensverwerkingen voor de betrokkenen, is eveneens aangewezen.

Naar onze overtuiging ligt in de aanpak van dit knelpunt besloten dat er duidelijkheid dient te komen over het beschermingsobject van het gegevensbeschermingsrecht. Pas als diepere inzichten bestaan in de precieze reikwijdte van dit beschermingsobject kan de vaagheid in de wettelijke bepalingen worden opgelost, hetzij door aanpassing daarvan, hetzij door een nadere discussie over de toepassing van de wettelijke bepaling. De reikwijdte van

438 Koelewijn, 2009, sectie 8.5.2.

439 Teepe, 2006.

440 Aldewereld, 2007.

441 Dijkstra e.a., 2007.

het beschermingsobject is naar onze overtuiging in ieder geval meer dan het recht op privacy alleen. In het uiterste geval is er zelfs sprake van een zelfstandig grondrecht dat we, bij wijze van werkhypothese, hebben geduid met het recht op vrijheid van gegevens. We hebben in hoofdstuk 3 laten zien dat de technologische ontwikkelingen een belangrijke sturende werking hebben in die reikwijdte. De technologische ontwikkelingen zullen dan ook een belangrijk onderdeel moeten vormen van de discussie over de reikwijdte van het object van bescherming in het gegevensbeschermingsrecht. In deze discussie ligt een rol weggelegd voor een ieder die zich met het gegevensbeschermingsrecht bezighoudt; wetgever, politie, justitie, toezichthouders en de wetenschap.

7.5.2 Capaciteitstekort

We hebben reeds opgemerkt dat wetgeving geen fte's aan CIE-en toebedeelt. Wel is het met wetgeving mogelijk om het gegevensbeschermingsrecht zo in te richten dat met minder fte's een gelijkwaardig beschermingsniveau kan worden behaald. We denken daarbij aan de hiervoor genoemde ICT-oplossingen, alsmede aan de nationale instantie die voor invulling van de vage regelgeving zorgt. Dit draagt eraan bij dat niet iedere individuele CIE die invulling zelf dient te geven, maar dat zij aansluiting zoeken bij de op nationaal niveau uitgezette richtlijnen voor de invulling.

Verder stellen wij een herinrichting van het kennisnemingsrecht voor. De huidige invulling is een kopie van het systeem zoals we dat onder de Wbp kennen. We hebben echter reeds gezien dat zelfstandige kennisneming door een betrokkene zich niet goed verhoudt met de taakuitvoering door de CIE. De selectie die als gevolg van deze onverenigbaarheid moet worden gemaakt is bijzonder tijdrovend. Tevens zagen we dat de essentie van het kennisnemingsrecht daarmee wordt ondergraven. Wij stellen voor het kennisnemingsrecht uit het gegevensbeschermingsrecht voor CIE-en te schrappen.

Ter compensatie zou kunnen worden voorzien in een procedure voor de betrokkene waarbij hij kan verzoeken om de over hem geregistreerde gegevens te bezien op hun rechtmatigheid, zonder dat hij daarvan zelf kennis kan nemen. Van de bevindingen naar aanleiding van een dergelijk verzoek zou dan verslag aan de betrokkene dienen te worden gedaan. Daarbij kan worden voorzien in een rechtsgang tegen dat verslag. De afhandeling van een dergelijk rechtmatigheidsverzoek zal de CIE-en een stuk minder tijd kosten en er zal evenveel waarborgende werking vanuit kunnen gaan als van de manier waarop het huidige kennisnemingsrecht is ingericht.

In de afhandeling van een rechtmatigheidsverzoek kan vervolgens ook aansluiting worden gezocht bij de nationale instantie die tevens voor invulling zorgt van de normen uit de Wpolg. Er worden thans slechts enkele kennisnemingsverzoeken gedaan door betrokkenen. Door centralisatie van de dergelijke verzoeken ontstaat er een grotere eenheid in de afhandeling ervan en wordt tevens voorkomen dat een betrokkene bij meerdere verzoeken dit

bij afzonderlijke regio's dient te doen. Daarnaast zorgt het onderbrengen van een dergelijk verzoek bij een instantie die niet direct onderdeel van de CIE zelf is ervoor dat de onafhankelijkheid waarmee de rechtmatigheid van de gegevensverwerking zal worden beoordeeld gewaarborgd is. Vanzelfsprekend zal in zo'n geval wel zorg dienen te worden gedragen voor een mogelijkheid tot kennisname van de gegevens die over een betrokkene worden verwerkt door de CIE-en en dient die instantie daarover vertrouwelijkheid te betrachten. Tegen het besluit waarbij al dan niet inzage wordt verleend zal beroep bij de bestuursrechter open dienen te staan.

7.5.3 Versnippering

Aangaande controle en toezicht hebben we gezien dat door de wetgever te makkelijk een aantal mechanismen in de wet is opgenomen, zonder dat specifiek voor de CIE wordt bepaald of die in de praktijk ook het gewenste effect zullen hebben. Het is voor ons lastig te begrijpen dat voor toezicht er binnen de politie maar liefst zes personen en instantie nodig zijn; een privacyfunctionaris, het CBP, een onafhankelijke EDP-audit, een functionaris gegevensbescherming, een CIE-ovj en de strafrechter. Zeker nu capaciteitsgebrek bij de meerderheid van deze personen en instanties een knellend probleem blijkt te zijn waar de Wpolg geen oplossing voor biedt, is aanpassing van deze mechanismen aangewezen. Dat moet wat ons betreft gezocht worden in kwantitatieve versobering enerzijds en kwalitatieve investering anderzijds. Met andere woorden, minder mensen, maar wel mensen die meer tijd hebben voor de CIE-en specifiek.

We zien op dit punt eveneens mogelijkheden om aansluiting te zoeken bij een op te richten nationale instantie. Deze instantie zou, naast de reeds hiervoor genoemde invulling van vage normen en afhandeling van de rechtmatigheidsverzoeken, controle uit dienen te voeren op de gegevensverwerkingen door de CIE-en. Ook zal deze instantie 3 van de 6 controle- en toezichtmechanismen kunnen samenvoegen, zodat de maatregelen materieel gezien blijven bestaan en door één organisatie worden uitgevoerd. Vanwege het specifieke werkgebeid van de CIE en de thans goed werkende rol die de CIE-ovj daarbij vervult, zou in onze ogen alleen die functie, naast die van de strafrechter, nog een meerwaarde hebben naast de hiervoor genoemde op te richten instantie.

Door de adviserende en controlerende taak bij één instantie neer te leggen ontstaat er een kenniscentrum gegevensverwerking CIE. Door de combinatie van taken zal zij enerzijds voor de CIE een vraagbaak kunnen zijn op het gebied van het gegevensbeschermingsrecht en bijvoorbeeld kunnen voorzien in een deel van de opleiding. Anderzijds zal het kenniscentrum in staat zijn om door haar kennis van het veld en regelgeving effectiever dan nu het geval is invulling kunnen geven aan verschillende toezichthoudende taken op het gebied van gegevensbeschermingsrecht bij de CIE-en. Daarbij zal zij bijvoorbeeld ook de opgedragen audits kunnen uitvoeren bij de

verschillende CIE-en. Materieel gezien blijven de thans bestaande controle- en toezichtsmechanisme bestaan, maar uitgevoerd door één organisatie. Dat sluit ook aan bij de conclusie van de commissie Brauwer-Kort dat ‘robuust extern toezicht en handhaving’ gewenst is. Geen beoordeling van de papieren werkelijkheid, maar van de werkelijkheid die zich op de werkvloer voordoet.⁴⁴² Dat vraagt echter, zeker in het domein van de CIE, om diepgravende kennis van wet- en regelgeving de CIE-praktijk. Naar onze mening zou een dergelijke wijziging van het systeem van controle en toezicht bijdragen aan een effectievere waarborging van zowel de politietaak als de bescherming van de vrijheid van gegevens.

We zijn ons ervan bewust dat de oprichting van een dergelijke organisaties nogal wat (staats)rechtelijke implicaties heeft. We wijzen op de verhouding tussen deze organisatie en het CBP, maar ook op de verhouding tussen de op te richten instantie en de politie en justitie. De wijze waarop deze organisatie vorm dient te worden gegeven en waarop deze ingekleed dient te worden gaat het bestek van dit onderzoek echter te buiten en zal onderwerp van toekomstig onderzoek moeten zijn. Daarbij zal onder meer aan de orde dienen te komen of een dergelijke organisatie als (zelfstandig) onderdeel van het CBP kan functioneren of dat, zoals wij hier voorstellen, een zelfstandige nationale instantie de meest wenselijke vorm is.

