



Universiteit  
Leiden  
The Netherlands

**Gegevensverwerking in het kader van de opsporing. Toepassing van datamining ten behoeve van de opsporingstaak: afweging tussen het opsporingsbelang en het recht op privacy.**

Sietsma, R.

**Citation**

Sietsma, R. (2007, January 10). *Gegevensverwerking in het kader van de opsporing. Toepassing van datamining ten behoeve van de opsporingstaak: afweging tussen het opsporingsbelang en het recht op privacy*. SDu Uitgevers, Den Haag. Retrieved from <https://hdl.handle.net/1887/8599>

Version: Corrected Publisher's Version

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

Downloaded from: <https://hdl.handle.net/1887/8599>

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

Gegevensverwerking  
in het kader van de opsporing



# GEGEVENSVERWERKING IN HET KADER VAN DE OPSPORING

TOEPASSING VAN DATAMINING  
TEN BEHOEVE VAN DE OPSPORINGSTAAK:  
AFWEGING TUSSEN HET OPSPORINGSBELANG  
EN HET RECHT OP PRIVACY

## PROEFSCHRIFT

ter verkrijging van  
de graad van Doctor aan de Universiteit Leiden,  
op gezag van de Rector Magnificus Dr. D.D. Breimer,  
hoogleraar in de faculteit der Wiskunde en  
Natuurwetenschappen en die der Geneeskunde,  
volgens besluit van het College voor Promoties  
te verdedigen op woensdag 10 januari 2007  
klokke 15.00 uur

*door*

Ruben Sietsma

geboren te Hengelo (O) in 1977

*Promotiecommissie:*

- Promotor: prof. mr. H. Franken
- Referent: prof. mr. Y. Buruma (Radboud Universiteit Nijmegen)
- Leden: prof. mr. P.A.M. Mevis (Erasmus Universiteit Rotterdam)  
prof. dr. H.J. van den Herik (Universiteit Maastricht en  
Universiteit Leiden)  
prof. mr. A.H.J. Schmidt  
prof. mr. Th.A. de Roos (Universiteit van Tilburg)

Van deze uitgave verschijnt een handelseditie onder ISBN 90 12 11826 3.

© R. Sietsma, Leiden, 2006

Ontwerp omslag en binnenwerk: Villa Y, Den Haag

Zetwerk: [www.az-gsb.nl](http://www.az-gsb.nl), Den Haag

Alle rechten voorbehouden. Behalve de door de Auteurswet 1912 gestelde uitzonderingen, mag niets uit deze uitgave worden veeelvoudigd (waaronder begrepen het opslaan in een geautomatiseerd gegevensbestand) en/of openbaar gemaakt door middel van druk, fotokopie, microfilm of op welke andere wijze dan ook, zonder voorafgaande schriftelijke toestemming van de uitgever.

De bij toepassing van art. 16b en 17 Auteurswet 1912 wettelijk verschuldigde vergoedingen wegens kopiëren dienen te worden voldaan aan de Stichting Reprorecht, Postbus 3060, 2130 KB Hoofddorp, tel.: 023-7997810.

Voor het overnemen van een gedeelte van deze uitgave in bloemlezingen, readers en andere compilatiewerken op grond van art. 16 Auteurswet 1912 dient men zich te wenden tot de stichting PRO, Postbus 3060, 2130 KB Hoofddorp, tel.: 023-7997809. Voor het overnemen van ene gedeelte van deze uitgave ten behoeve van commerciële doeleinden dient men zich te wenden tot de uitgever.

Hoewel aan de totstandkoming van deze uitgave de uiterste zorg is besteed, kan voor de afwezigheid van eventuele (druk)fouten en onvolledigheden niet worden ingestaan en aanvaardt auteur(s), redacteur(en) en uitgever deswege geen aansprakelijkheid voor de gevolgen van eventueel voorkomende fouten en onvolledigheden.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system of any nature, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written permission of the publisher.

While every effort has been made to ensure the reliability of the information presented in this publication, Sdu Uitgevers neither guarantees the accuracy of the data contained herein nor accepts responsibility for errors or omissions or their consequences.

---

# Inhoudsopgave

<b>Woord vooraf</b>	<b>13</b>
<b>Lijst van afkortingen</b>	<b>15</b>
<b>1 Opzet van het onderzoek</b>	<b>17</b>
1.1 Aanleiding	17
1.2 Het sociaal contract	19
1.2.1 Spanningsveld	20
1.3 Datamining	22
1.3.1 Bewerken en verwerken	24
1.3.2 Het dataminingsproces	25
1.3.3 De fasen van het dataminingsproces	26
1.3.4 Toepassing van het dataminingsproces	27
1.4 Onderzoeksvragen	29
1.5 Afbakening van het onderzoeksdomein	32
1.6 Plan van aanpak	34
<b>2 Het proces van informatiegaring</b>	<b>37</b>
2.1 De opsporingstaak	37
2.2 De Parlementaire Enquêtecommissie	38
2.3 Het proces van informatiegaring	40
2.3.1 Stadium A: Het opbouwen en in stand houden van een zekere informatiepositie	40
2.3.1.1 Het opslaan, bewerken, gebruiken en analyseren van gegevens	41
2.3.1.2 Het vergaren van gegevens door de toepassing van niet-ingrijpende middelen	41
2.3.1.3 Verhouding tot fase I van de PEC	44
2.3.2 Stadium B: Het verkennend onderzoek	44
2.3.2.1 Verhouding tot fase II van de PEC	49
2.3.3 Stadium C: Het opsporingsonderzoek	50
2.3.3.1 De pro-actieve fase	53
2.3.3.2 Verhouding tot fase III van de PEC	54

2.3.4	Schema wettelijke regeling opsporing versus visie PEC	55
2.4	Inzet van bijzondere opsporingsmethoden en verbetering van de informatiepositie	55
<b>3</b>	<b>Het proces van informatiegaring en datamining</b>	<b>61</b>
3.1	Informatiegaring en informatie-inwinning	61
3.2	Onderzoeksmethoden	62
3.2.1	Misdaadanalyse	63
3.2.2	Flexibiliteit dataminingsproces	66
3.3	Uitgangspunten toepassing dataminingonderzoek	68
3.4	Van dataminingsproces naar onderzoeksmethode	71
3.4.1	Het ongerichte dataminingonderzoek	72
3.4.2	Het gerichte dataminingonderzoek	75
3.4.3	Verificatie	78
3.4.4	Schema van de drie stadia van het dataminingproces als opsporingsmethode	80
3.5	De toepassingsvarianten van het dataminingsproces en het proces van informatiegaring	80
3.5.1	Het ongerichte dataminingonderzoek	81
	3.5.1.1 Terugkoppeling naar het proces van informatiegaring	81
	3.5.1.2 Verkennend onderzoek en opsporingsonderzoek	81
3.5.2	Het gerichte dataminingonderzoek	82
	3.5.2.1 Terugkoppeling naar het proces van informatiegaring	83
	3.5.2.2 Het verkennend onderzoek	84
	3.5.2.3 Het opsporingsonderzoek	85
3.5.3	De verificatie	88
3.6	Het juridische kader	89
<b>4</b>	<b>De Wet Politierregisters en het Besluit Politierregisters</b>	<b>91</b>
4.1	Bescherming van de persoonlijke levenssfeer	92
4.2	De Wet Politierregisters	98
4.2.1	Algemene voorwaarden dataminingonderzoek	99
	4.2.1.1 Aanleg en inhoud politieregister	99
	4.2.1.2 Het reglement	100
	4.2.1.3 Datawarehouse en reglement	101
	4.2.1.4 Het modelreglement	102
4.2.2	Voorwaarden voor het verwerken van gegevens	104
	4.2.2.1 Het gebruik van persoonsgegevens	104
	4.2.2.2 Registratie op grond van bepaalde kenmerken	105
	4.2.2.3 Het gebruik van zachte opsporingsinformatie	106
	4.2.2.4 Koppeling	109

4.2.2.5	Het verstrekkingenregime	115
4.2.2.6	Het doelbindingsbeginsel	120
4.3	<b>Afsluitend</b>	<b>122</b>
<b>5</b>	<b>Het datawarehouse</b>	<b>125</b>
5.1	<b>Kenmerken van het politieregister</b>	<b>126</b>
5.1.1	Geen verplichte aanleg politieregister	128
5.1.2	Status datawarehouse	128
5.2	<b>Kwalificatie datawarehouse</b>	<b>135</b>
5.2.1	Varianten dataminingonderzoek	135
5.2.2	Kwalificatie datawarehouse gericht dataminingonderzoek	137
5.2.2.1	Doelstelling	138
5.2.2.2	Verstrekkingenregime	139
5.2.2.3	Tijdelijk karakter	143
5.2.3	Ontbreken reglement tijdelijk politieregister	144
5.2.3.1	Modelreglement	145
5.3	<b>Afsluitend</b>	<b>146</b>
<b>6</b>	<b>Koppeling</b>	<b>149</b>
6.1	<b>Koppelingsvormen</b>	<b>149</b>
6.2	<b>De wettelijke koppelingsregeling</b>	<b>154</b>
6.2.1	Koppeling en registervergelijking	155
6.2.2	Onderscheid tussen bepaald en onbepaald	156
6.2.3	Kenmerken van juridische koppeling	158
6.3	<b>Verhouding van juridische koppeling volgens Wpolr tot de koppelingsvormen</b>	<b>158</b>
6.4	<b>Bewustwording en verduidelijking</b>	<b>160</b>
6.5	<b>Koppeling en het dataminingsproces</b>	<b>163</b>
6.5.1	Het bevragen van bestanden op een bepaalde persoon	164
6.5.2	Koppeling en verstrekking van gegevens	166
6.6	<b>Overzicht koppeling</b>	<b>167</b>
6.7	<b>Afsluitend</b>	<b>168</b>
<b>7</b>	<b>Ongericht dataminingonderzoek en de gewone politieregisters</b>	<b>169</b>
7.1	<b>Functies politieregisters en dataminingonderzoek</b>	<b>169</b>
7.2	<b>Toepassing ongericht dataminingonderzoek</b>	<b>171</b>
7.3	<b>Vier verschillende onderzoeksmogelijkheden</b>	<b>173</b>
7.3.1	Geen gebruik externe gegevens	173
7.3.2	Het gebruik van externe, niet uit een politieregister afkomstige gegevens	177

7.3.2.1	Aard ongericht dataminingonderzoek	178
7.3.2.2	Koppeling	179
7.3.2.3	Wpr en Wbp	180
7.3.2.4	Vrijwillige verstrekking en ‘fishing expeditions’	182
7.3.2.5	Gebruik van gegevens uit openbare registers	184
7.3.3	Het gebruik van gegevens uit een gewoon politieregister	186
7.3.3.1	De doelbinding	187
7.3.3.2	De aard van de politietaak	189
7.3.3.3	Koppeling	193
7.3.3.4	De aard van het ongerichte dataminingonderzoek	194
7.3.3.5	Weigering door de beheerder	200
7.3.4	Het gebruik van gegevens uit een bijzonder politieregister	202
7.3.4.1	Het gebruik van een tijdelijk politieregister	205
7.3.4.2	Het gebruik van een voorlopig politieregister	208
7.3.4.3	Het gebruik van het register zware criminaliteit	213
7.4	Afsluitend	226
<b>8</b>	<b>Onggericht dataminingonderzoek en het register</b>	
	<b>Ongebruikelijke Transacties</b>	<b>233</b>
8.1	Toepassing van ongericht dataminingonderzoek	236
8.2	Vier verschillende onderzoeksmogelijkheden	240
8.2.1	Geen gebruik externe gegevens	240
8.2.2	Het gebruik van externe, niet uit een politieregister afkomstige gegevens	242
8.2.2.1	De aard van ongericht dataminingonderzoek	243
8.2.2.2	Koppeling	244
8.2.2.3	Vrijwillige verstrekking van gegevens	245
8.2.2.4	Gebruik van gegevens uit openbare registers	246
8.2.3	Gebruik van gegevens uit een gewoon politieregister	247
8.2.3.1	De doelbinding	248
8.2.3.2	De aard van de politietaak	248
8.2.3.3	Koppeling	249
8.2.3.4	De aard van ongericht dataminingonderzoek	250
8.2.3.5	Het gebruik van de MRO-verwijsindex	250
8.2.3.6	Weigering door de beheerder	260
8.2.4	Het gebruik van gegevens uit een bijzonder politieregister	261
8.2.4.1	Het gebruik van een tijdelijk politieregister	262
8.2.4.2	Het gebruik van een voorlopig politieregister	263
8.2.4.3	Het register zware criminaliteit	266
8.2.4.4	Conclusie verwerking bijzondere politieregisters	270
8.3	Afsluitend	271

<b>9</b>	<b>Ongericht dataminingonderzoek en de bijzondere politieregisters</b>	<b>277</b>
9.1	De criminele inlichtingeneenheden	277
9.1.1	De toepassing van dataminingonderzoek	279
9.1.2	Datamining door de CIE	281
9.1.3	Datamining door de NCIE	282
9.2	Functieverdeling bijzondere politieregisters	284
9.2.1	Analyse register zware criminaliteit en voorlopig politieregister	286
9.3	Ongericht dataminingonderzoek en het tijdelijke politieregister	288
9.4	Ongericht dataminingonderzoek en het voorlopige politieregister	291
9.5	Vier verschillende onderzoeksmogelijkheden	294
9.5.1	Geen gebruik van externe gegevens	294
9.5.2	Het gebruik van niet uit een politieregister afkomstige gegevens	295
9.5.2.1	De aard van ongericht dataminingonderzoek	295
9.5.2.2	Koppeling	297
9.5.2.3	Vrijwillige verstrekking	298
9.5.2.4	Het gebruik van gegevens uit openbare registers	298
9.5.3	Het gebruik van gegevens uit een gewoon politieregister	299
9.5.3.1	Beperkingen aan het gebruik van gewone politieregisters	299
9.5.4	Het gebruik van gegevens uit een bijzonder politieregister	307
9.5.4.1	Het gebruik van een tijdelijk politieregister	307
9.5.5	Het gebruik van een ander voorlopige politieregister	311
9.5.6	Het gebruik van het register zware criminaliteit	311
9.5.6.1	De doelbinding	311
9.5.6.2	Koppeling	313
9.5.6.3	De aard van het ongerichte dataminingonderzoek	313
9.5.6.4	Weigering door de beheerder	314
9.5.7	De mogelijkheden ter verbetering van de informatiepositie van een voorlopig politieregister	315
9.6	Ongericht dataminingonderzoek en het register zware criminaliteit	316
9.7	Vier verschillende onderzoeksmogelijkheden	319
9.7.1	Geen gebruik van externe gegevens	321
9.7.2	Het gebruik van niet uit een politieregister afkomstige gegevens	322
9.7.2.1	De aard van ongericht dataminingonderzoek	322
9.7.2.2	Koppeling	324
9.7.2.3	Vrijwillige verstrekking	325
9.7.2.4	Gebruik van gegevens uit openbare registers	325
9.7.3	Het gebruik van gegevens uit een gewoon politieregister	326
9.7.3.1	De doelbinding	326
9.7.3.2	De aard van de politietaak	327
9.7.3.3	Koppeling	328

9.7.3.4	De aard van het ongerichte dataminingonderzoek	328
9.7.4	Het gebruik van gegevens uit een bijzonder politieregister	329
9.7.4.1	Het gebruik van een tijdelijk politieregister	329
9.7.4.2	Het gebruik van een voorlopig politieregister	332
9.7.4.3	Het gebruik van een ander register zware criminaliteit	334
9.7.5	Afsluitend	335
<b>10</b>	<b>Het gerichte dataminingonderzoek</b>	<b>341</b>
10.1	Kenmerken gericht dataminingonderzoek	341
10.2	Positie binnen het proces van informatiegaring	342
10.2.1	Het verkennend onderzoek	343
10.2.1.1	Beperkingen van het verkennend onderzoek	345
10.2.1.2	Datawarehouse	348
10.2.2	Het opsporingsonderzoek	350
10.2.3	Toepassingsmogelijkheden van het gerichte dataminingonderzoek	352
10.3	Gericht dataminingonderzoek en het tijdelijke politieregister	353
10.3.1	Geen gebruik van externe gegevens	354
10.3.2	Gebruik van niet uit een politieregister afkomstige gegevens	354
10.3.2.1	De aard van het gerichte dataminingonderzoek	355
10.3.2.2	Koppeling	355
10.3.2.3	Vrijwillige verstrekking	356
10.3.2.4	Gebruik van gegevens uit openbare registers	356
10.3.3	Het gebruik van gegevens uit een gewoon politieregister	357
10.3.3.1	De doelbinding	357
10.3.3.2	De aard van de politietaak	358
10.3.3.3	Koppeling	358
10.3.3.4	De aard van het gerichte dataminingonderzoek	358
10.3.3.5	Het BPS	359
10.4	Het gebruik van gegevens uit een bijzonder politieregister	359
10.4.1	Het gebruik van een tijdelijk politieregister	359
10.4.1.1	De doelbinding	359
10.4.1.2	Koppeling	360
10.4.1.3	De aard van het gerichte dataminingonderzoek	360
10.5	Het gebruik van een voorlopig politieregister	361
10.5.1	De doelbinding	362
10.5.2	Koppeling	362
10.5.3	De aard van het gerichte dataminingonderzoek	363
10.6	Het gebruik van het register zware criminaliteit	364
10.6.1	De doelbinding	364
10.6.2	Koppeling	365
10.6.3	De aard van het gerichte dataminingonderzoek	365

10.6.4 Weigering door de beheerder	366
10.7 Afsluitend	366
<b>11 Beantwoording van de onderzoeksvragen</b>	<b>369</b>
Conclusies en aanbevelingen	369
11.1 Het strafvorderlijke kader voor dataminingonderzoek	370
11.1.1 Datamining en het proces van informatiegaring	370
11.1.2 Wettelijke inkadering datamining	374
11.1.2.1 Datamining als opsporingsmiddel	374
11.1.2.2 Het belang van wettelijke regeling van het dataminingsproces	376
11.1.2.3 Reikwijdte van de bestaande wettelijke grondslag	377
11.1.2.4 Uitgangspunten van de wettelijke regeling	380
11.1.3 Conclusies en aanbevelingen met betrekking tot het strafvorderlijke kader voor dataminingonderzoek	381
11.2 Het privacyrechtelijk kader voor de toepassing van dataminingonderzoek	382
11.2.1 Uitwerking privacybescherming in de WPoI en het BPOI	383
11.2.1.1 Beperkte verwerking van gevoelige en zachte gegevens	384
11.2.1.2 Het doelbindingsbeginsel	384
11.2.1.3 Het noodzakelijkheidsbeginsel	386
11.2.1.4 Het reglement	388
11.2.1.5 Handhaving privacywaarborgen in wet- en regelgeving	388
11.2.2 Conclusies en aanbevelingen met betrekking tot het privacyrechtelijke kader voor dataminingonderzoek	390
11.3 Toepassing van dataminingonderzoek ten behoeve van de opsporingstaak	392
11.3.1 Registratie	392
11.3.1.1 Kwalificatie datawarehouse	393
11.3.1.2 Beperkende werking functies politieregisters	394
11.3.1.3 Beperkingen van het reglement	398
11.3.1.4 Raadplegen van het datawarehouse	399
11.3.2 Analysefunctie in de koppelingsregeling van artikel 6 WPoI	400
11.3.2.1 De koppeling	400
11.3.2.2 Herziening van de koppelingsregeling	402
11.3.2.3 Proces-verbaal koppeling	405
11.3.2.4 Het reglement	406
11.3.3 Raadplegen en het (doen) verwerken van gegevens	407
11.3.3.1 Onderscheid raadplegen en analyseren	407
11.3.3.2 Het spanningsveld tussen voor- en nadelen van algemene beschikbaarheid binnen het politieapparaat	407
11.3.3.3 Het (doen) uitvoeren van een analyse	408