7.6 AANBEVELINGEN

In deze sectie doen wij op basis van ons onderzoek en onze conclusies 6 concrete aanbevelingen aan de wetgever (subsectie 7.6.1), aan de politie en justitie (subsectie 7.6.2) en aan de toezichthouders (subsectie 7.6.3).

7.6.1 Aan de wetgever

Wij hebben betoogd dat bepaalde bevoegdheden zich in het gegevensbeschermingsrecht onder de huidige technologische ontwikkeling zich hebben ontwikkeld tot informationele opsporingsmethoden. We hebben eveneens betoogd dat die informationele opsporingsbevoegdheden vergezeld dienen te gaan van bijpassende strafvorderlijke waarborgen en dat dit thans nog niet het geval is. Hier ligt een taak voor de wetgever. Als eerste aanbeveling formuleren we dat hij de inzet van deze informationele opsporingsmethoden dient te regelen in het wetboek van strafvordering, zodat duidelijk is dat de inzet ervan niet zonder de daarbij behorende waarborgen mogelijk is.

Daarnaast hebben wij aangegeven dat voor de Wpolg het keurslijf van de privacy te klemmend is. Het beschermingsobject lijkt zich mogelijk zelfs te ontwikkelen richting een zelfstandig grondrecht, dat wij hebben geduid

442 Brouwer-Korf e.a., 2009, sectie 3.7.

als het recht op vrijheid van gegevens. Als tweede aanbeveling formuleren we dat de wetgever initiator van een discussie is op beleidsmatig, politiek en wetenschappelijk gebied naar de vraag of, en zo ja hoe, de grondwet op dit punt dient te worden aangepast. Op die manier kan de Wpolg, maar ook de Wbp in het juiste grondwettelijke perspectief worden geplaatst, hetgeen de discussie over de wijze van toepassing ten goede zal komen.

Ten slotte hebben we gezien dat de fundamentele knelpunten die zich onder de Wpolr voordeden zich onder de Wpolg nog steeds zullen laten gevoelen. We hebben daarbij aangetoond dat de wetgeving in de oplossing hiervan een grotendeels faciliterende functie heeft. Wetgeving op het gebied van gegevensbescherming dient naar onze overtuiging ruimte te laten voor interpretatie. Daarbij dient wetgeving een systeem te bevatten dat zorg draagt voor een invulling van die normen die aansluiten bij de stand van de techniek en wensen uit de praktijk. Daarnaast hebben we gezien dat het huidige door de wetgever gekozen systeem van kennisneming, advisering, en controle en toezicht te wensen overlaat. In de discussiesectie hebben we reeds een aanzet gegeven over de richting waarin het gegevensbeschermingsrecht zich op dit punt zou moeten ontwikkelen. Voordat dit zich kan vertalen dient daar eerst onderzoek naar te worden verricht.

Als derde aanbeveling formuleren we dat de wetgever door aanpassing van de Wpolg zorg draagt voor een systeem dat op een dynamische wijze invulling kan geven aan de wettelijke normen, zodat de gegevensverwerking effectiever kan plaatsvinden dan thans onder de Wpolg het geval zal zijn.

7.6.2 Aan politie en justitie

Een van de drie fundamentele problemen die bij de uitvoering van het gegevensbeschermingsrecht naar voren is gekomen, is de daarvoor beschikbare capaciteit bij onder meer de politie. We hebben reeds in de discussiesectie aangegeven op welke wijze naar onze mening de wetgeving aan dit knelpunt tegemoet dient te komen. Er ligt hier echter ook een taak voor politie en justitie zelf. Capaciteit is een kwestie van prioriteit. Uitvoering van de Wpolg kost de politie wellicht meer capaciteit dan zij zou willen, maar zij dient niet uit het oog te verliezen dat het haar wettelijke en ook morele plicht is om haar taak in overeenstemming met wet- en regelgeving uit te voeren. Het politie-apparaat kan alleen op een integere manier functioneren door zichzelf ook aan de regels en normen te houden die ook voor anderen gelden. Het argument dat er geen capaciteit is eigenlijk geen argument zijn om niet aan de verplichtingen te voldoen. Iets anders is dat die keuze in bepaalde gevallen voor ons wel begrijpelijk is.

Onze vierde aanbeveling is in de richting van politie en justitie en luidt dat zij meer moeten doen dan nu om inzichtelijk te maken hoeveel tijd zij kwijt zijn aan het voldoen aan de regels en normen uit de Wpolg.

Daarnaast wordt dit soort wetgeving door de politie te veel als lastig en opgelegd ervaren. Het dient beschouwd te worden als beroepseer om poli-

tiegegevens op een zorgvuldige manier te verwerken. Daar kunnen zij zelf aan bijdragen door voorstellen te doen waarop een gelijk niveau van zorgvuldigheid wordt bereikt, maar door de inzet van minder capaciteit. Wij wijzen hier nogmaals op het door ons in de discussie voorgestelde kenniscentrum gegevensverwerking CIE, dat naar ons idee daarbij een belangrijke rol kan vervullen. Een eerste aanzet hiertoe, en dat is onze vijfde aanbeveling, kan door de politie gegeven worden doordat het onder de huidige Wpolg mogelijk zou moeten zijn om met alle CIE-en gezamenlijk een functionaris gegevensbescherming te benoemen die binnen aan hem opgedragen taken controle uitvoert op de gegevensverwerkingen door de CIE.

7.6.3 Aan de toezichthouders

De toezichthouders zijn slechts over de band van de in de Wpolg opgenomen controle- en toezichtmechanismen onderwerp van onderzoek geweest. Daarin is evenwel naar voren gekomen dat de versnippering van de controle en het toezicht in dat kader het belangrijkste knelpunt is. Om die reden hebben we de wetgever aanbevolen het systeem van de Wpolg op dat punt te herzien. De toezichthouders hebben in het debat dat daaraan vooraf dient te gaan hun eigen rol. Als zesde aanbeveling roepen we hen op om hun verantwoordelijkheid in dit debat te nemen en vanuit hun eigen positie aan te geven wat de sterke kanten zijn van hun controlerende en toezichthoudende taak, en tevens wat daarvan de minder sterke kanten zijn. Alleen op die manier zal de wetgever in staat zijn om de Wpolg zo aan te passen dat het gegevensbeschermingsrecht effectiever vorm zal worden gegeven dan thans het geval is.

7.7 SLOTBESCHOUWING

Dit proefschrift vormt de neerslag van het onderzoek naar de waarborgende werking van het gegevensbeschermingsrecht binnen het domein van de CIE-en. We hebben gezien dat de Wpolg slechts op een aantal punten tegemoet is gekomen aan de knelpunten die onder de Wpolr waren geconstateerd. We hebben echter ook moeten constateren dat de meer fundamentele knelpunten door de Wpolg niet zijn opgelost en in sommige gevallen zelfs sterker naar voren zijn gekomen.

We hebben daarbij aangegeven in welke richtingen het gegevensbeschermingsrecht zich naar ons idee dient te ontwikkelen om wel aan deze fundamentele knelpunten tegemoet te komen. Deze aanzet zal echter eerst moeten leiden tot een discussie over hoe in het domein van de politie de verwerking van politiegegevens zo kan worden gewaarborgd dat daarbij recht wordt gedaan aan de goede uitvoering van de politietaak enerzijds en de bescherming van de vrijheid van gegevens anderzijds. Pas nadien is wijziging van wetgeving, zodat een effectiever systeem van waarborging ontstaat, mogelijk.

Referenties

Aldewereld, 2007

H.M. Aldewereld, *Autonomy vs. Conformity, An institutional perspective on Norms and Protocols*, (diss. Utrecht), Enschede: Gildeprint drukkerijen, 2007.

Bacon, 1645

F. Bacon, *Novum Organum Scientiarum*, Lugduni Batavorum: Adrianum Wijngaerde et Franciscum Moiardum 1645, IV.

Beijer e.a., 2004

A. Beijer, R.J. Bokhorst, M. Boone, C.H. Brants en J.M.W. Lindeman, *De Wet bijzondere opsporingsbevoegdheden, Eindevaluatie*, WODC, 2004.

Van der Bel 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 informatieverwerking, -verwerking en -verstrekking ten behoeve van de opsporingspraktijk*, Zutphen: Studiecentrum Rechtspleging, 2007.

Berkvens, 2004

J.M.A. Berkvens, *Ontvreemde privacy*, *Rechtsgeleerd Magazijn Themis*, 2004, nr. 5.

De Brauw, 1965

P.J.W. de Brauw, 'Behoort de wetgever regelen te treffen ter bescherming van de individu tegen het doen, het gebruiken en het openbaarmaken van waarnemingen, diens persoonlijke levenssfeer betreffende', in: *Handelingen 1965 der Nederlandse Juristen-Vereniging deel 2*, Zwolle: W.E.J. Tjeenk Willink 1965.

Blok, 2001

P.H. Blok, 'De splitsing van privacy. Advies over het grondrecht op privacy in het digitale tijdperk', *Ars Aequi* 50 (2001) nr. 6, p. 435-439.

Blok, 2002

P.H. Blok, *Het recht op privacy: een onderzoek naar de betekenis van het begrip 'privacy' in het Nederlandse en Amerikaanse recht* (diss. UvT), Den Haag: Boom Juridische Uitgevers, 2002.

Blok, 2005

P.H. Blok, *De waarde van de omnibuswet, P&I*, 2005(6).

Blok en Vedder, 2002

P. Blok en A. Vedder, 'Privacy in ontwikkeling', in: J.E.J. Prins en J.M.A. Bervens (red.), *Privacy-regulering in theorie en praktijk*, Kluwer, Deventer: 2002, p. 5-31.

Brouwer-Korf e.a., 2009

A.H. Brouwer-Korf, C.P.M. Cleiren, L.K. Geluk, S. Harchaoui, E.P. De Jong, A.J.A.M. Nieuwenhuizen, J.E.J. Prins, J.G. Stam en E.H. Swaab, *GEWOON DOEN, beschermen van veiligheid en persoonlijke levenssfeer*.

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, 1997

Y. Buruma, 'Schade en schuld bij het verstrekken van politieke informatie', in: Ad van Ruth en Lodewijk Gunther Moor, *Lekken of verstrekken? De informele informatie-uitwisseling tussen opsporingsinstanties en derden*, Ubbergen: Tandem Felix 1997.

Buruma, 2002

Y. Buruma, Inleiding als dagvoorzitter bij de CIE-themadag, 1 februari 2001. Privacyregelgeving in relatie tot informatiehuishouding CIE, in: *Recherchereeks* 11, p. 91.

Buruma, 2008

Y. Buruma, *Privacy en veiligheid: de passie voor de werkelijkheid*, Den Haag: College bescherming persoonsgegevens, 2008.

Corstens, 2008

G.J.M. Corstens, *Het Nederlandse strafprocesrecht*, (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.

Cuijpers, 2004

C. Cuijpers, Privacyrecht of privaatrecht? Een privaatrechtelijk alternatief voor de implementatie van de Europese privacyrichtlijn, Sdu uitgevers Den Haag, 2004.

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 e.a., 2000

H. Franken, J. Arnbak, M.A.P. Bovens, J.P.H. Donner, A.M. Gerritsma, H.R.B.M. Kummeling, J.E.J. Prins, H.J. de Ru, I.Th.M. Snellen, P. Vogelzang, *Rapport van de commissie Grondrechten in het Digitale Tijdperk*, Rotterdam: Phoenix & Den Oudsten, 2000.

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.

Foqué en 't Hart, 1990a

R. Foqué en A.C. 't Hart, strafrecht en beleid, instrumentaliteit van rechtsbescherming, in: C. Fijnaut en P. Spierenburg (red.), *Scherp toezicht. Van "Boeventucht" tot "Samenleving en Criminaliteit"*, Arnhem: Gouda Quint 1990, p. 193-209.

Foqué en 't Hart, 1990

R. Foqué, A.C. 't Hart, Instrumentaliteit en rechtsbescherming: Grondslagen van een strafrechtelijke waardendiscussie, Arnhem/Antwerpen 1990.

De Graaf, 1977

F. de Graaf, Rechtsbescherming van persoonlijkheid, privéleven, persoonsgegevens, H.D. Tjeenk Willink, Alphen aan den Rijn: 1977.

Goos, 1995

M. Goos, Schending Wet politieregisters geen gevolgen in strafzaak, *Computerrecht* 1995/3.

Groenhuijsen, 2008

M.S. Groenhuijsen, Strafrechtelijk stromenland in 2008, *Delikt en delinkwent*, 28(10), 1093-1112.

Van den Herik, 1991

H.J. van den Herik, *Kunnen computers Rechtspreken*, (oratie, Leiden), Arnhem: Gouda Quint, 1991

Van den Herik en Postma, 2009

H.J. van den Herik en E.O. Postma, *Geloof in Computers* (2009).

De Hert, 2003

P. De Hert, 'Strafrecht en Privacy. Op zoek naar een tweede adem', *Rechtshulp* 2003, nr. 10, p. 41-54.

De Hert en Gutwirth, 2003

P. de Hert en S. Gutwirth, 'Making sense of privacy and dat protection. A prospective overview in the light of the future of identity, location bases services and the virtual residence', in: IPTS-JRC-EC, *Security and Privacy for the Citizen in the Post-September 11 Digital Age. A prospective overview*, Technical Report Series, EUR 20823 EN, 2003, p. 111-162.

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, *Veiligheid. Studies over inhoud, organisatie en maatregelen*, Deventer: Kluwer, 2005.

De Hert, Huisman en Vis, 2005

P.J.A. De Hert, W. Huisman & T. Vis, 'Intelligence led policing ontleed', *Tijdschrift voor Criminologie* (47), 2005-4, p. 365-375.

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. *Artificial Intelligence and Law*, 2006, nr. 13, p. 133-151.

Holvast, 1996

J. Holvast, *Persoonsgegevens of niet: dat is de vraag*, Alphen aan den Rijn/Diegem 1996.

Hoogendoorn, 2008

R. Hoogendoorn, Meer rook zonder vuur. Nieuwe wetgeving voor opslag politiegegevens, *Advocatenblad*, nr. 8, 2008, p. 208-212.

Hustinx, 2004

P.J. Hustinx, bescherming van persoonsgegevens op Koers, *Rechtsgeleerd magazijn THEMIS*, 2004, nr. 5.

Kielman en Koelewijn, 2006

Kielman & Koelewijn, 'Privacy als tunnelvisie', *Privacy & Informatie* 2006.

Kielman en Koelewijn, 2005

H.H. Kielman en W.I. Koelewijn, 'Minder registers, meer gegevens. Over gegevensverwerking betreffende zware criminaliteit', *Ars Aequi* 2005(6), p. 451-457.

Van der Klaauw-Koops en Prins, 2002

F.A.M. van der Klaauw-Koops en J.E.J. Prins, Internationale privacyregulering: belangen, problemen en mogelijkheden in: J.E.J. Prins (ed.), *Privacyregulering in theorie en praktijk* (Recht en Praktijk), Deventer: Kluwer, 2002, p. 485-510.

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.

Koelewijn, 2009

W.I. Koelewijn, Privacy en politiegegevens. Over 'geautomatiseerde normatieve informatie-uitwisseling', (diss. Leiden), Amsterdam, Leiden University Press 2009.

Van Kralingen en Prins, 1996

R.W. van Kralingen en J.E.J. Prins, Waar een wil is, is een weg? Een onderzoek naar de behoefte en de verstrekking van politieke en justitiële informatie voor buiten de strafrechtspleging gelegen doelen, SDU Uitgevers, Den Haag: 1996.

Kranenborg, 2007

H.R. Kranenborg, Toegang tot documenten en bescherming van persoonsgegevens in de Europese Unie: over de openbaarheid van persoonsgegevens, Kluwer, Den Haag: 2007.

Kuitenbrouwer, 1991

F. Kuitenbrouwer, *Het recht om met rust gelaten te worden. Over privacy*, Amsterdam: Uitgeverij Balans 1991, p. 65-79.

Leenes en Prins, 2006

R. Leenes en C. Prins, Techniek als alternatief reguleringsinstrument, Implicaties voor privaatrechtelijke verhoudingen, in: B. Dorbeck-Jung en M. Oude Vrielink-van Heffen, *Op weg naar bruikbare regulering? 's-Gravenhage*: Reed Business Information, 2006, pp.117-134.