11.3.4	Conclusies en aanbevelingen in het kader van toepassing van dataminingonderzoek ten behoeve van de opsporingstaak	409
11.3.4.1	Conclusies en aanbevelingen in het kader van de registratie	409
11.3.4.2	Conclusies en aanbevelingen in het kader van de analyse-functie in de koppelingsregeling van art. 6 WPolr	410
11.3.4.3	Conclusies en aanbevelingen in het kader van raadplegen en het (doen) verwerken van gegevens	414
<b>12</b>	<b>Eindconclusies en aanbevelingen</b>	<b>417</b>
<b>13</b>	<b>Beschouwing wetsvoorstel Wet Politiegegevens</b>	<b>421</b>
13.1	Algemeen	422
13.2	De verwerking van politiegegevens	424
13.2.1	De dagelijkse uitvoering van de politietaak	425
13.2.2	Gerichte verwerking van artikel 9	428
13.2.3	Gerichte verwerking van artikel 10	429
13.2.4	Geautomatiseerd vergelijken en in combinatie zoeken artikel 11	434
13.2.5	Ondersteunende taken van artikel 13	436
13.3	Ten slotte	437
	<b>Summary</b>	<b>441</b>
	<b>Literatuurlijst</b>	<b>449</b>
	<b>Trefwoordenregister</b>	<b>457</b>
	<b>Over de auteur</b>	<b>461</b>

---

## Woord vooraf

In zijn brief van medio juli 2004 aan de Tweede Kamer der Staten-Generaal stelt de minister van Binnenlandse Zaken en Koninkrijksrelaties:

*'Zoals in de brief gemeld is de inzet voor alles gericht op het zo vroeg mogelijk identificeren van de voorbereiding van mogelijke terroristische acties en de daders daarvan. Nieuwe vormen van geautomatiseerde data-analyse worden daarvoor ingezet, zoals het zoeken aan de hand van profielen en het opsporen van bepaalde patronen met behulp van data-mining. Daartoe moeten grote bestanden met persoonsgegevens van niet-verdachte personen doorzocht worden (...).'*<sup>1</sup>

Het kabinetsbeleid staat zeer ruime mogelijkheden voor inzake gegevensverwerking door opsporingsinstanties en veiligheidsdiensten, teneinde in de veranderende maatschappelijke werkelijkheid hun werk te kunnen blijven doen. Hierbij wordt het gebruik van dataminingstechnieken met zoveel woorden genoemd. In het kader van de bestrijding van terroristische acties lijken nauwelijks nog beperkingen te gelden voor het verwerken van informatie over personen, verdacht of onverdacht. Het is de vraag in hoeverre dergelijke ruime mogelijkheden tot de verwerking van informatie en daarmee gepaard gaande inbreuken op de privacy wenselijk en toelaatbaar zijn. De maatschappelijke ontwikkelingen nopen de wetgever tot het vinden van een balans tussen het effectief waarborgen van de veiligheid van de burger enerzijds en de bescherming van de privacy van diezelfde burger anderzijds.

Dit onderzoek beoogt duidelijkheid te scheppen omtrent de mogelijkheden en onmogelijkheden van de verwerking van gegevens in het kader van de opsporingstaak. Daartoe is onder meer voor het gebruik van datamining onderzocht wat binnen de grenzen van de juridische en maatschappelijke kaders wenselijk en mogelijk is. De verschillende vraagstukken die in dit onderzoek worden behandeld hangen sterk met elkaar samen. Het streven naar een zo volledig mogelijk juridisch over- en inzicht ten behoeve van de verwerking van gegevens in het kader van de opsporing zal onvermijdelijk leiden tot enige

---

1. *Kamerstukken II, 2003 /04, 29 200 VII, nr. 61.*

herhalingen in het betoog. Om de resultaten van dit onderzoek breed inzichtelijk te maken zijn de noodzakelijke juridische verdiepingen en kaders vertaald in tabellen.

Gedurende de afronding van dit proefschrift verschenen de evaluatie van de Wet bijzondere politieregisters en het wetsvoorstel Wet Politiegegevens ter vervanging van de Wet Politieregisters. Met instemming heb ik kennis genomen van het feit dat de knelpunten en oplossingsrichtingen die in het proefschrift worden beschreven, ook in een breder verband worden onderkend en gedragen. Voor een volledig beeld dienaangaande is de visie van de wetgever inzake de verwerking van politiegegevens, als verwoord in voornoemd wetsvoorstel, in de vorm van een naschrift getoetst aan de conclusies en aanbevelingen die uit dit onderzoek naar voren komen.

Op deze plaats wil ik een ieder die op enigerlei wijze een bijdrage heeft geleverd aan de realisatie van dit proefschrift, waaronder vanzelfsprekend alle medewerkers van de afdeling eLaw@Leiden, van harte dankzeggen.

Een speciaal woord van dank gaat uit naar Fenna Bruininkweerd, die mij vanaf de aanvang van dit onderzoek met raad en daad heeft bijgestaan.

Dit onderzoek kwam tot stand in het kader van het Nationaal Programma Informatietechnologie en Recht (ITzR) en werd uitgevoerd bij de afdeling eLaw@Leiden, centrum voor recht in de informatiemaatschappij van de Universiteit Leiden.

---

## Lijst van afkortingen

ABRIO	Aanpak Bedrijfsvoering Recherche Informatiehuishouding en Opleidingen
AMvB	Algemene maatregel van bestuur
BOB	Bijzondere opsporingsbevoegdheden
BOOM	Bureau Ontnemingswetgeving Openbaar Ministerie
BPoI	Besluit Politierregisters
BPS	Bedrijfsprocessensysteem
CBP	College Bescherming Persoonsgegevens
CID	Criminele Inlichtingendienst
CIE	Criminele Inlichtingen Eenheid
CRI	Centrale Recherche Informatiedienst
CTC	Centrale Toetsingscommissie
DNRI	Dienst Nationale Recherche Informatie
EG	Europese Gemeenschap
EK	Eerste Kamer
EU	Europese Unie
EVRM	Europees Verdrag ter bescherming van de Rechten van de Mens en de fundamentele vrijheden
Gw	Grondwet
HKS	Herkenningsdienstsysteem
HR	Hoge Raad
ICT	Informatie- en Communicatie Technologie
IGO	Informatiegestuurde opsporing
IRT	Interregionaal Recherche Team
IT&R	Nationaal Programma voor Informatietechnologie en Recht
IVBPR	Internationaal Verdrag inzake Burgerrechten en Politieke Rechten
KDD	Knowledge discovery in databases
KLPD	Korps Landelijke Politie Diensten
KMar	Koninklijke Marechaussee
LOvJ	Landelijk Officier van Justitie
MDRO	Meldingen Districtelijke Recherche-Onderzoeken
MOT	Meldpunt Ongebruikelijke Transacties
MRO	Meldingen Recherche-Onderzoeken
MvA	Memorie van antwoord

MvJ	Minister van Justitie
MvT	memorie van toelichting
NCIE	Nationale Criminele Inlichtingen Eenheid
NI	Unit Nationaal Inzicht
<i>NJ</i>	<i>Nederlandse Jurisprudentie</i>
<i>NJB</i>	<i>Nederlands Juristenblad</i>
NvT	Nota van toelichting
OM	Openbaar Ministerie
OOH-register	Register openbare-ordehandhaving
OPS	Opsporingsregister
OvJ	Officier van Justitie
PbEG	Publicatieblad van de Europese Gemeenschappen
PEC	Parlementaire Enquêtecommissie Opsporingsmethoden (Commissie Van Traa)
PSO	Politie Suite Opsporing
RAF	Roten Armee Fraktion
RIP	Regeling Informatiebeveiliging Politie
RIU	unit Recherche Informatie Uitwisseling
<i>Stcrt</i>	<i>Staatscourant</i>
<i>Stb.</i>	<i>Staatsblad</i>
Sv	Wetboek van Strafvordering
TK	Tweede Kamer
VROS	Verwijzingsindex Recherche-Onderzoeken Subjecten
Wbp	Wet bescherming persoonsgegevens
WED	Wet op de economische delicten
WES	Wetgeving voor de Elektronische Snelweg
Wet MOT	Wet melding ongebruikelijke transacties
WMM	Wet wapens en munitie
WPolg	Wet Politiegegevens
WPolr	Wet Politierregisters
Wpr	Wet Persoonsregistraties
WVW	Wegenverkeerswet
WWW	World Wide Web

---

# 1 Opzet van het onderzoek

*‘De mens is tot zoveel in staat als hij weet, eerst door kennis is hij in staat de natuur te beheersen, zijn wereld vorm te geven, want kennis is macht’*  
– Francis Bacon –

## 1.1 Aanleiding

Het waarheidsgehalte achter de wijsheid ‘kennis is macht’ van de Engelse filosoof Francis Bacon vindt op evidente wijze bevestiging in onze hedendaagse samenleving. Door de turbulente ontwikkelingen op het gebied van de informatie- en communicatietechnologie (ICT) is de wijze waarop informatie kan worden verzameld, bewaard en bewerkt drastisch veranderd. Ook de schaal waarop directe en indirecte informatiegaring plaatsvindt is enorm toegenomen. Instellingen en bedrijven beschikken over veel en goed toegankelijke gegevens over personen die hun diensten en producten afnemen, of van wie zij om andere redenen gegevens verwerken. In onze dagelijkse handel en wandel laten wij steeds frequenter elektronische sporen na. Mobiel telefoneren, betalen met de pinpas of surfen op het internet zijn voorbeelden van alledaagse handelingen die gepaard gaan met de, veelal digitale, opslag van gegevens met betrekking tot die handelingen<sup>1</sup>. Al deze gegevens kunnen informatie (kennis) bevatten waarmee op uiteenlopende terreinen voordeel (macht) kan worden behaald. Er bestaat een groot verschil tussen informatie en kennis. Een overvloed aan informatie kan het inzicht verminderen en initiatieven ontmoedigen. Bij dataminingonderzoek gaat het niet om het verkrijgen van maximale, maar van optimale informatie, welke uiteindelijk kennis oplevert.

In dit onderzoek worden de begrippen ‘gegevens’, ‘informatie’ en ‘kennis’ gehanteerd<sup>2</sup>. Wanneer hier wordt gesproken over gegevens gaat het om gegevens in de zin van informatie. Wij definiëren informatie als geïnterpreteerde gegevens, dat wil zeggen: gegevens die van een betekenis zijn voorzien. EJ-LN-59 is een Nederlands nummerbord; +31715255873 is een Nederlands telefoonnummer. Gegevens die in het kader van een dataminingonderzoek worden gebruikt en daartoe in een datawarehouse zijn opgeslagen,

- 
1. Zie ook *Kamerstukken II*, 2000 /01, 25 764, nr. 17 inzake het toenemende gebruik van nieuwe identificatiemethoden, (Reisdocumenten; verslag algemeen overleg op 21 juni 2001, over biometrie in reisdocumenten en elektronische identiteitskaart).
  2. Zie ook Schreiber e.a. 2000.

kunnen in beginsel steeds worden aangemerkt als informatie. Zij hebben een bepaalde betekenis voor het onderzoek waarvoor zij worden gebruikt. Op grond van die betekenis worden ze geselecteerd. Kennis is informatie die in een context is geplaatst. Wanneer de gegevens in een datawarehouse worden bewerkt, vindt die bewerking plaats in een context en kunnen de resultaten na afloop van een dataminingonderzoek in een context worden geplaatst. Er is sprake van kennis aan het einde van elk afzonderlijk dataminingonderzoek.

Door de kwantiteit van de informatie wordt het steeds moeilijker om bruikbare kennis te onderscheiden van nutteloze informatie. Een goed voorbeeld van de enorme expansie van het informatieaanbod is het internet. Zonder de juiste software is het voor de gebruikers van dit wereldwijde netwerk vrijwel onmogelijk om hun weg te vinden naar de gewenste informatie. De technologische ontwikkelingen hebben echter gezorgd voor een aanzienlijke uitbreiding van verzamelings- en bewerkingsmogelijkheden. Databases kunnen relatief eenvoudig worden verbonden en met elkaar vergeleken<sup>3</sup>, waardoor het tot op zekere hoogte mogelijk wordt om de informatie te beheersen. Dankzij de technologie wordt naast een kwantitatieve ook een kwalitatieve toename van informatie gerealiseerd.

Inmiddels wordt vooral in het bedrijfsleven gebruik gemaakt van nieuwe in de technologie ontwikkelde mogelijkheden om uit beschikbare gegevens bruikbare informatie te vergaren. Hierbij kan worden gedacht aan het gebruik van een klantenkaart door de grootste kruidenier van Nederland<sup>4</sup> of aan de – in opspraak geraakte – praktijken van Nederlandse internetproviders bij het verwerken van klantgegevens<sup>5</sup>. Niet alleen de private sector heeft belang bij bruikbare informatie. Ook voor de publieke sector, informatieverzamelaar bij uitstek, is een goede informatiepositie cruciaal. Informatisering kan op uiteenlopende wijzen de mogelijkheden voor het openbaar bestuur bij de vervulling van zijn taken verruimen en vereenvoudigen. Zowel de politieke als de justitie sector willen om die reden in toenemende mate gebruik gaan maken van kennistechnologische onderzoeksmethoden als datamining.

Het centrale thema van dit onderzoek is gegevensoptimalisering door politie en justitie in het kader van de opsporingstaak, een taak waarbij informatie en informatiegaring een prominente plaats innemen. Informatiegaring, of beter gezegd: het proces van informatiegaring, ziet op het opbouwen en in stand houden van een goede informatiepositie door politie en justitie. Bij het vervullen van de opsporingstaak streeft de overheid naar een zo efficiënt mogelijk gebruik van de voorhanden zijnde middelen en informatie teneinde een optimaal resultaat te bereiken. Daarbij is het van belang om te kunnen

---

3. Frissen 1996.

4. Zie ook CBP 1998 (uitspraak betreffende de Albert Heijn Bonus Kaart).

5. Zie ook Artz & Van Eijk 2000.

beschikken over de juiste gegevens (over personen) die kunnen bijdragen aan de strafvordering of de opsporing van strafbare feiten. De met de opsporing belaste instanties zien zich over het algemeen geconfronteerd met een omvangrijke hoeveelheid informatie, verspreid over een groot aantal afzonderlijke gegevensverzamelingen. Door de omvang en fragmentatie van de informatie kan het daadwerkelijke potentieel ervan in de praktijk vaak maar gedeeltelijk worden benut. Nieuwe toepassingen van kennistechnologie kunnen hier uitkomst bieden.<sup>6</sup>

## 1.2 Het sociaal contract

Een van de belangrijkste verworvenheden van de mens is vrijheid, of het fundamentele recht om zelf te kunnen kiezen. Met name de Franse filosoof Jean-Jacques Rousseau heeft hieraan in zijn werk veel aandacht besteed. In zijn theorie van het ‘contrat social’ gaat hij uitvoerig in op de vraag hoe in de relatie tussen de burger en de overheid de vrijheid van de eerste zich dient te verhouden tegenover de autoriteit van de laatste. Volgens Rousseau is de enige reden waarom de mens zijn individuele vrijheid zou willen opgeven het feit dat zijn rechten, geluk en bezit beter kunnen worden beschermd door een formele overheid dan door hemzelf in een maatschappij waarin het recht van de sterkste geldt. Vanuit dat besef is men bereid een deel van zijn vrijheid op te geven in ruil voor bescherming van zijn rechten door een overheid. Op deze manier wordt een wederzijds contract tot stand gebracht tussen die overheid en haar onderdanen. Volgens Rousseau’s theorie dient te allen tijde sprake te zijn van een evenwichtssituatie, waarbij beide partijen bepaalde rechten en plichten tegenover elkaar hebben. De burger geeft weliswaar een deel van zijn soevereiniteit op, maar daartegenover staat dat de overheid de rechten van haar onderdanen dient te beschermen en te respecteren. Wanneer de overheid op die punten in gebreke blijft wordt het contract verbroken; er is dan immers geen sprake meer van een evenwichtssituatie van rechten en verplichtingen.

Maatschappelijke denkbeelden plegen van oudsher hun neerslag te vinden in wetgeving, die daardoor een afspiegeling vormt van het algemene bewustzijn van een samenleving op een bepaald moment. Hoewel Rousseau leefde in de tijd van de Verlichting, hebben zijn ideeën in onze huidige democratische rechtsstaat nog maar weinig aan kracht ingeboet. De grondgedachte van het sociaal contract werkt in onze huidige wetgeving nog steeds door: er is nog steeds sprake van een soort contract tussen overheid en burger. De regelgeving die de macht van de overheid moet reguleren kan worden gevonden in de zogenaamde klassieke grondrechten, welke zijn neergelegd in de artikelen 1 tot en met 18 van de Grondwet. Deze vrijheids- en gelijkheidsrechten dienen onder meer te voorkomen, dat de overheid misbruik maakt van de haar toebedeelde macht. Ook het verbod van analoge of extensieve interpretatie en het rechtszekerheids- en legaliteitsbeginsel kunnen als uitvloeisels van dit streven worden gezien. Deze bepalingen hebben uiteinde-

---

6. Zie ook Prins 2004.

lijk tot doel om, in het licht van de theorie van het sociaal contract, tegenwicht te bieden aan de mogelijkheden van de overheid om te interveniëren in de vrijheid van de burger, zodat een evenwichtssituatie van rechten en verplichtingen tussen burger en overheid bewerkstelligd en gehandhaafd kan worden.

### 1.2.1 *Spanningsveld*

Terugkijkend op de geschiedenis blijkt de drang van overheden om grip te behouden op nieuwe ontwikkelingen in de maatschappij altijd aanwezig te zijn geweest, maar de omstandigheden waaronder dit gebeurt zijn veranderd. De informant die in het belang van de veiligheid van het koninkrijk voor de koning spioneerde, is vervangen door de moderne politieambtenaar, die in het belang van de opsporing en met behulp van de modernste apparatuur omvangrijke digitale informatiestromen verwerkt. De stand der techniek in combinatie met de toegenomen onderlinge compatibiliteit maakt het mogelijk digitale informatie snel en eenvoudig uit te wisselen en met behulp van onder meer dataminningstechnieken te verwerken. In die omstandigheid is het van belang dat de burger weet welke gegevens over hem worden verzameld of vastgelegd en waarvoor. Verwerking van verouderde gegevens en verstrekking aan onbevoegde personen dient te worden voorkomen<sup>7</sup>. Een overheid die daadwerkelijk de bevoegdheid heeft om alle beschikbare gegevens(bestanden) met elkaar te koppelen en naar eigen inzicht te verwerken, roept al snel de associatie op met een Big Brother-samenleving<sup>8</sup> waarin de overheid, in het kader van de opsporingstaak, alles en iedereen in de gaten houdt en onvoldoende afstand bewaart tot de 'civil society'. Dat het technisch mogelijk is om nagenoeg onbeperkt gegevens te verzamelen en deze verder te verwerken betekent niet automatisch dat dit ook vanuit juridisch en maatschappelijk oogpunt mogelijk is of mogelijk dient te zijn. Bij de inzet van het recht als instrument voor de overheid dient het zwaartepunt, wanneer het de opsporing betreft, in beginsel te liggen op het nemen van strafvorderlijke beslissingen en niet op het opbouwen van een goede informatiepositie<sup>9</sup>. Er dient voor te worden gewaakt dat technologische ontwikkelingen, in combinatie met ingrijpende maatschappelijke veranderingen en gebeurtenissen als die van 11 september 2001, vergaande inbreuken op de rechten van de burger al te eenvoudig rechtvaardigen. Eenmaal gedane concessies op dit vlak zijn in een later stadium niet of nauwelijks meer terug te draaien.

In het kader van dit onderzoek wordt nagegaan hoe de verwerking van gegevens in het kader van de opsporing zich verhoudt tot de bescherming van een ieders persoonlijke

---

7. Hier zij ook verwezen naar het gevaar van besluitvorming op basis van virtuele persoonlijkheid, Buruma 2004, p. 665-675.

8. Zie ook Frissen 1996.

9. De MvT bij het wetsvoorstel Wet Politiegegevens geeft aan dat de opbouw van een informatiepositie onder omstandigheden wel aan een gegevensverwerking ten grondslag dient te kunnen liggen (*Kamerstukken II, 2005 /06, 30 327, nr. p. 12*).

levenssfeer. De wet- en regelgeving ter bescherming van persoonsgegevens vindt haar oorsprong in het grondrecht van de burger op eerbiediging van zijn persoonlijke levenssfeer. Hoewel een sterke verbinding bestaat tussen persoonsgegevens enerzijds en de privacy anderzijds, is er wel degelijk sprake van een onderscheid. Enerzijds bestrijken principes ten aanzien van een behoorlijke omgang, als juistheid en vertrouwelijkheid, met persoonsgegevens een breder doel dan privacy alleen. Anderzijds bestrijkt privacy een breder gebied dan persoonsgegevens. Het recht op privacy is moeilijk exact te definiëren; bij een omschrijving van dit begrip wordt vaak verwezen naar noties als het recht om met rust gelaten te worden<sup>10</sup>. Meer actief is de recentere benadering voor het duiden van privacy als: het recht om zelf te bepalen wat er met de toegang tot persoonsgegevens en met die persoonsgegevens gebeurt<sup>11</sup>. 'Bij privacy kunnen verschillende onderdelen onderscheiden worden: de ruimtelijke privacy waartoe het huisrecht behoort, de lichamelijke privacy waartoe de integriteit van lichaam en geest behoort, de relationele privacy op grond waarvan niet alleen verschillende vormen van communicatie, maar bijvoorbeeld ook het familieleven wordt beschermd en ten slotte de informatiele privacy: 'het recht op de bescherming van personen in verband met de informatie die over hen bekend is en ten aanzien van hen wordt toegepast'<sup>12</sup>. De nadruk ligt daarbij op de controle over de eigen gegevens en informatie en de beslissingen die daarop zijn gebaseerd. Een wet die de informatiele privacy reguleert is de Wet bescherming persoonsgegevens (Wbp).<sup>13</sup>

Het privacyrecht impliceert steeds een afweging tegen de rechten en belangen van anderen. Om een goede invulling te kunnen geven aan de normen uit de privacywetgeving gaat het vaak om het bereiken of in stand houden van een situatie waarin niet alleen aan specifieke regels is voldaan, maar waarin ook meer in het algemeen het privacybelang in balans is met andere belangen. Daarbij kunnen maatschappelijke en technologische ontwikkelingen de bestaande balans bedreigen, maar deze bieden tegelijkertijd vaak kansen om een nieuw evenwicht tot stand te brengen<sup>14</sup>. Deze dissertatie is in dit verband in beginsel in het algemeen steeds gericht op de informatiele privacy, het privacyrecht in de betekenis van het recht op niet-inmenging van de overheid in persoonlijke informatie en communicatie, en in het bijzonder op de bescherming van persoonlijke informatie in digitale vorm en de uitwisseling van informatie tussen personen die geheel of gedeeltelijk via digitale weg plaatsvindt<sup>15</sup>. Het belang van de burger kan worden verwoord als 'de behoefte om met rust gelaten te worden'. Om de haar toegewezen opsporingstaak met

---

10. Warren & Brandeis 1980, p. 195.

11. Westin 1967, p. 7.

12. Schreuders 2001, p. 57.

13. Alberdingk Thijm 2002, p. 250-259.

14. CBP 2002, p. 9 en 10.

15. Zie ook Dommering e.a. 2000, p. 50-51. Het betreft hier de informatiele privacy, het gedeelte van het privacyrecht dat ziet op het recht van het individu om de opslag van persoonsgegevens te beperken of te veranderen. Tevens behelst het de verplichtingen en beperkingen die gelden voor de personen en instellingen die deze informatie opslaan.

succes te kunnen volbrengen is de overheid echter gebaat bij een zo ruim mogelijke bevoegdheid om inbreuk te kunnen maken op juist dat recht van de burger. Overheid en burgers hebben – ieder in hun eigen belang – bepaalde concessies gedaan, voortvloeiende uit de grondbeginselen van het sociaal contract dat tussen beide kan worden verondersteld te bestaan. Inherent daaraan is dat de overheid bij de uitvoering van de opsporingstaak slechts binnen strikte, wettelijk vastgestelde kaders mag handelen, en voorts dat de burger zich in die bij wet bepaalde gevallen inbreuken op zijn persoonlijke levenssfeer moet laten welgevalen. Bij een afweging terzake dient een inbreuk op de persoonlijke levenssfeer noodzakelijk te zijn om het van overheidswege gestelde doel te bereiken (noodzakelijkheidsbeginsel). Bovendien dient een dergelijke inbreuk in een redelijke verhouding te staan tot het beoogde doel (proportionaliteitsbeginsel) en dient dat doel niet met minder ingrijpende middelen te kunnen worden bereikt (subsidiariteitsbeginsel).

Het strafprocesrecht is een gebied waarop de tegengestelde belangen van overheid en burger zich duidelijk manifesteren. Het geeft de grenzen aan waarbinnen de overheid zich in het kader van haar opsporingstaak kan en mag bewegen. Inbreuken op de rechten van de burger door de overheid zijn in principe niet toegestaan; de uitzonderingen daarop zijn in het strafprocesrecht vastgelegd. Ter uitvoering van haar opsporingstaak kan de overheid, middels het strafprocesrecht, beschikken over een aantal instrumenten. Inherent aan deze instrumenten is dat de toepassing ervan in beginsel steeds gepaard gaat met een inbreuk op de rechten van de burger, hetgeen in een democratische rechtsstaat niet vanzelfsprekend is. De overheid kan bij het vervullen van haar opsporingstaak inspelen op en gebruik maken van de mogelijkheden die de informatiemaatschappij daartoe biedt. Dit gebruik dient te worden afgewogen tegen de rechten van de burger<sup>16</sup>. Het bewaren van het evenwicht tussen het recht als waarborg voor de burger en het recht als instrument ten dienste van de overheid vereist een grote mate van inspanning en zorgvuldigheid van de kant van de wetgever. Dit geldt bij zowel het handhaven van reeds bestaande wetgeving als bij het tot stand brengen van nieuwe wetgeving. Onduidelijke of tekortschietende wetgeving kan dit evenwicht in gevaar brengen.

### 1.3 Datamining

Dematerialisering en technologische turbulentie zijn twee processen die kenmerkend zijn voor de informatiemaatschappij<sup>17</sup>. Dematerialisering ziet op het verschijnsel dat informatie in toenemende mate wordt vastgelegd in digitale vorm, waardoor deze niet langer is gebonden aan een bepaalde fysieke drager of plaats. Het proces van technologische turbulentie geeft aan dat nieuwe informatietechnieken en -producten elkaar in hoog tempo opvolgen. In het kader van dit onderzoek gaat het daarbij in het bijzonder om de

---

16. Zie ook Koops & Vedder 2001.

17. Ministerie van Justitie 1998 (*Kamerstukken II*, 1997/98, 25 880, nrs. 1-2, p. 51).  
Nota Wetgeving voor de elektronische snelweg, hierna te noemen de Nota WES.

ontwikkeling van de technische mogelijkheden om digitale gegevens steeds efficiënter te verwerken. Beide processen zijn in belangrijke mate verantwoordelijk voor het ontstaan van de ideale omstandigheden voor het uitvoeren van dataminingonderzoek. De huidige technologie maakt het mogelijk om omvangrijke gegevensverzamelingen snel en efficiënt te analyseren. Dit analyseproces staat ook bekend als ‘datamining’ (informatiemijnbouw of informatiewinning). Een andere veelvoorkomende benaming is ‘knowledge discovery<sup>18</sup> in databases’ (KDD). Voor een antwoord op de vraag wat nu precies onder datamining moet worden verstaan wordt verwezen naar onderstaande (kennistechnologische) omschrijvingen van dit verschijnsel in de literatuur.

‘Datamining is the process of discovering meaningful new correlations, patterns and trends by sifting through large amounts of data stored in repositories, using pattern recognition technologies as well as statistical and mathematical techniques’.<sup>19</sup>

‘Datamining is the exploration and analysis, by automatic and semi-automatic means, of large quantities of data in order to discover meaningful patterns and rules’.<sup>20</sup>

‘Datamining is the use of advanced statistical tools to reach into a company’s existing databases to discover patterns and relationships that can be exploited in a business context’.<sup>21</sup>

‘Datamining is a combination of powerful methods that help reducing costs and risks as well as increasing revenues, by extracting information from the available data’.<sup>22</sup>

‘Datamining is the non trivial extraction of implicit, previously unknown, and potentially useful information from data’.<sup>23</sup>

‘Datamining is the non-trivial process of identifying valid, novel, potentially useful, and ultimately understandable patterns in data’.<sup>24</sup>

‘Datamining is het geautomatiseerd doorzoeken van grote gegevensbestanden en het combineren van gegevens die verspreid in bestanden liggen opgeslagen waarna met behulp van speciale programmatuur in deze gegevens vervolgens wordt gezocht naar anomalieën, trends of bepaalde kenmerken’.<sup>25</sup>

---

18. Zie ook Dijkstra & Schuyt 2002, p. 58 e.v.

19. St@tsurf 2000.

20. Berry & Linoff 1997.

21. Trajecta lexicon 2001.

22. Fahmy 2000.

23. Frawley, Piatetsky-Shapiro & Matheus 1991.

24. Fayyad 1996.

‘Datamining is het proces van de analyse en verkenning van grote hoeveelheden data, om daar betekenisvolle patronen in te ontdekken’.<sup>26</sup>

‘Datamining kan worden omschreven als het zoeken naar patronen en verbanden in uw gegevens om uw werk beter te kunnen doen’.<sup>27</sup>

‘Datamining betreft de techniek die wordt gebruikt om gegevens te analyseren en strategische informatie te genereren. Met datamining beoogt men onverwachte, zinvolle verbanden en verborgen patronen te ontdekken in grote databases’.<sup>28</sup>

Uit de voorgaande beschrijvingen kan ten minste worden geconcludeerd, dat het begrip niet eenduidig is gedefinieerd. Wel wordt een aantal kenmerken aangetroffen die stelselmatig met datamining worden geassocieerd:

- er is sprake van een deels of volledig geautomatiseerde analyse;
- de analyse heeft betrekking op één of meer gegevensbestanden;
- de analyse heeft tot doel nieuwe informatie te ontdekken (anomalieën, bepaalde kenmerken of verbanden);
- het resultaat van de analyse kan niet (of slechts met veel grotere inspanning) op een andere wijze worden verkregen.

### *1.3.1 Bewerken en verwerken*

De verscheidene definities van het begrip ‘datamining’ hebben dus een aantal gemeenschappelijke kenmerken, maar wijken op een belangrijk punt van elkaar af: in sommige wordt datamining als een ‘bewerking van gegevens’ bestempeld, in andere als een ‘verwerking van gegevens’. De Commissie Strafvorderlijke gegevensvergaring in de informatiemaatschappij (hierna: de commissie) maakt in haar rapport Gegevensvergaring in strafvordering onderscheid tussen het verwerken en het bewerken van gegevens<sup>29</sup>. Onder ‘verwerken’ verstaat zij hetzelfde als de Wet Bescherming Persoonsgegevens<sup>30</sup> (hierna: Wbp), namelijk elke menselijke dan wel geautomatiseerde handeling ten aanzien van (persoons)gegevens. Een verwerking is iedere handeling – zoals ontvangen, opslaan, vastleggen, vernietigen, bewerken en verstrekken – die na het ontstaan van een gegeven met dat gegeven wordt verricht. Van een bewerking van gegevens is volgens de commissie sprake wanneer uit de analyse, vergelijking of combinatie van verschillende gegevens of

---

25. *Kamerstukken II*, 1997/198, 25 880, nrs. 1-2, p. 30 en 42.

26. Hoeksema 2001.

27. Lopez 2000.

28. Commissie Mevis 2001, p. 20.

29. Commissie Mevis 2001, p. 5.

30. Wet van 6 juli 2000, *Stb.* 2000, 302. De Wbp is per 1 september 2001 in werking getreden (*Stb.* 2001, 337).

verschillende verzamelingen van gegevens een nieuw gegeven wordt verkregen, dat zonder de bewerking niet beschikbaar zou zijn. Dit betekent dat de selectie van een bepaald gegeven uit een verzameling gegevens niet gerekend wordt tot het bewerken van gegevens. Deze interpretatie geldt ongeacht de complexiteit van de zoekvraag. Ook het ontsleutelen van gegevens wordt niet gerekend tot het bewerken van gegevens, omdat een ontsleuteling niet leidt tot het ontstaan van een nieuw gegeven. Met betrekking tot de verhouding tussen KDD en datamining schrijft de commissie in haar rapport:

*‘In het proces van KDD worden drie fasen onderscheiden: datawarehousing<sup>31</sup>, datamining en interpretatie van door datamining verkregen gegevens. Bij datawarehousing wordt een database gebouwd en gevuld die specifiek is ingericht op het analyseren van gegevens. De techniek die vervolgens wordt gebruikt om gegevens te analyseren en strategische informatie te genereren wordt aangeduid met de term datamining. Met datamining beoogt men onverwachte, zinvolle verbanden en verborgen patronen te ontdekken in grote databases<sup>32</sup>.*

De commissie gaat ervan uit dat datamining een bewerkingsmethode is die onderdeel uitmaakt van het proces van KDD. Dit geheel aan handelingen, inclusief de bewerking, kan gerangschikt worden onder de noemer ‘het verwerken van gegevens’. In het kader van dit onderzoek is deze gehele range van handelingen van belang. Voor een toetsing aan de huidige wet- en regelgeving en het uitwerken van een juridisch kader wordt onderscheid gemaakt tussen bewerken en verwerken, waarbij het bewerken binnen dit onderzoek als geheel slechts onderdeel uitmaakt van de meeromvattende ‘verwerking van gegevens in het kader van de opsporing’.

### 1.3.2 Het dataminingsproces

Bij onderzoek naar de juridische mogelijkheden voor het gebruik van dataminingstechnologie verdient het hanteren van de term ‘KDD’ de voorkeur boven die van ‘datamining’. KDD duidt namelijk het gehele proces van het ontdekken van bruikbare kennis in informatie.<sup>33</sup> Naast stappen als het verzamelen, het opschonen en het opslaan van gegevens (verwerking), wordt datamining beschouwd als een afzonderlijke stap in dat proces

31. Borking, Artz & Almelo 1998. Het CBP definieert een datawarehouse als een informatiepakhuis. Datawarehousing is het verzamelen en massaal opslaan van gegevens ten behoeve van analyse, informatiewinning en kennisvergaring. De universiteit van Stanford hanteert de volgende definitie van een datawarehouse: ‘A Data Warehouse is a repository of integrated information, available for queries and analysis. Data and information are extracted from heterogeneous sources as they are generated. This makes it much easier and more efficient to run queries over data that originally came from different sources’ (Warehouse 2000).

32. Commissie Mevis 2001, p. 20.

33. Aldus ook Fayyad, Piatetsky-Shapiro & Smyth 1996a, p. 37-54 en Fayyad, Piatetsky-Shapiro & Smyth 1996b, p. 28.

(bewerking). Om te voorkomen dat de term KDD wordt gebruikt als synoniem voor datamining wordt in dit onderzoek gesproken over ‘het proces van datamining’. Dit dataminingsproces behelst, naast het bewerken van gegevens, ook de stadia daarvoor en daarna. Binnen het dataminingsproces wordt de eigenlijke bewerking van gegevens aangeduid met de term ‘datamining’. Aangezien het dataminingsproces niet zozeer valt aan te merken als één bepaald instrument of één bepaalde methode, kan het worden beschouwd als een proces waaraan op verschillende manieren uitvoering kan worden gegeven. Het dataminingsproces is een – relatief nieuw en complex – proces van analyse en verkenning van (grote hoeveelheden) gegevens, teneinde daarin betekenisvolle patronen en trends te ontdekken. Bestanden van (persoons)gegevens, verbonden en toegankelijk via digitale weg, bieden nieuwe mogelijkheden bij het zoeken naar en het combineren van gegevens. Door samenvoeging en bewerking van verschillende gegevens krijgen deze een meerwaarde. Er ontstaat kennis die in potentie reeds aanwezig is, maar eerst met behulp van dataminingonderzoek zichtbaar wordt gemaakt. Wegens het ontbreken van een standaardmodel voor de toepassing van het dataminingsproces wordt het begrip in beginsel omschrijvend en breed gedefinieerd:

- *Het dataminingsproces* betreft ten minste het selecteren, verzamelen, opschonen en vastleggen van gegevens teneinde deze vervolgens te bewerken met als doel het ontdekken van informatie/kennis die zonder deze bewerking niet zichtbaar/voorhanden is (of slechts met veel grotere inspanning kan worden verkregen).
- *Datamining*: het in het kader van het dataminingsproces bewerken van gegevens(bestanden), ter verkrijging van informatie/kennis die zonder deze bewerking niet zichtbaar/voorhanden is (of slechts met veel grotere inspanning kan worden verkregen).<sup>34</sup>

### 1.3.3 De fasen van het dataminingsproces

Vanwege het complexe karakter van het dataminingsproces is opdeling in een aantal stappen wenselijk. Dit biedt meer houvast en werkt verhelderend bij het overbrengen van dit technologisch ingewikkelde proces in een juridisch kader. Afhankelijk van het doel van het onderzoek zijn daarvoor verschillende modellen denkbaar. Eén mogelijkheid is een onderverdeling in de onderstaande vijf stappen<sup>35</sup>.