Middelburg en Vugts, 2006

B. Middelburg en P. Vugts, De Endstra-tapes. De integrale geprekken van Willem Endstra met de recherche, Nieuw Amsterdam: Amsterdam, 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.

Moerings, 2006

L.M. Moerings, 'Risicojustitie als inzet voor een veiliger samenleving. Zeden- en antiterrorismedwetgeving als illustratie', in: W. Huisman, L.M. Moerings & G. Suurmond (red.), *Veiligheid en recht. Nieuwe doelwitten en strategieën*, Boom Juridische Uitgevers: Den Haag, 2006, p. 161 – 174.

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.

Muijen, 2004

P.J.D.J. Muijen, *Handleiding politie en privacy*, Den Haag: Elsevier Overheid, 2004.

Muller, Kummeling 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.

Nabben en Van de Luytgaarden, 1996

P.H.P. Nabben en H.J.L.M. van de Luytgaarden, *De ultieme vrijheid. Een rechtstheoretische analyse van het recht op privacy*, Kluwer: Deventer, 1996.

Overkleef-Verburg, 1995

G. Overkleef-Verburg, *Wet Persoonsregistraties. Norm, toepassing en evaluatie*, (diss. KUB), Zwolle: W.E.J. Tjeenk Willink 1995.

Peters, 1972

A.A.G. Peters, *Het rechtskarakter van het strafrecht*, oratie Utrecht, Deventer 1972.

Peters, 1993

A.A.G. Peters, *Individuele vrijheid en de positie van verdachten in het strafproces*, in: *Recht als kritische discussie*, Gouda Quint, Arnhem, 1993.

Rietveld, Slump en Beerepoot, 2004

M. Rietveld, G.J. Slump en A. Beerepoot, *Toets uitvoerbaarheid Wet politiegegevens*, verslag van bevindingen, DSP-groep, 2004.

Van de Pol, 2002

U. van de Pol, 'Toezicht en kwaliteit nog beneden de maat: terugblik op een jaar bijzondere politieregisters', in: *Criminele informatie; afscherming of openheid* (Studiereeks recherche deel 11), 's-Gravenhage: Elsevier 2002.

Rozenbeek, 2003

M. Rozenbeek, 'Kan niet bestaat vaak niet. De (on)mogelijkheden van de bijzondere politieregisters', in: *Recherche Magazine*, nr. 8, oktober 2003.

Van Ruth en Gunther Moor, 1997

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 Politieregisters*, Registratiekamer, mei 2000.

Schermer, 2007

B.W. Schermer, *Software agents, and the right to privacy: a legislative framework for agent-enabled surveillance*, (diss. UL), Leiden: Leiden University Press, 2007.

Schreuders, 2001

E. Schreuders, *Data mining, de toetsing van beslisregels en privacy. Een juridische Odyssee naar een procedure om het toepassen van beslisregels te kunnen toetsen*, (diss. UL), Den Haag, Sdu Uitgevers, 2001.

Schreuders e.a., 2005

E. Schreuders e.a., *Evaluatie wet bijzondere politieregisters*, WODC 2005.

Sietsma, 2006

R. Sietsma, *Gegevensverwerking in het kader van de opsporing, toepassing van datamining ten behoeve van de opsporingstaak: afweging tussen het opsporingsbelang en het recht op privacy*, (diss. UL), Den Haag, SDU Uitgevers, 2006.

Sietsma, Verbeek en Van den Herik, 2002

Ruben Sietsma, Joop Verbeek en Jaap van den Herik, *Datamining en opsporing. Toepassing van datamining ten behoeve van de opsporingstaak: strafprocesrecht versus recht op privacy*,

Den Haag: Sdu Uitgevers, 2002.

Schmidt en Zwenne, 2005

Aernout Schmidt en Gerrit-Jan Zwenne, Recht en risico: kanttekeningen bij het voorstel voor een richtlijn over de bewaring van telecommunicatieverkeersgegevens, *Mediaforum* 2005, p. 292-302.

Steenhuis, 1984

D.W. Steenhuis, Strafrechtelijk optreden: stapje terug en een stapje voorwaarts, *Delict en Delinkwent* nr. 5, mei 1984, blz. 395-414; nr. 6, juni 1984, blz. 497-512.

Steenhuis, 1988

D.W. Steenhuis, *Doelmatigheid van rechtsvervolgning*, Wetenschappelijk Raad voor Regeringsbeleid, 's-Gravenhage, juli 1988.

Stol, 2004

W.Ph. Stol, 'Biedt de politiepraktijk ruimte voor prestatiecontracten?', in: *Tijdschrift voor de politie*, nr. 9, 2004.

Van Stratum, 2001

M. van Stratum, Van afscherming van geheime informantgegevens naar transparantie en openheid van gelopen CID-trajecten?, *Delict en Delinkwent* 31 (2001), afl. 2, p. 174-192.

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 bedrijfsinformatie 2002, p. 29-38.

Van Stratum, 1999

M. van Stratum, 'Inzage in bestanden van politie en justitie. Vergeten mogelijkheden voor advocaten', *Advocatenblad* 17, 17 september 1999, p. 900-903.

Tak, 2002

J.P. Tak, 'De afscherming van informanten; een knelpunt', in: *Recherchereeks* deel 11, CIE Themadagen, 2001.

Teepe, 2006

W.G. Teepe, *Reconciling Information Exchange and Confidentiality. A Formal Approach*, (diss. Groningen), Groningen, 2006.

Terstegge, 2005

Jeroen Terstegge, 'Toepassingen en toekomst van RFID', in: G.J. Zwenne & B. Schermer, *Privacy en andere juridische aspecten van RFID: unieke identificatie op afstand van producten en personen*, NVvIR, 2005.

Vanderlooy, 2009

S. Vanderlooy, *Ranking and Reliable Classification*, (diss: Tilburg), Tilburg 2009.

Vedder, 1996,

A.H. Vedder, 'Privacy en woorden die tekort schieten', in: *Privacy in het informatietijdperk*, SDU Uitgevers, Den Haag: 1996, p. 17-30.

Verbeek, 2004

J.P.G.M. Verbeek, *Politie en de nieuwe internationale informatiemarkt, Grensregionale politieke gegevensuitwisseling en digitale expertise*, (diss. Maastricht), Den Haag: SDU uitgevers, 2004.

De Vlieger en Verstuyft, 2007

L. De Vlieger en N. Verstuyft, Politierregisters en Privacy, in: G. Vermeulen (red.), *Privacy en Strafrecht. Nieuwe en grensoverschrijdende verkenningen*, Antwerpen/Apeldoorn, Maklu, 2007.

Warren en Brandeis, 1890

S.D. Warren en L.D. Brandeis, *The Right to Privacy*, 4. Harvard Law Review 1890, 193-220.

Westin, 1967

A. Westin, *Privacy and Freedom*, New York: Atheneum Press 1967.

Winter e.a., 2008

Winter, H.B., Jong, P.O. de, Sibma, A., Visser, F.W., Herweijer, M., Klingenberg, A.M., Prakken, H. Wat niet weet, wat niet deert. Een evaluatieonderzoek naar de werking van de Wet bescherming persoonsgegevens in de praktijk, WODC 2008.

Zwenne e.a. 2007,

G.J. Zwenne, A.W. Duthler, M.M. Groothuis, H.H. Kielman, W.I. Koelewijn, L. Mommers, *Eerste fase evaluatie Wet bescherming persoonsgegevens. Literatuuronderzoek en knelpuntenanalyse*, WODC 2007.

Opportuun, 2002

Onzichtbare werelden in het Openbaar Ministerie. Theo de Jong: 'We zoeken wel de grenzen op', Opportuun, 2002.

Samenvatting

In dit proefschrift stellen we vast in hoeverre met de wijziging van het wettelijke regime rond de verwerking van persoonsgegevens door de politie tegemoet is gekomen aan de knelpunten die onder het regime van de Wet politieregisters zijn geconstateerd. Sinds 1990 zijn er regels en normen voor het gebruik van politieke gegevensverzamelingen. Aanvankelijk waren ze opgenomen in de Wpolr; vanaf 1 januari 2008 is de Wpolg van kracht. Met de invoering van de Wet politiegegevens heeft de wetgever tegemoet willen komen aan de knelpunten die bij de uitvoering van de Wet politieregisters en de Wet bijzondere politieregisters naar voren zijn gekomen. De volgende probleemstelling (PS) is als leidraad van het onderzoek genomen.