1. *Opstartfase*: bepalen van de doelstelling van het dataminingonderzoek.
2. *Gegevensoriëntatie*: verzamelen van de te gebruiken gegevens.

---

34. Wanneer in dit onderzoek over datamining wordt gesproken, gaat het om datamining als onderdeel (bewerking) van het meeromvattende dataminingsproces.

35. Dit model is grotendeels ontleend aan Meij 2004 (Data Mining Projectplan van Stichting Toekomstbeeld der Techniek project (STT)).

3. *Gegevenspreparatie*: prepareren van de geselecteerde gegevens voor de daadwerkelijke analyse. De gegevens dienen te worden opgeschoond om ontbrekende waarden en fouten te vermijden.
4. *Modelleringsfase*: het eigenlijke ‘mining’, waarbij een bepaald algoritme<sup>36</sup> op de gegevens wordt toegepast.
5. *Evaluatiefase*: evalueren van het gevonden resultaat. Belangrijk is dat hiervoor een juiste strategie wordt bepaald, zodat de informatie bij de juiste personen of instanties terecht komt.

Zoals opgemerkt is de te kiezen onderverdeling mede afhankelijk van het doel waarvoor deze wordt gebruikt. In dit onderzoek is dat doel het scheppen van een juridisch kader voor het gebruik van het dataminingsproces bij de strafvorderlijke opsporing. Daarbij past een model<sup>37</sup> dat enigszins afwijkt van het bovenstaande. Hoewel alle in dat model genoemde onderdelen ook in het onderstaande model<sup>38</sup> zijn opgenomen, bestaat het slechts uit drie fasen. De drie fasen als geheel vormen de verwerking, terwijl fase twee de bewerking betreft.

1. *Het datawarehousing*: verzamelen, verrijken, opschonen en coderen van de gegevens die bij het dataminingsonderzoek zullen worden gebruikt (een combinatie van de stappen 1, 2 en 3 in het vorige schema). Hiertoe worden de gegevens in beginsel opgeslagen in een zogenaamd datawarehouse.
2. *Het eigenlijke datamining*: de bewerking van de gegevens die in het datawarehouse zijn opgeslagen (stap 4 in het voorgaande model).
3. *De interpretatie van het resultaat*: de verwerking van het resultaat van het dataminingsonderzoek. Aan de orde komen vragen zoals de manier waarop het resultaat dient te worden opgeslagen, welke conclusies op basis van de uit de analyse voortgekomen informatie kunnen worden getrokken en wie het resultaat vervolgens mag gebruiken (stap 5 uit het voorgaande model).

#### 1.3.4 Toepassing van het dataminingsproces

De toepassingsmogelijkheden en het nut van het dataminingsproces voor de opsporingspraktijk worden in het navolgende verduidelijkt aan de hand van vier eenvoudige voorbeelden. Aan de hand van praktijksituaties wordt geschetst hoe datamining tot resultaten kan leiden die zonder toepassing van deze wijze van onderzoek niet of in zeer beperkte mate verkregen zouden zijn.

---

36. Een algoritme is een in formules uitdrukbaar systeem van voorschriften met behulp waarvan logische en/of rekenkundige bewerkingen worden uitgevoerd. In de computercontext is een algoritme een deel van een programma.

37. Zie ook Verbeek, De Roos & Van den Herik, 2000, p. 32.

38. Commissie Mevis 2001, p. 20.

### **Uitkeringsfraude I**

Eén van de meest eenvoudige toepassingen van datamining is die van de registervergelijking, waarbij twee of meer registers of gegevensverzamelingen worden gekoppeld en vergeleken. Zo kan een door de belastingdienst bijgehouden register A worden vergeleken met register B dat informatie bevat over personen in Nederland die een uitkering ontvangen. Door te onderzoeken of in beide registers namen van personen voorkomen die loonbelasting betalen en tegelijkertijd een uitkering ontvangen is het mogelijk, eventuele gevallen van uitkeringsfraude op te sporen.

### **Uitkeringsfraude II**

Een complexere toepassing van registerkoppeling is gelegen in het volgende voorbeeld. Register A bevat gegevens over personen in Nederland die een uitkering ontvangen. Register B is een politieregister, waarin onder meer uitgeschreven bekeuringen worden bijgehouden. Stel dat uit register B blijkt dat een zekere mijnheer X de afgelopen maand een aantal malen in dezelfde straat is bekeurd wegens fout parkeren; bij nadere bestudering van het proces-verbaal blijkt dat in die straat alleen bedrijven zijn gevestigd. Wanneer bij combinatie met register A blijkt dat mijnheer X een uitkering geniet kan dit aanleiding vormen tot het instellen van een nader onderzoek naar de handel en wandel van mijnheer X: de hoge aanwezigheidsfrequentie van mijnheer X in een straat waar zich alleen bedrijfspanden bevinden kan erop wijzen dat hij daar zwart werkt. Deze toepassing van datamining is dermate ingrijpend van aard, dat het de vraag oproept of gegevensverzamelingen die qua doelstelling zo sterk van elkaar afwijken wel gecombineerd mogen worden. Bovendien kan men zich afvragen of het doel van het onderzoek, namelijk de opsporing van uitkeringsfraude in combinatie met de beschreven zoekstrategieën, een dergelijke inbreuk op de persoonlijke levenssfeer rechtvaardigt.

### **Analyse telefoonverkeer**

Het derde voorbeeld stamt uit het onderzoek naar de vuurwerkramp in Enschede. Het bewijs dat tot een aanhouding in deze zaak leidde werd onder meer verkregen door een analyse van het mobiele telefoonverkeer. Hieruit bleek dat een verdachte op de bewuste middag vanaf het bedrijventerrein van de vuurwerfabriek mobiel had gebeld. Dit vormde een belangrijke aanwijzing dat de verdachte inderdaad op de plaats delict aanwezig was geweest.

Omdat mobiele telefoons voortdurend contact houden met de dichtstbijzijnde centrale kan vrij nauwkeurig worden bepaald waar die telefoon, en daarmee vaak ook de eigenaar ervan, zich bevindt. Nieuwe generaties mobiele telefoons maken zelfs een nog veel nauwkeuriger plaatsbepaling mogelijk. Voor de opsporingspraktijk schept dit, gezien de hoge gebruiksfrequentie van dit communicatiemedium, nieuwe kansen. Analyse van telefoonverkeer met behulp van datamining kan naar twee zijden werken. Aan de ene kant kan de verdachte worden gevonden door analyse van telefoongegevens. In een geval als de vuurwerkramp kunnen alle telefoongegevens van de dag van de ramp worden

onderzocht op gesprekken die eventueel vanaf het bedrijfsterrein zijn gevoerd. Daarmee wordt iedereen die op de bewuste dag in de omgeving met een mobiele telefoon heeft gebeld onderwerp van onderzoek. Aan de andere kant is het ook mogelijk dat er reeds sprake is van een verdachte en dat de telefoongegevens bij nader onderzoek als ondersteunend bewijs gebruikt worden. In dat geval kan gericht in de voorhanden zijnde telefoongegevens van die dag worden gezocht. In theorie heeft de politieactiviteit dan alleen betrekking op de persoon van de verdachte<sup>39</sup>.

### **Rasterfahndung**

Het laatste voorbeeld, de Rasterfahndung<sup>40</sup>, betreft een zeer uitgebreide vorm van koppeling van allerhande gegevensverzamelingen die voor het determineren van bepaalde patronen met elkaar worden vergeleken.<sup>41</sup> Rasterfahndung is vooral bekend geworden door het gebruik van die methode door de Duitse politie en veiligheidsdiensten bij de opsporing van terroristen in de jaren zeventig. Bij het onderzoek naar de Rote Armee Fraktion (RAF) onderzocht men gegevensverzamelingen van uiteenlopende instanties onder het motto ‘wir wissen nicht, was wir nicht wissen’. De Rasterfahndung werd toegepast aan de hand van een aantal veronderstellingen. De Duitse opsporingsinstanties vermoedden dat de terroristen hun water- en elektriciteitsrekeningen contant betaalden, dat zij tussen de twintig en veertig jaar waren, bepaalde typen woningen huurden en gebruik maakten van gestolen auto's, bij voorkeur van het merk Porsche en BMW. Op basis van dit profiel werden talloze publieke en private gegevensverzamelingen onderzocht om personen op het spoor te komen die aan één of meer van deze kenmerken voldeden. Toen de gevonden resultaten aan elkaar en aan andere gegevens werden gekoppeld en met elkaar vergeleken, bleek dit voor opsporingsinstanties belangrijke kennis op te leveren. Vanwege de teruglopende resultaten en de afnemende bereidheid onder de bevolking om mee te werken aan deze vergaande (inbreukmakende) methode, geraakte de Rasterfahndung aan het eind van de jaren zeventig echter steeds meer in onbruik<sup>42</sup>.

## **1.4 Onderzoeksvragen**

Gegevensverwerking is voor de (justitiële) politietaak van essentieel belang. Hiermee verschaft de politie zich aanknopingspunten voor de opsporing van daders en delicten. Informatiegaring richt zich in toenemende mate op elektronische gegevensverzamelingen, hetgeen de mogelijkheid biedt informatie sneller en efficiënter te verwerken dan tot voor kort het geval was. In dit verband zij ook gewezen op het concept van ‘informatie-

---

39. In het eerste geval kan worden gesproken van gericht dataminingonderzoek en in het tweede van verificatie (hoofdstuk 2).

40. Zie ook Wuchold 2001.

41. Wellicht kan de figuur van Rasterfahndung in de nabije toekomst worden toegepast in het kader van het verkennend onderzoek. *Kamerstukken II, 2005/06*, 30 164, nr. 7, p. 26.

42. Gardeniers, Van Kralingen & Schreuders 1996.

gestuurde opsporing', kortweg IGO<sup>43</sup>. Het gaat hierbij meer om een manier van denken over politiewerk dan om een specifieke technologie. De essentie ervan is dat grondige informaticanalyse richtinggevend moet zijn voor opsporingsoperaties. De belangrijkste beleidsmatige vraag op dit terrein is welke koppelingen kunnen worden toegestaan en wat nu precies mag worden gedaan met informatiebestanden.<sup>44</sup> Hiermee zijn wij weer aangekomen bij de balans tussen veiligheid en privacy bij de toepassing van het dataminingsproces. De aard van de te verwerken gegevens speelt een cruciale rol bij de vraag naar de toepassingsmogelijkheden van dit proces. Dataminings technieken worden al veelvuldig toegepast in de private sector. Met behulp van de informatie die daarmee wordt verkregen, is het bedrijfsleven in staat in te spelen en te anticiperen op de vraag van de markt en zodoende haar concurrentiepositie te verbeteren. Het dataminingsproces heeft hierbij tot doel informatie te verkrijgen over groepen van niet-direct te individualiseren personen. Voor het ontdekken van patronen en het opstellen van groepsprofielen zijn persoonsgegevens, strikt genomen, niet noodzakelijk. Toepassing van het dataminingsproces waarbij het privacyvraagstuk niet prominent aanwezig is, vormt mede de verklaring van het feit dat het dataminingsonderzoek tot op heden voornamelijk door de private sector wordt aangegrepen. Maar ook de overheid erkent het belang om gebruik te (kunnen) maken van dataminings technieken. Vanwege het relatief nieuwe en technische karakter van uitvoerige gegevensverwerking met behulp van het dataminingsproces lijkt de wetgeving op het moment van dit schrijven nog niet (afdoende) te voorzien in de regulering ervan. Ten aanzien van de toelaatbaarheid van het onderling verbinden van computersystemen, databases en computernetwerken in combinatie met geavanceerde dataminings technieken ontbreekt het aan het benodigde juridische in- en doorzicht. Hoewel de wettelijke mogelijkheden betreffende strafvorderlijke gegevensvergaring onder de loep worden genomen<sup>45</sup>, mist tot op heden<sup>46</sup> een duidelijk wettelijk kader voor de (verdere) verwerking van gegevens. De Wet Politierregisters (WPoI)<sup>47</sup> en het Besluit Politierregisters (BPoI)<sup>48</sup> besteden thans nog (te) weinig aandacht aan dataminings technieken<sup>49</sup> en lopen achter waar het gaat om de privacyrechtelijke aspecten van gegevensverwerking.

---

43. Stuurgroep IGO 2001 en Klerks e.a. 2002.

44. Stol 2004, p. 48.

45. Commissie Mevis 2001.

46. Hier zij gewezen op het wetsvoorstel Wet politiegegevens, ter vervanging van de huidige WPoI (*Kamerstukken II*, 2005/06, 30 327, nr. 2. In hoofdstuk 13 van dit onderzoek wordt nader op dit wetsvoorstel ingegaan.

47. Wet van 21 juni 1990, houdende regels ter bescherming van de persoonlijke levenssfeer in verband met politierregisters, zoals laatstelijk gewijzigd bij Wet van 10 juni 2004, *Stb.* 320.

48. Besluit van 14 februari 1991, houdende bepalingen ter uitvoering van de Wet Politierregisters, zoals laatstelijk gewijzigd bij besluit van 9 september 2004, *Stb.* 454.

49. Aldus ook Verbeek e.a. 1999.

Vanuit het besef dat het dataminingsproces voor de publieke sector, meer specifiek in het kader van de opsporingstaak, een belangrijke functie kan vervullen is een dergelijk kader voor de toepassing daarvan voor strafvorderlijke doeleinden noodzakelijk. Het strafvorderlijk gebruik dient met de nodige waarborgen te worden omkleed teneinde een te vergaande inbreuk op de rechten van de burger, in dit geval in het bijzonder het privacyrecht, te voorkomen en de toepassing ervan door de overheid in een democratische rechtsstaat te kunnen legitimeren. In tegenstelling tot de toepassing van dataminings technieken in de private sector is het in het kader van de opsporingstaak onvermijdelijk, dat in enig stadium gebruik wordt gemaakt van gegevens die herleidbaar zijn tot individuele personen. Het gaat in beginsel steeds om gegevens die betrekking hebben op personen of gebeurtenissen die van nut (kunnen) zijn voor de opsporing. Daarbij zullen opsporingsautoriteiten geneigd zijn een zo ruim mogelijke uitleg te geven aan 'het van nut zijn voor de opsporing'.<sup>50</sup> Het belang dat de overheid heeft bij het gebruik van een proces als dataminings dient te worden afgewogen tegen de inbreuk op de persoonlijke levenssfeer die dat voor de burger met zich meebrengt<sup>51</sup>. Hierbij dient de juiste balans te worden gevonden in het spanningsveld tussen het recht als instrument voor de overheid en het recht als bescherming voor de burger tegen al te vergaande inbreuken op zijn rechten door diezelfde overheid<sup>52</sup>. Daarom is privacyrechtelijk en strafvorderlijk onderzoek gewenst, waarbij de juridische en praktische mogelijkheden van het dataminingsproces tegen elkaar moeten worden afgewogen. Zo moet worden gekomen tot een wettelijke inkadering van de gegevensverwerking in het kader van de opsporingstaak met behulp van het dataminingsproces, die de nodige waarborgen biedt. Het voorgaande leidt tot de volgende twee onderzoeksvragen.

- 
50. In de zin van: 'Hoe meer gegevens (input), des te groter de kans op interessante uitkomsten (output)'. De kennistechnologische literatuur leert echter, dat dit niet altijd het geval behoeft te zijn (zie ook Van der Pol 2000).
51. Ministerie van Binnenlandse Zaken en Koninkrijksrelaties 2000 (*Kamerstukken II*, 1999 /00, 26 387, nr. 8) Nota 'Contract met de toekomst'. Er zijn ook andere redenen om opsporingsmethoden te normeren, welke kunnen worden samengevat onder de noemer van het belang van de integriteit van de strafrechtspleging. Daarbij valt bovenal te denken aan de wens om de verantwoordelijkheden voor het gebruik van bepaalde bevoegdheden daar te leggen waar zij horen, de kans op misbruik van bepaalde methoden te verkleinen en in verband daarmee het gevaar van corruptie van de politie tegen te gaan (*Kamerstukken II*, 1995 /96, 24 072, nr. 14, p. 16).
52. Zie ook de aanbeveling van het comité van Ministers van de Raad van Europa betreffende het gebruik van persoonlijke gegevens in de politiesector (*Recommendation* No. R (87) 15). 'Considering that the aim of the Council of Europe is to achieve a greater unity between its members; Aware of the increasing use of automatically processed personal data in the police sector and of the possible benefits obtained through the use of computers and other technical means in this field; Taking account also of concern about the possible threat to the privacy of the individual arising through the misuse of automated processing methods; Recognising the need to balance the interests of society in the prevention and suppression of criminal offences and the maintenance of public order on the one hand and the interests of the individual and his right to privacy on the other.'

- *Wat is het strafvorderlijke en privacyrechtelijke kader voor de toepassing van dataminingsonderzoek door de Nederlandse overheid ten behoeve van de opsporingstaak?*
- *Op welke wijze kan (en mag) de Nederlandse overheid gebruik maken van het proces van datamining ten behoeve van de opsporingstaak?*

Het doel van dit onderzoek is om vast te stellen wat de privacyrechtelijke en strafvorderlijke grenzen zijn die (dienen te) worden gesteld aan het gebruik van het dataminingsproces door opsporingsinstanties in het kader van de opsporingstaak. Om te bepalen op welke wijze het dataminingsproces kan worden gebruikt ten behoeve van de (gegevensverwerking in het kader van de) opsporing, wordt onderzocht wat de betekenis is van de bestaande wet- en regelgeving voor het dataminingsproces, alsmede op welke punten die wet- en regelgeving eventueel moet worden herzien. Hierbij zal steeds worden uitgegaan van de huidige juridische inzichten en de lijn die blijkt uit literatuur en praktijk.

### **1.5 Afbakening van het onderzoeksdomein**

Ter verduidelijking van de manier waarop in dit onderzoek naar een beantwoording van de onderzoeksvragen wordt toegewerkt, volgt onderstaand een korte toelichting op de wijze waarop het onderzoeksdomein is afgebakend.

#### **Nationale benadering**

De nadruk ligt in dit onderzoek op de toepassing van het dataminingsproces ten behoeve van de opsporingstaak binnen Nederland. Het zou te ver voeren om uitvoerig in te gaan op de toepassing van datamining op internationaal niveau.<sup>53</sup> Nu, en voor zover, het nationaal juridisch kader voor de toepassing van het dataminingsproces mede wordt gevormd door internationale opvattingen en regelingen, zullen deze aan bod komen. Dit is onder meer het geval voor het privacyrechtelijke kader.

#### **Specificatie bewerkingsmethoden**

De term 'datamining' wordt gebruikt ter aanduiding van een breed scala aan bewerkingsmethoden om uit grote hoeveelheden gegevens nieuwe kennis te kunnen destilleren. Om welke bewerkingsmethode het daarbij precies gaat, is afhankelijk van verschillende factoren, zoals de aard van de instantie die het dataminingsproces toepast en het doel dat met het onderzoek wordt beoogd. Voor een juridische beschouwing van het dataminingsproces is niet direct van belang op welke wijze in technische zin uitvoering wordt gegeven aan dit proces. Uitputtend ingaan op die technische details zou in het kader van dit onderzoek te ver voeren. Alleen daar waar de (technische) aard van de gebruikte bewer-

---

53. Vgl. Verbeek e.a. 1999.

kingsmethode ook vanuit juridisch oogpunt van belang is, zal dat aspect in de beschouwingen worden betrokken.

### Fenomeenonderzoek

In het kader van het dataminingsproces kan ook het zogenaamde ‘fenomeenonderzoek’<sup>54</sup> worden genoemd. Fenomeenonderzoek behelst het doorlichten van een geografisch gebied of bevolkingsgroep, een misdaadveld of criminele markt en/of een sector of verschijnsel in de samenleving.<sup>55</sup> Bij fenomeenonderzoek gaat het om het opstellen van profielschetsen voor het verkrijgen van informatie over groepen van personen. Daarbij zijn diegenen die aan een bepaalde profielschets hebben bijgedragen niet interessant als afzonderlijke individuen. Het privacyvraagstuk speelt hier geen rol van betekenis; er is namelijk in beginsel geen sprake van individualiseerbaarheid van de verwerkte gegevens. Dit is een essentieel verschil met het gebruik van het dataminingsproces ten behoeve van de opsporingstaak, waarbij een overgang plaatsvindt van generalis naar specialis, van groep naar individu. Vanwege de noodzaak tot individualiseerbaarheid van de verwerkte gegevens is het privacyvraagstuk hier juist wel van belang. Met het oog op het individuele karakter van het strafrecht zal namelijk op enig moment een herleiding tot een individu mogelijk moeten zijn, aangezien strafrechtelijk optreden in beginsel is uitgesloten wanneer het eindresultaat van het onderzoek bestaat uit een profiel van niet individualiseerbare personen. Wanneer het dataminingsproces wordt toegepast in het kader van de opsporingstaak, is het einddoel niet het opstellen van een profiel, maar het komen tot een specialis; het vergaren van gegevens met behulp van dataminings technieken die als generalis kunnen worden aangemerkt vormt daarbij een tussenstap.

Het opstellen van een profielschets zoals dat bij fenomeenonderzoek plaatsvindt, wordt hier om twee redenen niet als een dergelijke tussenstap aangemerkt. Ten eerste zou het, wanneer het een anonieme profielschets (generalis) betreft, onmogelijk zijn om in een later stadium nog te geraken tot een individualiseerbare specialis. Ten tweede zullen de uitkomsten van een dataminingsonderzoek, uitgevoerd in het kader van de opsporingstaak, mogelijk aanleiding vormen voor een vervolgonderzoek. Een eventueel gevonden profiel is dan slechts een tussenresultaat. Bij fenomeenonderzoek is een gevonden profiel het eindresultaat. De bij een fenomeenonderzoek onderzochte informatie heeft geen directe strafrechtelijke impact<sup>56</sup>. Dergelijk meer op het vlak van sociologie of

54. *Kamerstukken II*, 1995/196, 24 072, nrs. 10-11. Met de introductie van het verkennend onderzoek in het juridisch instrumentarium is de betekenis van het begrip fenomeenonderzoek ingeperkt. Bij fenomeenonderzoek gaat het om niet-strafvorderlijk onderzoek, met als mogelijk doel criminaliteitspatronen in beeld te krijgen.

55. *Kamerstukken II*, 1995/196, 24 072, nr. 10-11.

56. *Kamerstukken II*, 1996/197, 25 403, nr. 3, p. 125.

wetenschap liggend onderzoek behoort niet primair tot de taak van de politie en wordt in dit onderzoek dan ook buiten beschouwing gelaten<sup>57</sup>.

### **1.6 Plan van aanpak**

Ter beantwoording van de vraag op welke wijze politie en justitie gebruik kunnen maken van het dataminingsproces, zullen de verschillende stappen van dat proces nader worden belicht. Daarbij worden de mogelijkheden die het dataminingsproces politie en justitie biedt bij het vervullen van de opsporingstaak afgezet tegen de juridische grenzen die in een rechtsstaat aan de opsporing dienen te worden gesteld.

Om de plaats van het dataminingsproces binnen de opsporing te bepalen wordt in hoofdstuk 2 het proces van de politieke informatiegaring behandeld. Met betrekking tot dat proces kan een onderscheid worden gemaakt in drie verschillende juridische stadia: het opsporingsonderzoek, het verkennend onderzoek en het stadium waarin sprake is van het opbouwen en in stand houden van een zekere informatiepositie door het opslaan van gegevens. Dit laatste kan worden gerealiseerd door het bewerken, gebruiken en analyseren van gegevens, dan wel door het vergaren van gegevens door de toepassing van niet-ingrijpende middelen.

In hoofdstuk 3 wordt de relatie tussen het dataminingsproces en het proces van informatiegaring nader onderzocht. Daarbij wordt het proces van informatiegaring bekeken aan de hand van een onderverdeling in twee technische stadia: datawarehousing en informatie-inwinning. Voorts wordt aangegeven welke drie vormen van dataminingsonderzoek binnen het dataminingsproces mogelijk zijn. Door een terugkoppeling van de drie stadia van het proces van informatiegaring naar het dataminingsproces (en de varianten daarvan) kan worden vastgesteld hoe het dataminingsproces zich verhoudt tot het proces van informatiegaring. Tevens wordt ingegaan op de overgang van dataminingsproces naar onderzoeksmethode.

Het vierde hoofdstuk geeft een overzicht van de wet- en regelgeving die, direct dan wel indirect, verband houdt met het politieke dataminingsproces. Naast de algemene privacywetgeving zijn met name de WPolr en het bijbehorende BPolr<sup>58</sup> daarbij van belang. Middels een analyse van de wet- en regelgeving die in dit hoofdstuk wordt besproken, kan

---

57. *Handboek voor de opsporingspraktijk 2000*, 1.2 Verkennend onderzoek, sectie 1.1.2-4, Fenomeenonderzoek. Op grond van art. 15 BPolr kunnen gegevens uit politieregisters worden aangewend in een niet door opsporingsambtenaren uitgevoerd fenomeenonderzoek. Het betreft dan evenwel geen verkennend onderzoek in de zin van art. 126gg Sv. Dat wordt immers noodzakelijkerwijs uitgeoefend door opsporingsambtenaren; zie sectie 2.4.

58. De WPolr spreekt niet van het BPolr maar van de AMvB.

zicht worden verkregen op de invloed van het bestaande wettelijke kader voor het dataminingsproces, inclusief de pluspunten daarvan alsook de mogelijke tekortkomingen.

In het vijfde hoofdstuk staat het datawarehouse centraal. Onderzocht wordt in hoeverre er sprake is van een datawarehouse en op welke wijze hiermee bij de toepassing van dataminingsonderzoek in het kader van de opsporingstaak rekening dient te worden gehouden.

De koppeling van gegevens komt in het zesde hoofdstuk aan bod. Hier wordt vastgesteld welke (juridische) betekenis aan het begrip ‘koppeling’ dient te worden gegeven en hoe die uitleg zich verhoudt tot de koppeling zoals de WPolr die kent. Voorts zal worden nagegaan of de koppelingsregeling in de WPolr nog volstaat om te voorzien in de huidige mogelijkheden om gegevens te verwerken.

In de eerste zes hoofdstukken zijn de juridische vragen die het dataminingsproces oproept, getoetst aan de bestaande wettelijke kaders. Aan de hand van de uitkomsten daarvan kan worden vastgesteld op welke wijze de bestaande wet- en regelgeving reeds voorziet in het politieële gebruik van het dataminingsproces en welke grenzen op grond daarvan aan het gebruik van dat proces gesteld dienen te worden. Met behulp van het op deze wijze verkregen juridische kader zal in de navolgende hoofdstukken een praktische toetsing plaatsvinden, waarbij voor de meest gangbare politieregisters wordt onderzocht op welke wijze een verbetering van de informatiepositie van deze registers kan worden nagestreefd met behulp van dataminingsonderzoek. Hierbij wordt onder meer gekeken naar de punten waarop de huidige wet- en regelgeving mogelijk tekortschiet.

In hoofdstuk 7 wordt onderzocht in hoeverre met behulp van (ongericht) dataminingsonderzoek een verbetering van de informatiepositie van gewone politieregisters kan worden nagestreefd.

Vervolgens wordt in hoofdstuk 8 stilgestaan bij een dergelijke verbetering van de informatiepositie van het register, dat door het Meldpunt ongebruikelijke transacties wordt bijgehouden.

Hoofdstuk 9 behandelt een mogelijke verbetering van de informatiepositie van de bijzondere politieregisters met behulp van (ongericht) dataminingsonderzoek.

Hoofdstuk 10 behandelt de toepassing van de gerichte dataminingsvariant in het kader van de politietaak.

In hoofdstuk 11 worden, aan de hand van de bevindingen uit de voorgaande hoofdstukken, de onderzoeksvragen beantwoord die in sectie 1.4 zijn geformuleerd. Zo kan worden vastgesteld of en op welke wijze het dataminingsproces kan worden ingezet in het kader van de opsporingstaak. Ook wordt aangegeven in hoeverre een herziening van de

bestaande Nederlandse wet- en regelgeving hiervoor noodzakelijk is, waar nodig vergezeld van aanbevelingen. Hoofdstuk 12 bevat de eindconclusies en aanbevelingen.

Dit onderzoek behelst de (juridische) ontwikkelingen die samenhangen met de toepassing van het dataminingsproces in het kader van de opsporing. Tijdens de afronding van dit onderzoek verscheen het wetsvoorstel Wet Politiegegevens. De Wet Politiegegevens dient ter vervanging van de WPolr en het BPolr. In hoofdstuk 13 wordt in de vorm van een naschrift nader op de merites van dit wetsvoorstel ingegaan. Daarbij worden de uitkomsten van dit onderzoek getoetst aan de wijze waarop de wetgever voornemens is de verwerking van politiegegevens middels de genoemde Wet Politiegegevens te regelen.

---

## 2 Het proces van informatiegaring

Ter beantwoording van de vraag in hoeverre en op welke wijze politie en justitie ten behoeve van de opsporingstaak gebruik kunnen en mogen maken van het dataminingsproces dient eerst duidelijk te zijn wat de begrippen ‘opsporing’ en ‘dataminingsproces’ precies behelzen.<sup>1</sup> In dit hoofdstuk wordt daartoe het proces van de politieke informatiegaring, beter bekend als ‘de opsporing’, behandeld<sup>2</sup>.

### 2.1 De opsporingstaak

Art. 2 Politiewet 1993<sup>3</sup> en art. 141 Wetboek van Strafvordering (Sv)<sup>4</sup> maken duidelijk dat de opsporingstaak van de overheid berust bij politie en justitie. Volgens art. 2 Politiewet 1993 heeft de politie tot taak om, 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 handhaving van de rechtsorde is een tweeledige taak, die uiteenvalt in de handhaving van de openbare orde en de strafrechtelijke handhaving van de rechtsorde. Onder de strafrechtelijke handhaving van de rechtsorde wordt verstaan: de daadwerkelijke 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 (OM) in strafzaken. Daaronder vallen alle taken die de politie onder de verantwoordelijkheid van het OM, en daarmee van de Minister van Justitie (MvJ), in verband met strafbare feiten of mogelijke strafbare feiten verricht<sup>5</sup>. Voor de politie gaat het daarbij om de daadwerkelijke voorkoming, opsporing en beëindiging van strafbare feiten. Art. 13 Politiewet bepaalt dat de politie onder het gezag van het OM staat indien zij optreedt ter strafrechtelijke handhaving van de rechtsorde, dan wel taken verricht ten dienste van justitie. In de praktijk heeft het OM vaak geen directe bemoeienis met de opsporing, hoewel dit wel mogelijk is op grond van art. 13 Politiewet 1993 en art. 148 Sv.

- 
1. Uiteraard geldt dit onverkort voor de beantwoording van onderzoeksvraag twee.
  2. Sietsma e.a. 2002.
  3. Wet van 9 december 1993 tot vaststelling van een nieuwe Politiewet *Stb.* 2004, 414 (Politiewet 1993).
  4. Hierin wordt onder meer bepaald dat met de opsporing van strafbare feiten zijn belast de ambtenaren van politie zoals bedoeld in art. 3, lid 1, sub *a* en *c* en lid 2 van de Politiewet 1993.
  5. Corstens 2002, p. 96-97.

## 2.2 De Parlementaire Enquêtecommissie

De IRT-affaire deed in 1996 veel stof opwaaien. Naar aanleiding van die affaire kreeg de parlementaire enquêtecommissie (PEC), onder voorzitterschap van het Tweede-Kamerlid Van Traa, de opdracht om onderzoek te doen naar de georganiseerde criminaliteit, de toepassing van opsporingsmethoden en het functioneren van de ambtelijke organisatie.<sup>6</sup> Eén van de zaken die in het rapport van de PEC uitgebreid aan de orde komt, is de visie van de Commissie op de opsporing en die ten grondslag ligt aan de huidige regeling van de opsporing. De PEC onderscheidt in haar rapport ten minste drie fasen binnen de opsporing<sup>7</sup>:

- fase 1: de voorfase, waarin nog geen sprake is van opsporing;
- fase 2: in deze fase is sprake van een redelijk vermoeden van een te plegen ernstig misdrijf (aangeduid als 'pro-actieve opsporing');
- fase 3: in deze fase is sprake van duidelijke aanwijzingen van één of meer gepleegde strafbare feiten van meer of minder ernstige aard:
  - a. de fase waarin sprake is van een redelijk vermoeden van een gepleegd strafbaar feit; er is sprake van een verdenking;
  - b. de fase waarin sprake is van een redelijk vermoeden van schuld aan een gepleegd strafbaar feit; er is sprake van een verdenking en een verdachte.

### Fase I

De eerste fase die de PEC onderscheidt is die welke aan de daadwerkelijke opsporing voorafgaat. Daarbij gaat het onder meer om 'het openhouden van ogen en oren' door politie en andere controlerende instanties. Deze controleren, winnen open informatie in en ontvangen passief tips van derden (mogelijk ook informant(en)). Dit is nog geen opsporing<sup>8</sup>.

### Fase II

De opsporing in de tweede fase is volgens de PEC alleen mogelijk wanneer sprake is van een redelijk vermoeden van te plegen ernstige misdrijven, dat wil zeggen: een vermoeden dat berust op feiten en omstandigheden en meer is dan een aanwijzing of een tip. Het zal daarbij bijna altijd gaan om georganiseerde criminaliteit of organisatiecriminaliteit. Effectieve bestrijding van de georganiseerde criminaliteit vraagt om een andere aanpak dan die welke wordt gehanteerd bij de traditionele criminaliteit. In plaats van een aangifte af te wachten, gaan de opsporingsautoriteiten zelf actief op onderzoek uit. Daarbij gaat het niet alleen om de opsporing van reeds gepleegde misdrijven, maar tevens om het in beeld brengen van de criminele organisatie. Om een complex van personen en feiten

---

6. Zie ook *Rapport Evaluatie wet bijzondere politieregisters* 2004.

7. *Kamerstukken II*, 1996/97, 25 403, nr. 3, p. 101.

8. *Kamerstukken II*, 1996/97, 25 403, nr. 3, p. 101.

te kunnen onderzoeken, teneinde een tot de georganiseerde criminaliteit behorende criminele groepering in beeld te brengen en de te vervolgen feiten en verdachten te selecteren, moeten in de optiek van de PEC bijzondere opsporingsbevoegdheden kunnen worden ingezet. Enerzijds dient er gelegenheid te zijn om bevoegdheden te hanteren voor de opheldering van meer dan één of enkele strafbare feiten, anderzijds beperkt dit criterium de inzet van deze bevoegdheden tot georganiseerde criminaliteit; zo wordt voorkomen dat de bevoegdheden onnodig ruim kunnen worden ingezet. Aangezien bij het onderzoek naar georganiseerde criminaliteit vaak al één of meer misdrijven zijn aan te wijzen maar het onderzoek daartoe niet kan worden beperkt, is het is niet geheel juist om in dit verband te spreken van ‘pro-actieve opsporing’<sup>9</sup>.

### Fase III

In de derde fase gaat het om feitelijk gepleegde strafbare feiten van meer of minder ernstige aard, waarbij onderscheid wordt gemaakt tussen de klassieke verdenking en de klassieke verdachte. In het eerste geval bestaat een redelijk vermoeden dat berust op feiten en omstandigheden van een gepleegd strafbaar feit. In het tweede geval is er een verdachte of een persoon ‘te wiens aanzien uit feiten en omstandigheden een redelijk vermoeden van schuld aan een strafbaar feit voortvloeit’. De PEC duidt opsporingsactiviteiten die zich richten op deze derde fase in de opsporing van gepleegde strafbare feiten.

### Schema

De visie van de PEC met betrekking tot de opsporing kan in schema (schema 1) worden weergegeven. Hierbij is voor elk van de drie fasen aangegeven aan welke voorwaarden moet zijn voldaan, wanneer de inzet van bijzondere opsporingsmethoden mogelijk is en op welk moment daadwerkelijk sprake is van opsporing.

	Opsporing volgens PEC		
	Fase I	Fase II	Fase III
<b>Kenmerken/ voorwaarden</b>	Geen specifieke beperkingen	Redelijk vermoeden van een te plegen ernstig misdrijf	Verdenking
<b>Inzet bijzondere opsporingsmethoden</b>	Nee	Ja	Ja
<b>Is er sprake van opsporing?</b>	Nee	Ja	Ja

Schema 1 De opsporing volgens de PEC

9. Kamerstukken II, 1997/198, 25 403, nr. 6, p. 9 en Kamerstukken II, 1996/197, 25 403, nr. 3, p. 4.

### 2.3 Het proces van informatiegaring

De standpunten van de PEC wat de opsporing en het gebruik van bijzondere opsporingsmethoden betreft zijn met de Wet Bijzondere Opsporingsbevoegdheden (Wet BOB)<sup>10</sup> grotendeels door de wetgever overgenomen. Volgens de MvT bij de Wet BOB is het opsporingsonderzoek een onderdeel van een meeromvattend proces van informatiegaring, dat ziet op het opbouwen en in stand houden van een goede informatiepositie door politie en justitie. Informatiegaring kan in alle stadia van de strafrechtelijke handhaving van de rechtsorde plaatsvinden. De mate van ingrijpendheid van de wijze waarop dit gebeurt, bepaalt in welk stadium een bepaalde vorm van informatiegaring plaatsvindt.<sup>11</sup> Binnen het proces van informatiegaring kunnen drie typen van onderzoek (of *juridische stadia*<sup>12</sup>) worden onderscheiden<sup>13</sup>:

- a. het opbouwen en in stand houden van een zekere informatiepositie, door:
  - het opslaan, bewerken, gebruiken en analyseren van gegevens, of
  - het vergaren van gegevens door de toepassing van niet-ingrijpende middelen;
- b. het verkennend onderzoek;
- c. het opsporingsonderzoek.