PS: In hoeverre waarborgt de Wet politiegegevens de goede uitvoering van de politietask en de grondrechten van de burger effectiever dan de Wet politieregisters?

Om deze probleemstelling te beantwoorden onderzoeken we de volgende drie onderzoeksvragen.

OV1: Op welke wijze zijn de politietask en de grondrechten van de burger betrokken bij het verwerken van politiegegevens?

OV2: Welke knelpunten zijn er in de literatuur en de praktijk geconstateerd ten aanzien van de waarborgende werking van de Wet politieregisters?

OV3: In hoeverre komt de Wet politiegegevens, mede in het licht van de ervaringen met de Wet bescherming persoonsgegevens, tegemoet aan de geconstateerde knelpunten?

Bij de regulering van de verwerking van politiegegevens heeft de wetgever drie waarborgen geïntroduceerd die ervoor moeten zorgen dat het gebruik van persoonsgegevens plaatsvindt in overeenstemming met de regels en normen uit het wettelijke regime. Zowel onder het huidige wettelijke regime (Wpolg) als onder het oude regime van de Wet politieregisters (Wpolr) zijn dit er drie, te weten:

- (1) **Wet:** de wettelijke beperkingen in het gebruik van persoonsgegevens zelf.
- (2) **Kennisnemingsrecht:** het recht van iedere individuele burger om in beginsel kennis te nemen van de gegevens die over hem zijn opgenomen in een politieregister.
- (3) **Controle en toezicht:** de controle en het toezicht op het gebruik van persoonsgegevens.

Aan de hand van deze drie waarborgen is in dit proefschrift het oude wettelijke regime vergeleken met het nieuwe wettelijke regime (hoofdstukken 4, 5 en 6). Binnen dit onderzoek is ervoor gekozen, mede als gevolg van een soortgelijke keuze binnen het ANITA-project (Administrative Normative Information Transaction Agents), om het onderzoek te beperken tot gegevensverwerking door Criminele inlichtingen eenheden (CIE) op nationaal niveau. Om het onderzoek in het juiste kader te plaatsen is in hoofdstuk 2 eerst een beschrijving gegeven van de CIE. In hoofdstuk 3 zijn de bij gegevensverwerking betrokken belangen besproken.

In hoofdstuk 2 is allereerst is de ontwikkeling van de CID naar de CIE beschreven. Daarbij is aandacht besteed aan de wijzigingen in de taken en bevoegdheden van de CID. De informatievoorziening van de recherchefunctie kwam centraal te staan bij de opsporing en bij het voorkomen van zware criminaliteit. Deze ontwikkeling heeft geleid tot een flinke hoeveelheid regelgeving die ziet op (1) de verwerking van politiegegevens door de CIE en (2) de wijze waarop de CIE haar informatie verkrijgt. Vervolgens is uitgebreid stilgestaan bij de informatie-inwinning en -veredeling door de CIE. Het inwinnen van informanteninformatie kan ten slotte worden teruggevoerd op twee verschillende bevoegdheden: (1) de algemene politietaakbepaling uit art. 2 Pw1993 en (2) de bijzondere opsporingsbevoegdheid voor het stelselmatig inwinnen van informatie bij informanten, neergelegd in art. 126v Sv.

In hoofdstuk 3 wordt OV1 beantwoord. De twee belangen, die bij de politieke gegevensverwerking zijn betrokken, komen uitvoerig aan de orde: (A) de goede uitvoering van de politietaak en (B) het beschermingsbelang. Zowel voor belang A als voor belang B is het onderkennen van de technologiegestuurde ontwikkeling noodzakelijk. Technologische ontwikkelingen geven meer instrumentele mogelijkheden voor belang A en stellen om die reden tegelijkertijd hogere eisen aan belang B. Hoewel technologie niet als een zelfstandig belang kan worden aangemerkt bij de opstelling van regelingen van het gegevensbeschermingsrecht, blijkt zij dus wel een belangrijke sturende factor te zijn in het denken over de betrokken belangen bij de inzet van gegevensverwerkingen. Vanuit deze achtergrond worden in de hoofdstukken 4, 5, en 6 de drie voornoemde waarborgen behandeld.

In hoofdstuk 4 is het proces van informatieverwerking door de CIE-en besproken. Daarbij is antwoord gegeven op OV2 en OV3 voor zover het *de wet als waarborg* betreft. We hebben beschreven op welke wijze de Wpolg tegemoet komt aan de onder de Wpolr geconstateerde knelpunten als het gaat om (1) het opslaan, (2) het bewaren, (3) het verstrekken, (4) het koppelen en (5) het analyseren van politiegegevens door de CIE. Bij de beschrijving van de knelpunten onder de Wpolr en de daarvoor door de Wpolg geboden oplossingen, is gebleken dat deze zich op drie gebieden laten voelen, namelijk (1) de vaagheid in toepassingsvoorwaarden, (2) de oplossingen die voor-

al instrumenteel van karakter zijn en (3) de noodzaak van sterkere overige waarborgen.

Ad(1) Vaagheid in toepassingsvoorwaarden

Als veruit het belangrijkste knelpunt onder de Wpolr is de vaagheid in de regeling naar voren gekomen. Dit werd vooral veroorzaakt door het gebruik van het begrip 'noodzakelijkheid' als toepassingsvoorwaarde voor de activiteiten bewaren, de weigeringsgrond voor het verstrekken van informatie, het koppelen en het analyseren. Ondanks de in de praktijk bestaande problemen is deze voorwaarde onder de Wpolg onverkort gehandhaafd. Sterker nog, zoals gezien is bij de activiteit 'bewaren' de noodzakelijkheid als voorwaarde een prominentere rol gaan spelen en introduceert de Wpolg met de themaverwerking een nieuwe vaagheid in toepassingsvoorwaarden. Ook bij de geconstateerde classificatieknelpunten blijven de toepassingsvoorwaarden onverkort gehandhaafd.

Ad(2) Oplossingen vooral instrumenteel

We hebben gezien dat de Wpolg ook een aantal prangende knelpunten heeft opgelost. Dit betrof echter vooral knelpunten vanuit een instrumenteel belang. We noemen het afbakeningsprobleem tussen het voorlopig register en het register zware criminaliteit. Daarnaast zijn met de Wpolg oplossingen gekomen voor de te knellende bewaartermijn van 5 jaar, de toegangsproblemen tot het informantenregister, en de te beperkte verstrekkingsmogelijkheden naar derden buiten de politieorganisatie. Voorts worden met de introductie van themaverwerkingen meer mogelijkheden geboden tot gegevensverwerking. De mogelijkheden in het verwerken van politiegegevens zijn onder de Wpolg dan ook ontegenzeggelijk ruimer dan onder de Wpolr. Dit gaat echter ten koste van de grondrechten van de burger.

Ad(3) Meer mogelijkheden, sterkere waarborgen?

Tegenover deze ruimere instrumentele mogelijkheden staat volgens de wetgever ook een strenger systeem van waarborgen. Maar die extra bescherming kan echter niet van de eerste waarborg worden verwacht. Die eerste waarborg is het verwerkingsregime voor politiegegevens zelf. Daarin zit wat de bevoegdheden betreft nu juist een aanzienlijke verruiming van de mogelijkheden. In de toepassingsvoorwaarden blijft de vaagheid bovendien een grote factor van betekenis. Op grond van het nieuwe verwerkingsregime concluderen wij dat het regime van de Wpolg aan waarborgende werking ten aanzien van de grondrechten van de burger inboet. Dat vraagt dus, bij wijze van compensatie, meer van de overige twee waarborgen, die in de hoofdstukken 5 en 6 aan bod zijn gekomen.

In hoofdstuk 5 wordt het *kennisnemingsrecht als waarborg* behandeld. De daarbij geconstateerde knelpunten zijn vooral praktische problemen bij de uitvoering van het kennisnemingsrecht die voortkomen uit de volgende twee belangen: (1) de CIE probeert heimelijk informatie over personen en groepen

te verzamelen en (2) de crimineel wil graag weten wat de politie over hem weet. Deze twee belangen die lijnrecht tegenover elkaar staan, maken dat niet zonder meer alle bij de CIE aanwezige informatie kan worden verstrekt aan de persoon die om inzage verzoekt. Daar moet, in verband met de goede uitvoering van de politietaak, eerst een selectie in gemaakt worden. Dit zorgt ervoor dat het recht op kennisneming van informatie uit de CIE-databanken een vrijwel onmogelijke taak is.

Doordat in het geval van kennisneming bij de CIE een groot deel van de informatie geheim blijft, is het voeren van een discussie over het al dan niet terecht geregistreerd hebben van een deel van die informatie niet goed mogelijk. We hebben daar in hoofdstuk 5 de conclusie aan verbonden dat de waarborgende werking van het kennisnemingsrecht te wensen overlaat. Het geringe aantal verzoeken en de wijze waarop die afgedaan worden dragen naar ons idee slechts marginaal bij aan de waarborgende werking. Net als bij de eerste waarborg, het wettelijk systeem zoals dat in hoofdstuk 4 is behandeld, leidt het gebrek aan waarborgende werking van het kennisnemingsrecht tot de conclusie dat daardoor meer moet worden verwacht van de derde en laatste waarborg, controle en toezicht.

In hoofdstuk 6 worden *controle en toezicht op de informatieverwerking als waarborg* behandeld. Daarbij is een antwoord gegeven op OV2 en OV3 voor zover het controle en toezicht als waarborg betreft. In het hoofdstuk hebben we beschreven op welke wijze de Wpolg tegemoet komt aan de onder de Wpolr geconstateerde knelpunten als het gaat om controle en toezicht door (1) de verantwoordelijke, (2) de privacyfunctionaris, (3) het CBP, (4) protocollering en auditing, (5) de CIE-ovj, en (6) de strafrechter.

Deze personen en instanties vormen in potentie zeer sterke controle- en toezichtmechanismen. Het succes daarvan lijkt in elk van de gevallen echter in te moeten boeten door een gebrek aan capaciteit. De manier waarop de controle en het toezicht op de verwerking van politiegegevens bij de CIE thans is vormgegeven, is naar onze mening te versnipperd. De Wpolg lost voor de individuele controle- en toezichtmechanismen weliswaar een aantal praktische knelpunten op, maar niet op de punten van capaciteit en versnippering. Integendeel, het systeem onder de Wpolg raakt door de invoering van de functionaris gegevensbescherming en de verplichte auditing meer versnipperd dan onder de Wpolr.

Geen van de genoemde personen en instanties is in staat om inhoudelijk, bij iedere regio en op regelmatige basis, toezicht te houden. Er is te gemakkelijk een aantal mechanismen in de wet opgenomen, zonder dat specifiek voor de CIE wordt bepaald of die in de praktijk ook effect zullen hebben. Zeker nu capaciteitsgebrek bij de meerderheid van voornoemde personen en instanties een knellend probleem blijkt te zijn waar de Wpolg geen oplossing voor biedt, is aanpassing van deze mechanismen aangewezen. Dat moet wat ons betreft, anders dan onder de Wpolg, gezocht worden in kwantitatieve versobering enerzijds en kwalitatieve investering anderzijds.

Met het voorgaande zijn de drie waarborgen (de wet, het kennisnemingsrecht, en controle en toezicht) besproken.

In hoofdstuk 7 wordt een antwoord gegeven op de probleemstelling. Bij de beantwoording van de probleemstelling is het de vraag of met de doorgevoerde wijzigingen de politietaak (belang A), alsmede de bescherming van de grondrechten van de burger (belang B) effectiever gewaarborgd worden dan onder de Wpolr.

De politietaak

De Wpolg lost voor de politiepraktijk een aantal prangende knelpunten op door het verwerkingsregime op een aantal punten te wijzigen. De wijzigingen zijn echter vooral wijzigingen op detailniveau en bevatten geen fundamentele wijzigingen in de wijze waarop politiegegevens dienen te worden verwerkt. Alleen voor deze knelpunten was naar onze overtuiging geen nieuwe wet nodig geweest.

De zingeving van nieuwe wetgeving is erin gelegen dat juist de meer fundamentele knelpunten worden aangepakt. We bedoelen met fundamentele knelpunten de knelpunten die voortkomen uit de wijze van regulering of de opzet van de regulering. We hebben aangetoond dat aangaande de verwerking van politiegegevens er zich drie van deze fundamentele knelpunten voordoen, te weten (1) de vaagheid in toepassingsvoorwaarden, (2) het capaciteitsgebrek, en (3) de geconstateerde versnippering. We zien dat de Wpolg deze drie punten ongemoeid laat. We zagen zelfs dat op sommige punten te verwachten is dat de geconstateerde knelpunten zich in verhevigde vorm zullen voordoen. Dit betekent dat de CIE zich in de praktijk geconfronteerd zal blijven zien met dezelfde of soortgelijke knelpunten bij de verwerking van politiegegevens.

De grondrechten van de burger

Tegenover de ruimere instrumentele mogelijkheden staat volgens de wetgever ook een strenger systeem van waarborgen. Echter, op grond van het nieuwe verwerkingsregime moet worden geconstateerd dat het verwerkingsregime van de Wpolg aan waarborgende werking afneemt als het gaat om de bescherming van de grondrechten van de burger. Van de waarborgende werking die van het kennisnemingsrecht uit zou moeten gaan, moet ook onder de Wpolg niet veel worden verwacht. Het recht werd onder de Wpolr immers weinig gebruikt en de invulling van die verzoeken die werden gedaan was dusdanig dat daarvan vrijwel geen waarborgende werking uitging.

Dit maakt dat de noodzakelijke extra waarborgende werking door de controle- en toezichtmechanismen geboden moet worden. We hebben op dit punt echter gezien dat de knelpunten op het gebied van controle en toezicht – capaciteit en versnippering – onder de Wpolg worden versterkt in plaats van afgezwakt. Met de invoering van extra controle- en toezichtmechanis-

men is het dus sterk de vraag of de effectiviteit van die controle en dat toezicht groter wordt dan onder de Wpolr. Zonder extra maatregelen, waarvan tot nu toe niet is gebleken, moet worden geconcludeerd dat dit niet het geval is.

In conclusie kunnen we stellen dat de Wpolg weliswaar meer mogelijkheden biedt voor de verwerking van politiegegevens, maar dat deze ruimere mogelijkheden vooral gepaard gaan met het oplossen van praktische knelpunten. Daarmee is de politietaak gediend. Die ruimere instrumentele mogelijkheden maken echter niet dat de politietaak effectiever gewaarborgd wordt, aangezien de meer fundamentele knelpunten niet worden aangepakt.

Als het gaat om de waarborging van de grondrechten van de burger hebben we laten zien dat zich daar soortgelijke problemen voordoen. In plaats van de fundamentele knelpunten (het bestaansrecht van het kennisnemingsrecht, alsmede versnippering van de controle en het toezicht en het daarmee gepaard gaande capaciteitstekort) aan te pakken, introduceert de Wpolg extra knelpunten.

Het voorgaande leidt tot de conclusie dat de Wpolg niet in staat is gebleken om de vrijheid van gegevens effectiever te waarborgen dan de Wpolr. Met wetgeving zijn de problemen niet opgelost.

Summary

In this thesis we determine the extent to which the bottlenecks observed under the regime of the Police Registers Act [Wet politieregisters (Wpolr)] have been dealt with by the change in the legal regime relating to the processing of personal details by the police. Since 1990 rules and standards have been in place for the use of police data collections. Initially they were included in the Wpolr; on 1 January 2008 the Police Data Act [Wet Politiegegevens (Wpolg)] came into force. With the implementation of the Wpolg the legislators intended to deal with the bottlenecks that arose through the execution of the Police Registers Act and the Exceptional Police Registers Act [Wet Bijzondere Politieregisters]. The following problem has functioned as the problem statement for the study.

PS: To what extent does the Police Data Act safeguard the proper execution of police duties and the constitutional rights of the citizen more effectively than the Police Registers Act?

To answer this question we investigated the following three research questions:

RQ1: In what way are police duties and the constitutional rights of the citizen involved in the processing of police data?

RQ2: What bottlenecks have been found in the literature and in real life with respect to the safeguarding processing of the Police Registers Act?

RQ3: To what extent does the Police Data Act, also in the light of experiences with the Personal Data Protection Act, deal with the bottlenecks observed?

With the regulation of the processing of police data the legislator introduced three safeguards that should ensure that the use of personal data takes place in accordance with the rules and standards of the legal regime. Both under the current legal regime (Wpolg) and under the old regime of the Police Registers Act (Wpolr) these three safeguards are as follows:

- (1) **The law:** the legal restrictions in the use of personal data as such.
- (2) **Right to inspect:** the right of every individual citizen to, in principle, inspect the data held about him/her in a police register.
- (3) **Monitoring and supervision:** the monitoring and supervision of the use of personal data.