De volgorde van de stadia hangt samen met het directe belang dat aan informatie wordt ontleend. In het opsporingsonderzoek is informatie van essentieel belang om tot strafvorderlijk onderzoek te kunnen overgaan. Het verkennend onderzoek gaat daaraan vooraf. Het opbouwen en in stand houden van een zekere informatiepositie is als het ware een noodzakelijke voorwaarde om het verkennend onderzoek en het opsporingsonderzoek adequaat en efficiënt te kunnen uitvoeren. In deze sectie wordt ingegaan op de wijze waarop de opsporing momenteel wettelijk is geregeld en hoe de wettelijke regeling zich verhoudt tot de visie op de opsporing van de PEC.

#### 2.3.1 Stadium A: Het opbouwen en in stand houden van een zekere informatiepositie

De basisactiviteit van het proces van informatiegaring is het opbouwen en in stand houden van een zekere informatiepositie in het belang van de strafrechtelijke handhaving van de rechtsorde. Dit gebeurt door het opslaan, bewerken, gebruiken en analyseren van gegevens, dan wel het vergaren van gegevens door de toepassing van niet-ingrijpende middelen. Bepaalde vormen van criminaliteit kunnen alleen, of op veel effectievere wijze, worden aangepakt wanneer de politie een informatiepositie van een zeker niveau

---

10. Wet van 27 mei 1999, *Stb.* 1999, 245. De Wet bijzondere opsporingsbevoegdheden is per 1 februari 2000 in werking getreden.

11. Zie ook Beijer e.a. 2004.

12. Zie ook Advies van het College van Procureurs-generaal 1997.

13. *Kamerstukken II*, 1996/97, 25 403, nr. 3, p. 9.

heeft<sup>14</sup>. Hoewel de wetgever hierbij voornamelijk de bestrijding van de zware criminaliteit noemt, zal het belang van een goede informatiepositie zich daartoe in de praktijk niet beperken.<sup>15</sup> Een goede informatiepositie is in beginsel onmisbaar voor de strafrechtelijke handhaving van de rechtsorde als geheel. Bij het streven naar een goede informatiepositie speelt de WPoI een belangrijke rol. Deze wet regelt de opslag, de bewerking en het gebruik van gegevens door de opsporingsautoriteiten. De gegevens in de politieregisters kunnen zijn verkregen uit opsporingsonderzoek, verkennend onderzoek, of de toepassing van niet-ingrijpende middelen zoals het ogen en oren openhouden of het inzetten van een informant op andere wijze dan voorzien in art. 126 Sv.

#### *2.3.1.1 Het opslaan, bewerken, gebruiken en analyseren van gegevens*

Informatiegaring kan om te beginnen plaatsvinden door het bewerken van de gegevens die reeds in de politieregisters aanwezig zijn. Dat deze gegevens kunnen worden gebruikt ten behoeve van de informatiepositie, kan worden afgeleid uit het feit dat wordt gesproken over het opslaan, bewerken, gebruiken en analyseren van (al aanwezige) gegevens. Opgemerkt zij dat dit slechts mogelijk is binnen de wettelijke grenzen; deze zullen in hoofdstuk 4 uitvoerig aan de orde komen.

#### *2.3.1.2 Het vergaren van gegevens door de toepassing van niet-ingrijpende middelen*

Een verbetering van de informatiepositie kan ook worden bereikt door het verzamelen van nieuwe gegevens met behulp van niet-ingrijpende middelen. Bij het opbouwen en in stand houden van een zekere informatiepositie is het in beginsel niet toegestaan dat gebruik wordt gemaakt van ingrijpende middelen. Dat laatste is voorbehouden aan de opsporing. Naarmate een bevoegdheid ingrijpender van aard is, worden hogere eisen gesteld aan de strafbare feiten met betrekking waartoe de bevoegdheid mag worden uitgeoefend<sup>16</sup>. Niet-ingrijpende middelen worden niet in de wet geregeld, omdat zij geen inbreuk op de privacy maken. De inzet van de daarmee verband houdende opsporingsmethoden vindt legitimatie in de art. 2 Politiewet 1993 en 141 en 142 Sv.<sup>17</sup> Deze methoden mogen overigens niet zonder enige beperking worden toegepast. Zij zijn alleen toegestaan indien zij passen binnen en dienen ter uitvoering van de politietaak met betrekking tot de strafrechtelijke handhaving van de rechtsorde. Dit betekent dat burgers gevrijwaard zijn van politieke activiteit indien hun persoon geen aanleiding geeft tot politieke bemoeienis<sup>18</sup>. Onder 'politieke activiteit' dienen alle activiteiten te worden verstaan die zijn gericht op de strafrechtelijke handhaving van de rechtsorde en verricht worden door de politie. Dit betekent dat noch zwaardere, noch lichtere opsporingsbevoegdheden

14. *Kamerstukken II*, 1996/197, 25 403, nr. 3, p. 8.

15. *Kamerstukken II*, 1996/197, 25 403, nr. 3, p. 8.

16. *Kamerstukken II*, 1996/197, 25 403, nr. 3, p. 8-9.

17. *Kamerstukken II*, 1996/197, 25 403, nr. 3, p. 98.

18. *Kamerstukken II*, 1996/197, 25 403, nr. 3, p. 8.

waarvan de grondslag in de politietaak besloten ligt, toegepast mogen worden wanneer de betrokkene daartoe geen aanleiding geeft. Het 'ongericht' bespieden en volgen van burgers is niet toegestaan<sup>19</sup>.

### **Reikwijdte art. 2 Politiewet 1993**

De bevoegdheden die de politie heeft ten behoeve van de strafrechtelijke handhaving van de rechtsorde zijn geregeld in het Wetboek van Strafvordering en in andere wetten, zoals de Opiumwet en de Wet wapens en munitie<sup>20</sup>. Lange tijd bevatte het Wetboek van Strafvordering nauwelijks enige systematische beschrijving van opsporingsmethoden met als resultaat, dat veel opsporingsonderzoek buiten elke wettelijke regeling viel<sup>21</sup>. Hoewel deze situatie inmiddels is verbeterd, bestaat dit probleem nog steeds. De actualiteit ervan blijkt onder meer uit de vraagstukken die zich opwerpen bij de toepassing van een relatief nieuw fenomeen als datamining, waarvoor momenteel geen specifieke wettelijke regeling voorhanden lijkt te zijn. Teneinde vast te stellen in hoeverre art. 2 Politiewet 1993 als legitimatie kan worden gezien voor het gebruik van dataminingonderzoek, worden onderstaand twee in dat licht relevant geachte artikelen, te weten art. 1 Sv en art. 2 Politiewet 1993, nader op hun merites gezien.

Naar de letter van art. 1 Sv heeft strafvordering alleen plaats op de wijze bij de wet (in formele zin) voorzien. Dit artikel slaat een brug naar de Grondwet (Gw), daar art. 107 Gw bepaalt dat het strafprocesrecht in een wet dient te worden geregeld. Inbreuken op grondrechten die plaatsvinden in het kader van de strafvordering zullen daarom in de wet moeten worden gelegitimeerd. Indien het gebruik van datamining dergelijke inbreuken met zich meebrengt, zal de toepassing ervan expliciet door middel van wetgeving dienen te worden geregeld teneinde het handelen van politie en justitie te legitimeren. Naarmate het gebruik van datamining dieper ingrijpt in de rechten van de burger neemt de behoefte aan rechtsbescherming, en daarmee aan een wettelijke grondslag, toe.

Een en ander neemt niet weg dat de politie in de praktijk gebruik kan maken van opsporingsmethoden zonder dat daar een directe wettelijke grondslag voor aanwezig is. Deze handelwijze kan volgens sommigen worden gerechtvaardigd door in art. 2 Politiewet 1993 een algemene bevoegdheidsverlening voor de politie te onderkennen. De vraag is echter in hoeverre deze stellingname terecht is. Indien het gaat om het gebruik van opsporingsmethoden die een inbreuk kunnen maken op fundamentele rechten van burgers is het, mede met het oog op het legaliteitsbeginsel van art. 1 Sv, onwenselijk dat die kunnen worden gelegitimeerd met een beroep op een zo algemeen gesteld artikel. Art. 2

---

19. *Kamerstukken II*, 1997/98, 25 403, nr. 7, p. 18.

20. *Parlementaire Enquêtecommissie Opsporingsmethoden*, Bijlage VI, sectie 2.2: 'Politie, openbaar ministerie en rechter-commissaris'.

21. Corstens 2002, p. 251.

Politiewet 1993 dient veeleer als taakbeschrijvend te worden beschouwd en niet zozeer als bevoegdheidverlenend. Dit uitgangspunt wordt bevestigd door de wetgever met betrekking tot het gebruik van niet-ingrijpende opsporingsmiddelen ten behoeve van de opsporingstaak.

In de MvT bij de wet BOB<sup>22</sup> wordt aangegeven, dat niet-ingrijpende middelen geen wettelijke basis behoeven omdat zij geen inbreuk op de privacy maken. De opvatting dat de politie op grond van art. 2 Politiewet 1993 onderzoeksbevoegdheden tegen burgers mag gebruiken voordat er sprake is van een concrete verdenking van een strafbaar feit, blijkt ook uit de jurisprudentie van de Hoge Raad (HR)<sup>23</sup>, zij het wel met een belangrijke nuance. In een uitspraak van de HR van 19 december 1995 aangaande opsporingsmethoden die geen wettelijke grondslag hadden en werden ingezet in de pro-actieve fase van het onderzoek, kan in de fase voorafgaand aan de opsporing op grond van art. 2 Politiewet 1993 een beperkte inbreuk op de persoonlijke levenssfeer worden gerechtvaardigd. De globale taakomschrijving van het artikel biedt daarvoor, volgens de HR, een toereikende wettelijke grondslag. Met de pro-actieve fase werd bedoeld op het stadium waarin niet of onvoldoende vaststaat dat een strafbaar feit is of wordt gepleegd en dus ook nog geen verdachte in de zin van art. 27 Sv aanwijsbaar is.

Met betrekking tot de reikwijdte van art. 2 Politiewet 1993 kan worden geconcludeerd dat bij het gebruik door de politie van onderzoeksmethoden en -technieken een inbreuk op fundamentele rechten slechts is toegestaan op grond van een verdragsrechtelijke dan wel grondwettelijke bepaling. Indien de Grondwet het stellen van een beperking op enig fundamenteel recht toelaatbaar acht, wordt dit slechts geëgitimeerd door of krachtens een wet in formele zin. Bij 'fundamentele rechten' moet voornamelijk worden gedacht aan het recht op de persoonlijke levenssfeer, zoals geregeld in art. 10 Gw en art. 8 lid 1 van het Europees Verdrag voor de rechten van de mens (EVRM). In het geval een opsporingsmethode een inbreuk impliceert, dient de bevoegdheid daartoe voldoende kenbaar en voorzienbaar in de wet te zijn omschreven. Het in algemene bewoordingen gestelde art. 2 kan niet als zodanig worden begrepen. Vooral ten aanzien van het dataminingsproces lijkt de HR deze mening te delen. In voornoemd arrest van 19 december 1995 merkt de HR op dat 'de voortschrijdende ontwikkeling van het fundamentele recht op de bescherming van de persoonlijke levenssfeer en de toenemende technische verfijning en intensivering van onderzoeksmethoden en -technieken een meer precieuzere legitimatie vereisen voor zulke inbreuken dan art. 2 Politiewet 1993 biedt'.

---

22. *Kamerstukken II*, 1996/97, 25 403, nr. 3, p. 8.

23. HR 14 oktober 1986, *NJ* 1987, 564; HR 14 oktober 1986, *NJ* 1988, 511; HR 13 oktober 1992, *NJ* 1993, 223; HR 19 december 1995, *NJ* 1996, 249.

### 2.3.1.3 *Verhouding tot fase I van de PEC*

Kenmerkend voor dit stadium van de opsporing – dat ziet op het opbouwen en in stand houden van een zekere informatiepositie – is, dat er nog geen verdenking is van een strafbaar feit en ook niet een vermoeden van het beramen of plegen van ernstige misdrijven in georganiseerd verband. Er is derhalve nog geen sprake van opsporing, maar wel van de strafrechtelijke handhaving van de rechtsorde in het kader waarvan het gehele proces van informatiegaring plaatsvindt. Het gebruik van bijzondere, c.q. ingrijpende opsporingsmethoden is hier uitgesloten. Er mogen geen politieke activiteiten worden ontplooid ten aanzien van burgers indien hun persoon daartoe geen aanleiding geeft. Dit vertoont duidelijke overeenkomsten met de voorfase zoals omschreven door de PEC. Ook daar wordt gestreefd naar het verkrijgen en behouden van een goede informatiepositie en worden de in de voorfase ontplooid activiteiten nog niet als opsporing aangemerkt.

### 2.3.2 *Stadium B: Het verkennend onderzoek*

Het tweede stadium binnen het proces van informatiegaring betreft het verkennend onderzoek, dat geschiedt onder het gezag van de Officier van Justitie (OvJ)<sup>24</sup>. Het verkennend onderzoek is vooral geïntroduceerd met de gedachte aan situaties waarin tegen een verzameling van personen aanwijzingen bestaan, die bemoeden met die groep rechtvaardigt. Er is nog geen sprake van opsporing, maar het onderzoek betreft wel de strafrechtelijke handhaving van de rechtsorde. In het kader van een verkennend onderzoek kan een inbreuk worden gemaakt op de persoonlijke levenssfeer, bijvoorbeeld doordat gegevens worden vastgelegd omtrent bepaalde personen zonder dat zij verdachte of betrokkene zijn. Daarom heeft het verkennend onderzoek een wettelijke basis gekregen in art. 126gg Sv.

*‘Indien uit feiten of omstandigheden aanwijzingen voortvloeien dat binnen verzamelingen van personen misdrijven worden beraamd of gepleegd als omschreven in artikel 67, eerste lid, die gezien hun aard of de samenhang met andere misdrijven die binnen die verzamelingen van personen worden beraamd of gepleegd een ernstige inbreuk op de rechtsorde opleveren, kan de officier van justitie bevelen dat opsporingsambtenaren daarnaar een onderzoek instellen met als doel de voorbereiding van opsporing.’*

Het verkennend onderzoek schept de bevoegdheid om in bepaalde gevallen ter voorbereiding van de opsporing een onderzoek in te stellen. Die gevallen doen zich voor wanneer er feiten of omstandigheden zijn waaruit aanwijzingen voortvloeien, dat binnen verzamelingen van personen misdrijven worden beraamd of gepleegd als omschreven in art. 67 lid 1 Sv die, gezien hun aard of de samenhang met andere misdrijven die binnen

---

24. Art. 13 Politiewet 1993.

die verzamelingen van personen worden beraamd of gepleegd, een ernstige inbreuk op de rechtsorde opleveren. Een bevel voor een dergelijk onderzoek kan alleen worden gegeven door de OvJ. Het verkennend onderzoek bestaat uit het vergaren, veredelen en analyseren van informatie met betrekking tot de in art. 126gg Sv bedoelde verzameling van personen<sup>25</sup>. Het onderzoek zal in belangrijke mate bestaan uit vergelijking van gegevens uit politieregisters met gegevens uit open bronnen. Omdat er nog geen sprake is van opsporingsonderzoek, kan een verkennend onderzoek zich ook richten tot personen die (nog) niet als verdachte kunnen worden aangemerkt. Daarbij kan inbreuk worden gemaakt op de persoonlijke levenssfeer van de personen die deel uitmaken van de onderzochte groeperingen. Het feit dat de gegevens zijn ontleend aan open bronnen, of aan het vergelijken van open bronnen met politieregisters, doet daar niet aan af. Ter voorkoming van inbreuken op de persoonlijke levenssfeer mag in dit stadium nog geen gebruik worden gemaakt van opsporingsbevoegdheden of dwangmiddelen die tot een dergelijke inbreuk kunnen leiden.

In veel gevallen zullen reeds voldoende feiten en omstandigheden bekend zijn die aanleiding geven tot een vermoeden dat misdrijven zijn gepleegd of worden beraamd, op grond waarvan direct een opsporingsonderzoek kan worden gestart. Het kan echter noodzakelijk zijn eerst onderzoek te doen naar de gehele sector teneinde vast te kunnen stellen op welke wijze de criminaliteit zich daarin heeft genesteld. Een mogelijke toepassing van het verkennend onderzoek is het verrichten van fenomeenonderzoek, waarmee op systematische wijze bepaalde onderwerpen – zoals een geografisch gebied, een bevolkingsgroep of een criminele markt – kunnen worden doorgelicht. Het onderzoek heeft een verkennend, pro-actief karakter waarbij kan worden geput uit een grote verscheidenheid aan informatiebronnen, zoals de Kamers van Koophandel, het kadaster, wetenschappelijke publicaties en private instellingen als banken en andere relevante bedrijven<sup>26</sup>. Op grond van de resultaten van een verkennend onderzoek kan worden besloten tot een opsporingsonderzoek.

Het verkennend onderzoek onderscheidt zich primair van de opsporing door het onderwerp van onderzoek: een grote verzameling burgers, ten aanzien waarvan geen verdenking en zelfs geen beeld van een concreet misdrijf hoeft te bestaan. Voorts verschilt de aard van een verkennend onderzoek van die van een opsporingsonderzoek. Het is nog niet gericht op een strafrechtelijke afdoening gebaseerd op een verdenking van een strafbaar feit en er is nog geen sprake van een redelijk vermoeden, dat in georganiseerd verband ernstige misdrijven worden beraamd of gepleegd. De informatie die wordt verzameld, veredeld en geanalyseerd heeft en mag slechts betrekking hebben op een duidelijk

---

25. *Handboek voor de opsporingspraktijk 2000*, Model Verkennend onderzoek.

26. *Kamerstukken II*, 1999/100, 26 883, nr. 3, p. 14.

afgebakende groep van personen<sup>27</sup>. Kenmerkend voor een verkennend onderzoek is dat het (nog) niet specifiek is gericht op een bepaalde verdachte. Derhalve mogen geen bijzondere opsporingsbevoegdheden worden toegepast<sup>28</sup>. Deze kunnen alleen worden ingezet ten behoeve van strafrechtelijke afdoening van delicten en niet ter verbetering van de algemene informatiepositie van politie en justitie<sup>29</sup>. Wanneer naar aanleiding van een verkennend onderzoek de wenselijk blijkt van teruggeleiding van eventuele bezwarende gegevens naar een individualiseerbare persoon dient te worden overgegaan tot een opsporingsonderzoek. Daarmee eindigt het verkennend onderzoek. Momenteel kan worden gesproken van een grijs gebied tussen deze twee stadia van het proces van informatiegaring, waardoor het niet zonder meer duidelijk is wanneer het ene eindigt en het andere begint.