In this thesis the old legal regime is compared with the new legal regime (Chapters 4, 5, and 6) on the basis of these three safeguards. The decision was made in this study, in part as a consequence of a similar choice within the ANITA project (Administrative Normative Information Transaction Agents), to restrict the investigation to data processing by the Criminal Information Units [Crimineel Inlichtingen Eenheden (CIE)] at national level. To set the investigation in the right context a description of the CIE is first provided in Chapter 2. The interests involved in data processing are discussed in Chapter 3.

The development of the Criminal Information Service [Crimineel Inlichtingendienst (CID)] into the CIE is described first of all in Chapter 2. Attention is paid to the changes in the duties and powers of the CID. The provision of information in terms of the detection task came to occupy a central position in the tracing and prevention of serious crime. This development results in a considerable body of rules that regulate (1) the processing of police data by the CIE and (2) the manner in which the CIE obtains its information. Thereafter the gathering and distribution of information by the CIE is discussed extensively. The collection of informant information can in the end be traced back to two different powers: (1) the general police task definition in Art. 2 Police Act [Politie Wet] 1993 and (2) the special powers of investigation for the systematic gathering of information from informants, set out in Art. 126v Dutch Penal Regulation Code [Wetboek strafvordering (Sv)].

Chapter 3 addresses RQ1; the two interests that are involved in data processing by the police are discussed in detail: (A) the proper execution of the police task and (B) the protection interest. For both, interest A and interest B, the identification of the technology-driven development is a necessity. Technological developments offer more instrumental possibilities for interest A and for that reason set higher demands on interest B. Although technology cannot be regarded as an independent interest when drafting the rules of the data protection law, it seems that it is a significant guiding factor in the thinking about the interests involved in the use of data processing. It is from this background that the three safeguards mentioned above are examined in Chapters 4, 5, and 6.

In Chapter 4 the process of information processing by the CIE is discussed. This results in the answers to RQ2 and RQ3 to the extent that they concern the *law as a safeguard*. We describe the way in which the Wpolg deals with the bottlenecks found under the Wpolr when it comes to the (1) saving, (2) storing, (3) distribution, (4) linking, and (5) analysis of police data by the CIE. With the description of the bottlenecks under the Wpolr and the solutions offered by the introduction of the Wpolg, it transpires that these are tangible in three domains, namely (1) the vagueness in conditions of use, (2) the solutions are mainly instrumental in nature and, (3) the need for other stronger safeguards.

(1) Vagueness in application conditions

The most important bottleneck, by far, under the Wpolr turns out to be the vagueness in the rules. This was caused principally by the use of the term ‘necessity’ as a condition of use for the ‘storing’ activities, the ground for refusal to provide information, the linking, and the analysis. Despite the problems that exist in practice this condition is retained unabridged under the Wpolg. Indeed, as we see in the ‘storing’ activity, that necessity as a condition now plays a more prominent role and the Wpolg introduces, with the thematic processing, a new vagueness in conditions of use. Also with the classification bottlenecks found the application conditions remain in use unabridged.

(2) Solutions mainly instrumental

We have seen that the Wpolg has also resolved a number of pressing bottlenecks from an instrumental interest. The delimitation problem between the provisional register and the serious crime register is one instance. In addition, through the Wpolg, solutions have been provided for the very brief storage period of 5 years, the access problems to the informants’ register, and the overly restricted possibilities of providing information to other parties outside the police organisation. Furthermore additional possibilities are offered for data processing with the introduction of thematic processing. The possibilities offered under the Wpolg for the processing of police data are indisputably greater than under the Wpolr. This, however, is at the expense of the constitutional rights of the citizen.

(3) More possibilities, stronger safeguards?

Against these broader instrumental possibilities there is, according to the legislator, a stricter system of safeguards. But this extra protection cannot be expected, however, from the first safeguard. This first safeguard is the processing regime for police data itself. In that there is now, as far as the powers are concerned, in fact a considerable expansion of the possibilities. In the conditions of use vagueness continues to be a very significant factor. We may conclude, on the basis of the new processing regime, that the safeguarding action of the regime of the Wpolg is weakened with respect to the constitutional rights of the citizen. Thus, by way of compensation, more is therefore demanded of the other two safeguards, which are discussed in Chapters 5 and 6.

Chapter 5 examines the *right of inspection as a safeguard*. The bottlenecks determined in this point are mainly practical problems involved with the execution of the right of inspection, which arises from the following two interests: (1) the CIE tries to collect secret information about persons and groups and (2) the criminal would like to know what the police know about him. These two interests are diagonally opposite, which means that not all the information present at the CIE can be provided to the person who has asked to inspect that information. A selection from that information has to be

made first, in relation to the proper execution of the police task. This means that the right to inspect information from the CIE databanks is a practically unexecutable task.

Because a large proportion of the information remains secret in the event of inspection of information at the CIE, it is not possible to conduct a discussion about whether or not part of that information is correctly registered. In Chapter 5 we therefore conclude that the safeguarding effect of the right of inspection leaves much to be desired. The low number of requests and the manner in which they are dealt with contributes, in our view, only marginally to the safeguarding effect. Just as with the first safeguard, the legal system that is discussed in Chapter 4, the lack of safeguarding effect by the right of inspection leads to the conclusion that as a consequence more has to be expected from the third and last safeguard, monitoring and supervision.

Chapter 6 deals with *monitoring and supervision of information processing as a safeguard*. A response to RQ2 and RQ3 in respect of monitoring and supervision as a safeguard is provided. In this chapter we describe how the Wpolg responds to the bottlenecks experienced under the Wpolr in respect of monitoring and supervision by (1) the responsible person, (2) the privacy officer (3) the Dutch Data Protection Agency (Dutch DAP), (4) protocols and auditing, (5) the CIE public prosecutor and (6) the criminal court.

These persons and bodies form potentially very strong monitoring and supervisory mechanisms. The success thereof seems in each of the cases however to be weakened by a lack of capacity. The way in which the monitoring and supervision of the processing of police data at the CIE is devised, in our opinion is too fragmented. The Wpolg did resolve a number of practical bottlenecks for the individual monitoring and supervisory mechanisms, but did not deal with those points relating to capacity and fragmentation. On the contrary, the system under the Wpolg became even more fragmented than under the Wpolr through the introduction of the officer data protection and the compulsory auditing.

None of the persons or bodies named above is able to supervise in terms of content, in every region and on a regular basis. A number of mechanisms have been too easily included in the act without it having defined, specifically for the CIE, whether they will have an effect in practice. Especially now that lack of capacity has turned out to be a pressing problem for the majority of the above-named persons and bodies, to which the Wpolg offers no solution, amendment of these mechanisms is appropriate. This has to be sought, in our view, other than under the Wpolg, in quantitative economies on the one hand and qualitative investment on the other.

The three safeguards (the law, the right to inspection, and monitoring and supervision) have thus been discussed in the afore-going.

The original problem is answered in Chapter 7. Responding to the problem raises the question of whether, with the changes implemented, the police

task (interest A), as well as the protection of the constitutional rights of the citizen (interest B) are more effectively safeguarded than under the Wpolr.

The police task

The Wpolg resolves a number of pressing bottlenecks for the practice of policing by altering the processing regime on a number of points. The changes are, however, mainly changes at the detail level and do not consist of any fundamental changes in the way in which police data should be processed. In our view, no new law was necessary solely for these bottlenecks.

The interpretation of new legislations lies in the fact that the more fundamental bottlenecks will actually be tackled. By fundamental bottlenecks we mean those bottlenecks that arise from the manner of regulation or the purpose of the regulations. We have shown that in respect of the processing of police data there are three of these fundamental bottlenecks, these being (1) the vagueness in the conditions of use, (2) the lack of capacity and (3) the fragmentation observed. We see that the Wpolg leaves these three points untouched. We even saw that at some points the observed bottlenecks will occur in more intense forms. This means that the CIE in practice will continue to be confronted with the same or similar bottlenecks in the processing of police data.

The constitutional rights of the citizen

According to the legislator there is a stricter system of safeguards to counter the more extensive instrumental possibilities. However, it has to be observed that, on the basis of the new processing regime of the Wpolg, the safeguarding effect diminishes when it comes to protecting the constitutional rights of the citizen. Under the Wpolg not much can be expected of the safeguarding effect that should be found in the right of inspection. The right was little used under the Wpolr and the fulfilment of those requests that were made was such that almost no safeguarding effect was exerted.

This means that the necessary extra safeguarding effect has to be offered through the monitoring and supervision mechanism. On that point we have, however, seen that the bottlenecks in the domain of monitoring and supervision – capacity and fragmentation – are strengthened under the Wpolg rather than weakened. The question is therefore very much whether the effectiveness of that monitoring and that supervision is actually greater than under the Wpolr, with the introduction of extra monitoring and supervision mechanisms. Without extra measures being taken, of which none have so far been apparent, we have to conclude that this is not the case.

In conclusion we may state that the Wpolg does offer more possibilities for the processing of police data, but that these greater possibilities are mainly associated with the solution of practical bottlenecks, thereby serving the police task. These greater instrumental possibilities do not however mean that the police task is effectively safeguarded, given that the more fundamental bottlenecks are not tackled.

When it comes to the safeguarding of the constitutional rights of the citizen, we have demonstrated that similar problems occur. Instead of the fundamental bottlenecks being tackled (the rationale of the right to inspect, as well as fragmentation of the monitoring and the supervision and the accompanying lack of capacity), the Wpolg introduces additional bottlenecks.

The foregoing therefore leads to the conclusion that the Wpolg is unable to safeguard the freedom of data more effectively than the Wpolr. The problems have not been resolved with legislation.

Curriculum vitae

Hugo Hendrik Kielman is geboren in Maassluis op 13 maart 1981. 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 diverse andere onderzoeksprojecten, waaronder de evaluatie van de Wet bescherming persoonsgegevens. Vanaf 2007 is Hugo werkzaam als Rechterlijk Ambtenaar In Opleiding in Den Haag, per 1 december 2009 als plaatsvervangend officier van justitie.

Hugo heeft zijn promotieonderzoek uitgevoerd bij eLaw@Leiden, 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 (CWI⁴⁴³) *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*

443 Abbreviations: SIKS – Dutch Research School for Information and Knowledge Systems; CWI – Centrum voor Wiskunde en Informatica, Amsterdam; EUR – Erasmus Universiteit, Rotterdam; KUB – Katholieke Universiteit Brabant, Tilburg; KUN – Katholieke Universiteit Nijmegen; OU – Open Universiteit; RUL – Rijksuniversiteit Leiden; RUN – Radboud Universiteit Nijmegen; TUD – Technische Universiteit Delft; TU/e – Technische Universiteit Eindhoven; UL – Universiteit Leiden; UM – Universiteit Maastricht; UT – Universiteit Twente, Enschede; UU – Universiteit Utrecht; UvA – Universiteit van Amsterdam; UvT – Universiteit van Tilburg; VU – Vrije Universiteit, Amsterdam.

- 6 Martijn van Welie (VU) *Task-Based User Interface Design*
- 7 Bastiaan Schonhage (VU) *Divia: 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 Weerd (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 Politie 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) *Fundamentals 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 Ramirez Camps (CWI) *Structural Features in XML Retrieval*
- 25 Joost Schalken (VU) *Empirical Investigations in Software Process Improvement*

2008

- 1 Katalin Boer-Sorbán (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 Knowledge 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-Universität 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: Controlling 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*
- 35 Wouter Koelewijn (UL) *Privacy en Politiegegevens; Over geautomatiseerde normatieve informatie-uitwisseling*
- 36 Marco Kalz (OUN) *Placement Support for Learners in Learning Networks*
- 37 Hendrik Drachsler (OUN) *Navigation Support for Learners in Informal Learning Networks*
- 38 Riina Vuorikari (OU) *Tags and self-organisation: a metadata ecology for learning resources in a multilingual context*
- 39 Christian Stahl (TUE, Humboldt-Universitaet zu Berlin) *Service Substitution -- A Behavioral Approach Based on Petri Nets*
- 40 Stephan Raaijmakers (UvT) *Multinomial Language Learning: Investigations into the Geometry of Language*
- 41 Igor Berezhnyy (UvT) *Digital Analysis of Paintings*
- 42 Toine Bogers (UvT) *Recommender Systems for Social Bookmarking*
- 43 Virginia Nunes Leal Franqueira (UT) *Finding Multi-step Attacks in Computer Networks using Heuristic Search and Mobile Ambients*
- 44 Roberto Santana Tapia (UT) *Assessing Business-IT Alignment in Networked Organizations*
- 45 Jilles Vreeken (UU) *Making Pattern Mining Useful*
- 46 Loredana Afanasiev (UvA) *Querying XML: Benchmarks and Recursion*

2010

- 1 Matthijs van Leeuwen (UU) *Patterns that Matter*
- 2 Ingo Wassink (UT) *Work flows in Life Science*
- 3 Joost Geurts (CWI) *A Document Engineering Model and Processing Framework for Multimedia documents*
- 4 Olga Kulyk (UT) *Do You Know What I Know? Situational Awareness of Co-located Teams in Multi-display Environments*
- 5 Claudia Hauff (UT) *Predicting the Effectiveness of Queries and Retrieval Systems*
- 6 Sander Bakkes (UvT) *Rapid Adaptation of Video Game AI*
- 7 Wim Fikkert (UT) *A Gesture interaction at a Distance*
- 8 Krzysztof Siewicz (UL) *Towards an Improved Regulatory Framework of Free Software. Protecting user freedoms in a world of software communities and eGovernments*

In de boekenreeks van de Graduate School of Legal Studies van de Faculteit der Rechtsgeleerdheid, Universiteit Leiden, zijn in 2009 en 2010 verschenen:

- 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) 2009 ISBN-13 978 90 4113 115 7
- 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
- MI-163 W.B. van Bockel, *The ne bis in idem principle in EU law*, (diss. Leiden), Amsterdam: Ipskamp 2009, ISBN 978 90 90 24382 5
- MI-164 J. Cartwright, *The English Law of Contract: Time for Review?*, (oratie Leiden), Leiden 2009.
- MI-165 W.I. Koelewijn, *Privacy en politiegegevens. Over geautomatiseerde normatieve informatie-uitwisseling*, (diss. Leiden), Leiden: Leiden University Press 2009, ISBN 9 789087 280703
- MI-166 S.R.M.C. Guèvremont, *Vers un traitement équitable des étrangers extracommunautaires en séjour régulier. Examen des directives sur le regroupement familial et sur les résidents de longue durée*, (diss. Leiden), Zutphen: Wöhrmann Printing Service 2009, ISBN 978 90 8570 419 5
- MI-167 A.G. Castermans, I.S.J. Houben, K.J.O. Jansen, P. Memelink & J.H. Nieuwenhuis (red.), *Het zwijgen van de Hoge Raad*, Deventer: Kluwer 2009, ISBN 978 90 13 07029 3
- MI-168 P.M. Schuyt, *Verantwoorde straftoemeting*, (diss. Nijmegen), Deventer: Kluwer 2009, ISBN 978 90 1307 156 6
- MI-169 P.P.J. van der Meij, *De driehoeksverhouding in het strafrechtelijk vooronderzoek*, (diss. Leiden), Deventer: Kluwer 2010, ISBN 978 90 1407 158 0
- MI-170 M.V. Polak (red.), *Inbedding van Europese procesrechtelijke normen in de Nederlandse rechtsorde*, Nijmegen: Ars Aequi Libri 2010, ISBN 978 90 6916 714 5
- MI-171 E. Koops, *Vormen van subsidiariteit. Een historisch-comparistische studie naar het subsidiariteitsbeginsel bij pand, hypotheek en borgtocht*, (diss. Leiden), Den Haag: Boom Juridische uitgevers 2010, ISBN 978 90 8728 070 3
- MI-172 H.H. Kielman, *Politiële gegevensverwerking. Naar een effectieve waarborging*, (diss. Leiden 2010). ISBN 978 90 8570 503 1
- MI-173 K. Siewicz, *Towards an Improved regulatory Framework of Free Software. Protecting user freedoms in a world of software communities and eGovernments*, (diss. Leiden 2010).
- MI-174 Laurens Mommers, Hans Franken, Jaap van den Herik, Franke van der Klaauw, Gerrit-Jan Zwenne (red.) *Het binnenste buiten. (Liber amicorum Leiden)*. Leiden: eLaw@leiden 2010.

Zie voor de volledige lijst van publicaties: www.law.leidenuniv.nl/onderzoek