Het is de vraag in hoeverre een verkennend onderzoek in de huidige vorm nog een bruikbaar instrument is. De wetgever geeft zelf aan dat een verkennend onderzoek in de huidige vorm alleen tot goede resultaten kan leiden wanneer er ruimte is om te beschikken over de zogenaamde naam-, adres- en woonplaats (NAW)gegevens.<sup>30</sup> Voor de Wet Vordere gegevens telecommunicatie<sup>31</sup> is echter besloten die bevoegdheid niet te introduceren voor het verkennend onderzoek. In het kader van het wetsvoorstel opsporen van terrorisme<sup>32</sup> wordt echter een uitbreiding van het verkennend onderzoek van art. 126gg Sv voorzien. De wetgever stelt met de toevoeging van art. 126hh Sv voor om de mogelijkheden tot verkennend onderzoek te vergroten in het geval er aanwijzingen bestaan dat binnen verzamelingen van personen terroristische misdrijven worden beraamd of gepleegd. Hierbij gaat het om de mogelijkheid tot het verkrijgen en gebruiken van niet-openbare gegevens van derden, waaronder identificerende gegevens (NAW-gegevens), al dan niet terzake telecommunicatie, en het bewerken (zoals vergelijken en koppelen) van gegevensbestanden van publieke en private organisaties. Dit bewerken van gegevens omschrijft de wetgever als het verkrijgen van nieuwe gegevens door een vergelijking of een combinatie van verschillende reeds beschikbare gegevens of verzamelingen van gegevens. De gegevens ontstaan eerst door de bewerking en zijn zonder deze niet voorhanden. Het voorgestelde art. 126hh Sv opent de weg naar de toepassing van datamining in de (vergaande) vorm van 'Rasterfahndung'.<sup>33</sup> Voorts worden de beperkingen, gesteld bij of krachtens de WPolr (deels) buiten toepassing verklaard. Ook indien de voorgestane

---

27. Deze beperking staat niet met zoveel woorden in de wet maar blijkt onder meer uit de definitie in het eindrapport van de PEC (*Kamerstukken II*, 1995/96, 24 072, nrs. 10-11) en het Handboek voor de opsporingspraktijk 2000, inzake het verkennend onderzoek.

28. *Kamerstukken II*, 1996/97, 25 403, nr. 3, p. 57-58.

29. *Kamerstukken II*, 1996/97, 25 403, nr. 3, p. 24.

30. *Kamerstukken II*, 2001/02, 28 059, nr. 3, p. 11 en Sietsma 2004.

31. *Stb.* 2004, 105.

32. *Kamerstukken II*, 2004/05, 30 164.

33. *Kamerstukken II*, 2004/05, 30 164, nr. 3, p. 29-33.

aanpassingen inzake het verkennend onderzoek worden doorgevoerd, blijft het doel van het onderzoek de voorbereiding van de opsporing en niet het nemen van concrete in de wet omschreven strafvorderlijke beslissingen. Bij de bespreking van art. 126gg Sv in het kader van dit onderzoek wordt hierna steeds uitgegaan van het verkennend onderzoek in de huidige vorm.

#### **Procedure verkennend onderzoek**

Een verkennend onderzoek behoort tot het takenpakket van de politie en kan alleen worden ingesteld op een bevel ex art. 126gg Sv van de OvJ. Toepassing is slechts mogelijk wanneer is voldaan aan de eisen die art. 126gg Sv daarvoor stelt. Voor het starten van een verkennend onderzoek dient de OvJ een schriftelijk bevel op te stellen, bevattende<sup>34</sup>:

- de aanleiding: de feiten en omstandigheden die aan het bevel ten grondslag liggen;
- de doelstelling: een concrete probleemstelling met betrekking tot een zo exact mogelijk omschreven verzameling van personen;
- een tijdsplanning: een omschrijving van het voorgenomen tijdspad.

Voor sommige onderzoeken is tevens de toestemming van het College van Procureurs-generaal vereist. Dit is het geval indien het onderzoek:

- wordt uitgevoerd door een kernteam, of
- maatschappelijke, politieke, economische of publicitaire consequenties kan hebben, of
- een landelijk of interregionaal karakter heeft.

De informatie die wordt gebruikt voor het verkennend onderzoek kan afkomstig zijn uit (politie)registers, open bronnen en lopende onderzoeken en dient te worden opgeslagen in een tijdelijk politieregister<sup>35</sup>. De WPolr bepaalt voor welke doeleinden en over welke personen gegevens mogen worden opgeslagen. Een tijdelijk register kan in beginsel alle categorieën van persoonsgegevens bevatten, voor zover nodig voor de verwezenlijking van het doel waarvoor het register is aangelegd.

#### **Herziening art. 126gg Sv**

In verband met de komst van de Wbp is een tweede lid aan art. 126gg Sv toegevoegd. Op grond daarvan is het mogelijk dat de OvJ, indien dit noodzakelijk is voor de uitvoering van het onderzoek, bepaalt dat art. 9 lid 1 Wbp met betrekking tot het onderzoek niet van toepassing is op daarbij nader aan te geven openbare registers die bij wet zijn inge-

34. *Handboek voor de opsporingspraktijk 2000*, Model Verkennend onderzoek.

35. Dit is een bijzonder politieregister als omschreven in art. 1 sub j WPolr.

steld<sup>36</sup>. Art. 9 Wbp ziet op het uitgangspunt dat persoonsgegevens niet (verder) worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor zij zijn verkregen. Het tweede lid van art. 126<sup>gg</sup> Sv maakt het mogelijk om dit uitgangspunt van onverenigbaar gebruik onder omstandigheden buiten beschouwing te laten. Gegevens die in eerste instantie voor andere doeleinden zijn verkregen, kunnen nu ten behoeve van de opsporing worden gebruikt.

In overeenstemming met art. 15 lid 3 onder *b* Handelsregisterwet 1996 kunnen de Kamers van Koophandel in het kader van een verkennend onderzoek overzichten op natuurlijke personen verstrekken in het belang van de opsporing van strafbare feiten. Een verstrekking op grond van art. 15 lid 3 onder *b* Handelsregisterwet 1996 kan plaatsvinden naar aanleiding van een concrete aanwijzing in een individueel geval, maar kan ook in bulk plaatsvinden. Een bulkverstrekking maakt het mogelijk te zoeken naar een op voorhand onbepaalde groep van personen. Van belang is dat het gebruik van de gegevens is beperkt tot een ‘bepaald geval’ in de zin van art. 13 WPolr<sup>37</sup>, dus bij een verdenking of een CIE-subject. Het meest ruime gebruik zou zijn bij een verkennend onderzoek. Buiten een verkennend onderzoek, verdenking of een andere ‘uitvoering van de politietaak in een bepaald geval’ (met een tijdelijk register) kan ten behoeve van de opsporing niet zonder meer gebruik worden gemaakt van gegevens uit een openbaar register.<sup>38</sup> Op grond van art. 4 WPolr is de verwerking van persoonsgegevens slechts mogelijk indien dit noodzakelijk is voor de uitvoering van de politietaak. Het noodzakelijkheidsvereiste brengt met zich mee dat de politietaak niet kan rechtvaardigen dat over een onbepaalde groep van burgers gegevens worden vergaard voor algemene politieke doeleinden, ook niet wanneer die gegevens uit openbare bronnen afkomstig zijn.

Deze constatering heeft verstrekking gevolgen voor het gebruik van openbare gegevensbronnen in het kader van de opsporingstaak. De wetgever geeft daarmee in beginsel aan dat het gebruik van (persoons)gegevens uit openbare bronnen slechts mogelijk is in het kader van de politietaak in een ‘bepaald geval’ in de zin van art. 13 WPolr. Dit impliceert ten eerste dat dergelijke gegevens in beginsel slechts tijdelijk mogen worden verwerkt.

Ten tweede kunnen zij alleen worden gebruikt ten behoeve van een bepaalde zaak, waarbij ten minste sprake dient te zijn van de voorwaarden die gelden voor het doen van een verkennend onderzoek. Dit betekent dat er in ieder geval feiten of omstandigheden moeten zijn waaruit aanwijzingen voortvloeien, dat binnen verzamelingen van personen misdrijven worden beraamd of gepleegd als omschreven in art. 67 lid 1 Sv die – gezien hun aard of de samenhang met andere misdrijven die binnen die verzamelingen van per-

---

36. *Kamerstukken II*, 1998/99, 26 410, nr. 3, p. 10-11.

37. Art. 13 WPolr regelt de aanleg van een tijdelijk politieregister.

38. *Kamerstukken II*, 1998/99, 26 410, nr. 3, p. 10-11.

sonen worden beraamd of gepleegd – een ernstige inbreuk op de rechtsorde opleveren. In alle andere gevallen is de verwerking van openbare gegevens, waartoe ook informatie op het internet kan worden gerekend, niet mogelijk op grond van art. 4 WPolr.

### 2.3.2.1 *Verhouding tot fase II van de PEC*

Opsporing in de tweede fase is volgens de PEC mogelijk bij te plegen ernstige misdrijven waarbij sprake is van een redelijk vermoeden, dat wil zeggen een vermoeden dat berust op feiten en omstandigheden en meer is dan een aanwijzing of een tip. De PEC merkt deze fase reeds aan als opsporing waarbij het gebruik van bijzondere opsporingsbevoegdheden is toegestaan. Hoewel het in fase II bijna altijd zal handelen om georganiseerde criminaliteit of organisatiecriminaliteit, kan het criterium dat de PEC hanteert veel ruimer worden uitgelegd. In beginsel kan het gaan om elk te plegen ernstig misdrijf. Nadeel daarvan is dat ook buiten de bestrijding van de georganiseerde criminaliteit gebruik kan worden gemaakt van bijzondere opsporingsmethoden, hetgeen door de wetgever ongewenst wordt geacht. Bovendien blijven de bevoegdheden van politie en justitie beperkt tot één te plegen misdrijf, terwijl het er bij het onderzoek naar de georganiseerde criminaliteit nu juist om gaat het geheel van de criminele activiteiten van de organisatie in beeld te brengen, alvorens het onderzoek toe te spitsen op de concrete misdrijven en verdachten<sup>39</sup>. De algemene, pro-actieve opsporingsbevoegdheid die de PEC hiermee voorstaat, gaat niet samen met het uitgangspunt dat alleen de verdenking van een gepleegd delict strafvordering legitimeert. Slechts met betrekking tot de georganiseerde criminaliteit dient hierop een uitzondering te worden gemaakt. Deze vormt een dermate grote bedreiging dat een afwijkende opsporingstactiek is vereist<sup>40</sup>. Normaal gesproken legitimeert de verdenking de opsporing die op het ophelderen van de verdenking gericht is. Hier legitimeert de verdenking van de gepleegde of beraamde misdrijven echter het onderzoek van het georganiseerde verband, teneinde te komen tot een selectie van personen en misdrijven die worden vervolgd. In dit geval wordt ook deze selectie aangemerkt als opsporing<sup>41</sup>.

Het verkennend onderzoek komt niet geheel overeen met de tweede fase zoals de PEC die onderscheidt. Volgens de wetgever maakt de pro-actieve fase onderdeel uit van het hierna te bespreken opsporingsonderzoek. Daarmee is de reikwijdte van de pro-actieve fase beperkt tot het onderzoek onder leiding van de OvJ naar aanleiding van een redelijk vermoeden dat in georganiseerd verband misdrijven worden beraamd of gepleegd, als omschreven in art. 67 lid 1 Sv die, gezien hun aard of samenhang met andere misdrijven die in dat georganiseerd verband worden beraamd of gepleegd, een ernstige inbreuk op

39. *Kamerstukken II*, 1996/97, 25 403, nr. 3, p. 5.

40. *Kamerstukken II*, 1997/98, 25 403, nr. 7, p. 14-15.

41. *Kamerstukken II*, 1997/98, 25 403, nr. 7, p. 13.

de rechtsorde opleveren. Het doel van het pro-actieve onderzoek dient het nemen van strafvorderlijke beslissingen te zijn. In het kader van dit onderzoek kunnen bijzondere opsporingsmethoden worden gebruikt. Het onderzoek valt onder de verantwoordelijkheid van het OM en kan achteraf door de rechter worden getoetst.

De mogelijkheden die de PEC aan fase II van de opsporing heeft toebedeeld, zijn nu deels middels het opsporingsonderzoek wettelijk geregeld. De overige functionaliteit van de tweede fase: het doen van onderzoek naar te plegen ernstige misdrijven indien sprake is van een redelijk vermoeden, dat wil zeggen een vermoeden dat berust op feiten en omstandigheden en meer is dan een aanwijzing of een tip, lijkt (in enigszins aangepaste vorm) te worden geregeld door het verkennend onderzoek. Een verkennend onderzoek kan namelijk worden gestart wanneer uit feiten of omstandigheden aanwijzingen voortvloeien dat binnen verzamelingen van personen misdrijven worden beraamd of gepleegd als omschreven in art. 67 lid 1 Sv die, gezien hun aard of de samenhang met andere misdrijven die binnen die verzamelingen van personen worden beraamd of gepleegd, een ernstige inbreuk op de rechtsorde opleveren. In tegenstelling tot fase II van de PEC is bij een verkennend onderzoek globaal aangegeven om welke misdrijven het dient te gaan. Bovendien dient het onderzoek zich te richten op verzamelingen van personen. De personen waarop een verkennend onderzoek zich richt, worden op grond van allerlei kenmerken geselecteerd, waarbij het in eerste instantie niet gaat om een georganiseerd verband. Een belangrijk verschil met fase II zoals de PEC die beschrijft is, dat het in het kader van een verkennend onderzoek niet mogelijk is om gebruik te maken van bijzondere opsporingsmethoden.

### *2.3.3 Stadium C: Het opsporingsonderzoek*

Het derde type onderzoek dat onderdeel uitmaakt van het proces van informatiegaring is het opsporingsonderzoek. Voor de komst van de Wet BOB werd slechts gesproken over het begrip 'opsporing'. Wat daar precies onder moest worden verstaan was onduidelijk. In het Wetboek van Strafvordering was geen omschrijving te vinden van dit begrip. Corstens<sup>42</sup> beschrijft het onderscheid tussen een beperkte en een ruime variant van de opsporing. Bij een beperkt opsporingsbegrip dient sprake te zijn van een al bestaande verdenking. Een ruim opsporingsbegrip omvat daarnaast de controle, waarbij tevens het speuren naar strafbare feiten die mogelijk zijn begaan tot het opsporen wordt gerekend. Bij de ruime variant hoeft nog geen sprake te zijn van een bekende verdachte. De HR ging in zijn jurisprudentie uit van het beperkte opsporingsbegrip. Hij stelde zich op het standpunt dat de opsporingsambtenaren bedoeld in de art. 141 en 142 Sv uitsluitend met het ophelderen van een al gerezen verdenking zijn belast. De werkzaamheden van de PEC en de daaruit voortgekomen Wet BOB hebben een nieuw licht geworpen op de

---

42. Corstens 2002, p. 245.

wijze waarop het begrip ‘opsporing’ dient te worden geïnterpreteerd. Op advies van de PEC is de regering overgegaan tot een nadere omschrijving van het opsporingsbegrip<sup>43</sup>. Dit heeft geresulteerd in een wettelijke definiëring van het begrip ‘opsporingsonderzoek’, welke is neergelegd in art. 132a Sv en als volgt luidt:

*‘Onder het opsporingsonderzoek wordt verstaan het onderzoek onder leiding van de officier van justitie naar aanleiding van een redelijk vermoeden dat een strafbaar feit is begaan of dat in georganiseerd verband misdrijven worden beraamd of gepleegd, als omschreven in artikel 67, eerste lid, die gezien hun aard of samenhang met andere misdrijven die in dat georganiseerd verband worden beraamd of gepleegd een ernstige inbreuk op de rechtsorde opleveren, met als doel het nemen van strafvorderlijke beslissingen.’*

Deze formulering impliceert dat het opsporingsonderzoek niet langer is beperkt tot feiten die reeds zijn gepleegd. Het verschil tussen het nieuwe criterium van art. 132a Sv en de traditionele verdenking<sup>44</sup> is, dat door het opnemen van de term ‘beramen’ een proactief element in het nieuwe criterium is opgenomen. Dit maakt het mogelijk dat personen die vermoedelijk deel uitmaken van een organisatie die in georganiseerd verband misdrijven beraamt, ook aan bevoegdheden onderworpen kunnen worden, ook al bestaat jegens hen nog geen redelijk vermoeden van schuld. Voor de georganiseerde misdaad wordt op deze wijze het ruime opsporingsbegrip gehanteerd en kan op grond van art. 132a Sv nu ook het vermoeden dat in georganiseerd verband ernstige misdrijven worden beraamd aanleiding vormen voor een opsporingsonderzoek. De in artikel 132a Sv vastgelegde definitie van opsporing is beperkt tot onderzoek dat is gebaseerd op een verdenking van een strafbaar feit, dan wel op een redelijk vermoeden dat in georganiseerd verband misdrijven worden beraamd of gepleegd die een ernstige inbreuk op de rechtsorde maken. Het opsporingsonderzoek is steeds gericht op een strafrechtelijke afdoening. Is er geen verdenking van een strafbaar feit en tevens geen vermoeden van het beramen of plegen van ernstige misdrijven in georganiseerd verband, dan is geen sprake van opsporing. Zo valt het kennismaken en vergaren van informatie over voornemens van burgers om een strafbaar feit te plegen zonder dat daadwerkelijk sprake is van een verdenking of vermoeden, zoals zojuist aangeduid, niet onder de definitie van opsporing. Laatstgenoemd handelen wordt gerekend tot de strafrechtelijke handhaving van de rechtsorde<sup>45</sup> en vindt op grond daarvan plaats onder het gezag van het OM<sup>46</sup>.

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

44. De invulling die hieraan werd gegeven voor de invoering van de Wet BOB.

45. *Kamerstukken II*, 1996/97, 25 403, nr. 3, p. 6.

46. Art. 13 Politiewet 1993.

In het kader van art. 132a Sv zij ook gewezen op het hiervoor reeds aangehaalde wetsvoorstel opsporen van terrorisme<sup>47</sup>. Met het wetsvoorstel beoogt de wetgever onder meer de huidige definitie van het opsporingsonderzoek van art. 132a Sv aan te passen. De wetgever geeft aan dat de aanleiding tot een onderzoek niet bepalend is voor de vraag of er sprake is van opsporing. De aanwezigheid van verdenking en redelijk vermoeden vormen voorwaarden voor het al dan niet mogen toepassen van een reeks strafvorderlijke bevoegdheden. Voorgesteld wordt om opsporing te omschrijven als: ‘het onderzoek in verband met strafbare feiten onder gezag van de officier van justitie met als doel het nemen van strafvorderlijke beslissingen’.<sup>48</sup> Naar aanleiding van deze voorgestelde herziening merkt Van Kempen<sup>49</sup> op dat het aangepaste opsporingsbegrip een aanmerkelijk grotere reikwijdte heeft dan de huidige definitie. Met deze aanpassingen wordt ook de opsporing die plaatsvindt op grond van aanwijzingen ingevolge bijzondere wetten als WED en WMM (en de eventuele preventieve onderzoeksbevoegdheden in veiligheidsrisicogebieden) binnen de definitie gebracht. In diverse, in de WED opgenomen opsporingsbevoegdheden wordt het begrip ‘in het belang van de opsporing’ aldus uitgelegd dat aanwijzingen van een economisch delict volstaan om de bevoegdheid te mogen toepassen.<sup>50</sup> Het begaan zijn van een strafbaar feit is niet langer het uitgangspunt, zodat ook pro-actief optreden zonder meer eronder valt. Zelfs kan ingevolge het begrip sprake zijn van opsporing bij de uitoefening van bevoegdheden zonder verdenking of aanwijzingen dat een strafbaar feit zal worden gepleegd. De algemene formulering ervan suggereert dat toepassing jegens burgers van allerlei opsporingsbevoegdheden zonder verdenking van een strafbaar feit altijd vanzelfsprekend is. Uit de MvT bij het genoemde wetsvoorstel blijkt echter dat dit niet het geval is. Om tot opsporing in verband met een toekomstig strafbaar feit te mogen overgaan, is vereist dat een verdenking van een reeds gepleegd strafbaar feit wordt vastgesteld.<sup>51</sup> De wetgever is echter van mening dat er ten behoeve van een adequate bestrijding van het terrorisme een uitzondering dient te worden gemaakt in die zin dat de toepassing van bijzondere opsporingsbevoegdheden ook mogelijk dient te zijn in het geval van aanwijzingen van een terroristisch misdrijf. De beschreven uitzondering die de wetgever maakt is met name ingegeven door de grote bedreiging die van terroristische aanslagen uitgaat en het grote aantal slachtoffers dat bij zo’n aanslag kan vallen.<sup>52</sup> In het kader van dit onderzoek wordt hierna steeds uitgegaan van het huidige art. 132a Sv.

---

47. *Kamerstukken II*, 2004/05, 30 164.

48. *Kamerstukken II*, 2004/05, 30 164, nr. 3, p. 26.

49. Van Kempen 2005, p. 7-8.

50. HR 9 maart 1993, *NJ* 1993, 633.

51. *Kamerstukken II*, 2004/05, 30 164, nr. 3, p. 20.

52. Het is niet geheel duidelijk hoe deze beperkte rechtvaardiging (tot terrorisme) voor de verstrekkende voorstellen, zich verhoudt tot de zogenaamde themaverwerkingen in het wetsvoorstel Wet politiegegevens dat in hoofdstuk 13 wordt besproken.

### 2.3.3.1 De pro-actieve fase

De pro-actieve fase is reeds ter sprake gekomen in het kader van fase II van de opsporing, zoals die er in de visie van de PEC uitziet. Gedurende de pro-actieve fase is er nog geen redelijk vermoeden van schuld aan enig strafbaar feit en kan het gaan om het door de politie zelfstandig zoeken naar informatie, het ontdekken van al gepleegde delicten, het verzamelen van informatie over nog te plegen delicten en het gebruik maken van controlebevoegdheden waarbij eventuele strafwaardige handelingen aan het licht kunnen komen<sup>53</sup>. Het doel van het gebruik van opsporingsmethoden in de pro-actieve fase is het verzamelen van informatie, zodat eventueel een strafrechtelijk onderzoek en mogelijk later strafrechtelijke vervolging kan plaatsvinden. In bepaalde gevallen heeft het verzamelen van informatie over criminele organisaties tot doel te komen tot het beëindigen van crimineel handelen of van een criminele organisatie<sup>54</sup>. Weinig landen, bijvoorbeeld Duitsland, kennen een scherp onderscheid tussen de pro-actieve en de reactieve fase binnen de opsporing. Tot voor kort bestond ook in Nederland daarvoor geen duidelijke, wettelijke regeling. In de praktijk werd het aan de rechterlijke macht overgelaten om het gebruik van bepaalde methoden op hun toelaatbaarheid te toetsen. De jurisprudentie bepaalde voor een groot gedeelte de normen van de opsporing, waardoor ten aanzien van de opsporing in toenemende mate sprake was van een 'rechterstaat'. Normering vooraf, een fundamentele eis in de rechtsstaat, bleef daarbij achterwege<sup>55</sup>. Uit het onderzoek van de PEC bleek dat politie en justitie bijzondere opsporingsmethoden hanteerden, terwijl er nog geen verdenking van enig strafbaar feit was. Dit vormde de aanzet om ook de activiteiten in de pro-actieve fase wettelijk te regelen. Om duidelijk aan te geven dat de pro-actieve opsporing niet meer mag zijn dan het verrichten van opsporingsactiviteiten ten aanzien van te plegen ernstige misdrijven die bijna altijd verbonden zijn met georganiseerde criminaliteit of organisatiecriminaliteit, adviseerde de PEC om de pro-actieve fase een eigen plaats te geven in het Wetboek van Strafvordering. Met de Wet BOB is een einde gemaakt aan de bestaande tweedeling van het opsporingsonderzoek doordat de onderzoeksfase, die in het verleden werd aangeduid als de pro-actieve fase, nu onderdeel uitmaakt van het opsporingsonderzoek<sup>56</sup>. In tegenstelling tot het advies van de PEC heeft de wetgever niet gekozen voor een toevoeging aan art. 1 Sv, maar is de inzet van opsporingsmethoden in de pro-actieve fase geregeld in een aparte Titel van Boek I van het Wetboek, namelijk Titel V; deze handelt over bijzondere bevoegdheden tot opsporing van misdrijven die in georganiseerd verband worden gepleegd of beraamd.

De pro-actieve fase zoals die door de PEC werd onderscheiden, maakt deel uit van het opsporingsonderzoek, zij het dat daarbij een beperkter criterium is gehanteerd dan door

53. Corstens 2002, p. 248.

54. *Rapport Opsporing gezocht* 1994 (*Kamerstukken II*, 1994/95, 23 945, nr. 2).

55. *Kamerstukken II*, 1995/96, 24 072, nrs. 10-11.

56. *Kamerstukken II*, 1996/97, 25 403, nr. 3, p. 17.

de PEC werd voorgesteld<sup>57</sup>. Door het samengaan van de pro-actieve fase met het opsporingsonderzoek is dat onderzoek niet beperkt tot feiten die reeds zijn gepleegd. Ook het redelijke vermoeden dat in georganiseerd verband ernstige misdrijven worden beraamd, kan aanleiding vormen voor een opsporingsonderzoek.<sup>58</sup> Het doel van het gebruik van opsporingsmethoden in de pro-actieve fase is het verzamelen van informatie, zodat eventueel een strafrechtelijk onderzoek en mogelijk later strafrechtelijke vervolging kan plaatsvinden. De personen op wie een verkennend onderzoek zich richt, worden op grond van allerlei kenmerken geselecteerd, waarbij zij geen enkele binding behoeven te hebben. Dit ligt anders bij het opsporingsonderzoek. Daarbij gaat het om een groep van personen die in een bepaald verband of wisselend verband systematisch misdaden beramen en plegen met ernstige gevolgen voor de samenleving, en die door de wijze waarop dat plaatsvindt een zodanige bedreiging vormt dat zelfstandig onderzoek gerechtvaardigd is<sup>59</sup>.

#### *2.3.3.2 Verhouding tot fase III van de PEC*

Het opsporingsonderzoek van art. 132a Sv komt op een aantal punten overeen met de derde fase binnen de opsporing zoals door de PEC onderscheiden. Er zijn ook enkele duidelijke verschillen. Zowel in de derde fase van de PEC als bij het opsporingsonderzoek is er sprake van opsporing ingeval een redelijk vermoeden bestaat van een strafbaar feit. Daarbij kan het gaan om allerlei strafbare feiten. Indien aan de voorwaarden die daarvoor gelden is voldaan, kan gebruik worden gemaakt van bijzondere opsporingsmethoden.

In beide situaties dient het onderzoek te zijn gericht op een strafrechtelijke afdoening. Zoals reeds gesteld is er ook een aantal verschillen. Zo hoeft het opsporingsonderzoek, in tegenstelling tot het uitgangspunt van de PEC, niet steeds te zijn gericht op feiten die al gepleegd zijn. Ook het redelijke vermoeden dat in georganiseerd verband ernstige misdrijven worden beraamd, kan aanleiding vormen voor een opsporingsonderzoek. Voorts maakt de PEC onderscheid (aangaande de derde fase) tussen de fase waarin sprake is van een redelijk vermoeden van een gepleegd strafbaar feit waarbij sprake is van een verdenking, en de fase waarin sprake is van een redelijk vermoeden van schuld aan een gepleegd strafbaar feit waarbij er een verdenking en tevens een verdachte is. De wetgever laat bij de definiëring van het opsporingsonderzoek dit onderscheid achterwege. Het verschil dat de PEC maakt kan echter wel van belang worden geacht in het kader van het data-miningsproces. In sectie 10.2.2 wordt hierop teruggekomen.

---

57. *Kamerstukken II*, 1996/197, 25 403, nr. 3, p. 102.

58. In andere gevallen is het pro-actief verwerken van persoonsgegevens onwenselijk, zie sectie 7.3.2.

59. *Kamerstukken II*, 1996/197, 25 403, nr. 3, p. 58.

### 2.3.4 Schema wettelijke regeling opsporing versus visie PEC

Het huidige beeld van de opsporing wijkt op een aantal punten af van dat van de PEC. In schema 2 is weergegeven hoe de opsporing op dit moment wettelijk is geregeld en hoe dit zich verhoudt tot de visie van de PEC. Het schema verschaft voorts duidelijkheid over de vraag wanneer binnen het proces van informatiegaring daadwerkelijk sprake is van opsporing en op welk moment de inzet van bijzondere opsporingsmethoden mogelijk wordt.

	Proces van informatiegaring		
	Informatiepositie	Verkennd onderzoek	Opsporingsonderzoek
<b>Kenmerken/voorwaarden</b>	Geen specifieke beperkingen	Aanwijzing misdrijven binnen verzamelingen van personen	Verdenking/pro-actief aanpak georganiseerde criminaliteit
<b>Inzet bijzondere opsporingsmethoden</b>	Nee	Nee	Ja
<b>Is er sprake van opsporing?</b>	Nee	Nee	Ja
<b>Verhouding tot visie van de PEC</b>	Fase I	(Fase II)	Fase II/Fase III

Schema 2 De wettelijke regeling van de opsporing vergeleken met de visie van de PEC

## 2.4 Inzet van bijzondere opsporingsmethoden en verbetering van de informatiepositie

Naast een regeling voor het gebruik van bijzondere opsporingsmethoden heeft de wetgever met de Wet BOB voorzien in een duidelijker juridisch kader, waarbinnen de opsporing en de activiteiten die in die context worden ontplooid, scherper zijn gereguleerd. In deze sectie wordt nader ingegaan op de inzet van bijzondere opsporingsmethoden, onder meer gedurende de pro-actieve opsporing buiten georganiseerd verband. Als afsluiting worden de mogelijkheden ter verbetering van de informatiepositie onder de loep genomen.

### *Inzet bijzondere opsporingsmethoden*

Het gebruik van bijzondere opsporingsmethoden is nadrukkelijk voorbehouden aan de opsporing. Van opsporing is in beginsel alleen sprake wanneer is voldaan aan art. 132a Sv. Of in het kader van de opsporing daadwerkelijk van bijzondere opsporingsmethoden gebruik kan worden gemaakt, is afhankelijk van de voorwaarden die daaraan in de Titels IVa en V Sv worden gesteld. Per opsporingsbevoegdheid gelden specifieke eisen. Naar-

mate een bevoegdheid ingrijpender is worden strengere eisen gesteld aan het gebruik ervan.

In de regeling van de diverse bevoegdheden noemt de wettekst telkens het belang van het onderzoek als doel van de toepassing van de bevoegdheid. Een bevoegdheid mag alleen worden gehanteerd wanneer deze bijdraagt aan de opsporing van het delict (Titel IVa) of de opsporing van het in georganiseerd verband beramen of plegen van misdrijven (Titel V)<sup>60</sup>. De bevoegdheden van Titel IVa mogen slechts worden gebruikt voor het onderzoek naar één of enkele misdrijven (de traditionele opsporing), terwijl de bevoegdheden die zijn geregeld in Titel V mogen worden gebruikt voor het onderzoek naar een complex van feiten en personen. Dit verschil impliceert dat de groep van personen die onderwerp van onderzoek kan zijn bij de toepassing van de bevoegdheden van Titel IVa, veelal kleiner zal zijn dan die welke onderwerp van onderzoek mag zijn op basis van Titel V. In beide gevallen is de groep van personen beperkt tot hen waarvan het in het belang van het onderzoek is dat zij voorwerp van onderzoek zijn. Bij Titel IVa richt het onderzoek zich op de verdachte, wat niet wil zeggen dat alleen hij voorwerp van onderzoek is. Om zekerheid te krijgen over de persoon van de verdachte en zijn rol, kan het immers nodig zijn ook anderen te onderzoeken. Bij Titel V richt het onderzoek zich op alle personen die bij het georganiseerde verband betrokken zijn, teneinde inzicht te verkrijgen in dat georganiseerde verband en de daarbinnen gepleegde misdrijven<sup>61</sup>. Met het oog op het voorgaande kan met betrekking tot het uitoefenen van de bevoegdheden van Titel V het standpunt worden ingenomen dat dit niet alleen gebeurt in het kader van de opsporing maar ook ten behoeve van een verbetering van de informatiepositie.

#### *Pro-actieve opsporing buiten georganiseerd verband*

Op grond van 132a Sv en uit de omschrijving van de verschillende bijzondere opsporingsbevoegdheden kan worden geconcludeerd dat het redelijke vermoeden dat een misdrijf wordt beraamd op zichzelf niet tot opsporing (en daarmee de mogelijke inzet van bijzondere opsporingsmethoden) kan leiden. Hiervoor is immers vereist dat een redelijk vermoeden bestaat dat ‘in georganiseerd verband misdrijven worden beraamd of gepleegd, als omschreven in art. 67 lid 1 Sv, die gezien hun aard of samenhang met andere misdrijven die in dat georganiseerde verband worden beraamd of gepleegd een ernstige inbreuk op de rechtsorde opleveren’.

Desondanks kan bij te plegen ernstige delicten van (pro-actieve) opsporing worden gesproken, ook indien deze niet door criminele organisaties worden voorbereid. In dat geval is opsporing op grond van Titel V niet mogelijk, maar wel op grond van Titel IVa Sv. De voorbereiding van delicten waarop naar de wettelijke omschrijving een gevange-

---

60. *Kamerstukken II*, 1996/97, 25 403, nr. 3, p. 7.

61. *Kamerstukken II*, 1996/97, 25 403, nr. 3, p. 22.

nisstraf van acht jaren of meer is gesteld, is ingevolge art. 46 Sr zelfstandig strafbaar. Het maximum van de hoofdstraffen op het misdrijf gesteld wordt dan met de helft vermindert; dat maximum bedraagt derhalve minimaal vier jaar. Dit brengt met zich mee dat ingeval van verdenking van strafbare voorbereiding, indien ook overigens aan de wettelijke voorwaarden is voldaan, gebruik kan worden gemaakt van bijzondere opsporingsbevoegdheden<sup>62</sup>. In alle overige situaties is geen sprake van opsporing en mag geen gebruik worden gemaakt van bijzondere opsporingsmethoden.

#### *Verbetering van de informatiepositie*

Het doel van de opsporing is het nemen van strafvorderlijke beslissingen. De opsporing met het enkele doel een informatiepositie op te bouwen is niet toegestaan<sup>63</sup>. Een verbetering van de informatiepositie lijkt wel te mogen worden nagestreefd in samenhang met het nemen van strafvorderlijke beslissingen. Daarbij kan worden gedacht aan de situatie waarin een redelijk vermoeden bestaat van ernstige misdrijven die in georganiseerd verband worden beraamd of gepleegd. Een onderzoek dient in dat geval om een complex van personen en feiten te analyseren ter opheldering van ernstige misdrijven die in georganiseerd verband worden beraamd of gepleegd. Daarmee ziet het onderzoek zowel op een verbetering van de informatiepositie als op het nemen van strafvorderlijke beslissingen. Het kennismaken en vergaren van informatie over voornemens van burgers om een strafbaar feit te plegen, zonder dat daadwerkelijk sprake is van een verdenking of vermoeden zoals bedoeld in art. 132a Sv, is in beginsel geen opsporing. Dit betekent niet dat het voor opsporingsinstanties op voorhand is uitgesloten dergelijke activiteiten te ontplooien. Binnen het proces van informatiegaring kunnen deze plaatsvinden in het kader van een verkennend onderzoek of van 'het opbouwen en in stand houden van een goede informatiepositie'. Beiden typen van onderzoek vinden plaats ter verbetering van de informatiepositie en worden gerekend tot de strafrechtelijke handhaving van de rechtsorde.

Bij het kennismaken en vergaren van informatie over voornemens van burgers om een strafbaar feit te plegen zonder dat daadwerkelijk sprake is van een verdenking of vermoeden, zijn de mogelijkheden beperkter dan bij de opsporing. Zo dient bij een verkennend onderzoek te worden voldaan aan de voorwaarden die art. 126gg Sv stelt. Omdat het onderzoek plaatsvindt ter voorbereiding van de opsporing, mogen geen strafvorderlijke bevoegdheden worden gebruikt. In het kader van een verkennend onderzoek kan er sprake zijn van inbreuken op de persoonlijke levenssfeer van de personen die deel uitmaken van de onderzochte groeperingen, bijvoorbeeld doordat omtrent deze personen gegevens worden vastgelegd zonder dat zij verdachte of 'betrokkene' zijn. Dat die gegevens

---

62. *Kamerstukken II*, 1997/98, 25 403, nr. 7, p. 15.

63. *Kamerstukken II*, 1997/98, 25 403, nr. 7, p. 18.

zijn ontleend aan open bronnen, doet daaraan niet af. In dit licht heeft het verkennend onderzoek een wettelijke grondslag.

Het kennismaken van en informatie vergaren over voornemens van burgers op de hierboven beschreven wijze kan ook plaatsvinden in het kader van de algemene verbetering van de informatiesituatie. Daarbij wordt gebruik gemaakt van de algemene opsporingsbevoegdheid van art. 2 Politiewet 1993. Met betrekking tot dit artikel heeft de HR meer dan eens uitgemaakt, dat een beperkte inbreuk op de persoonlijke levenssfeer gerechtvaardigd kan worden<sup>64</sup>. De toepassing van niet-ingrijpende methoden ter verbetering van de algemene informatiesituatie is echter niet zonder meer toegestaan. Voorop staat dat burgers gevrijwaard dienen te zijn van politieke activiteit indien hun persoon geen aanleiding geeft tot politieke bemoeienis<sup>65</sup>. De verwerking van gegevens over deze burgers kan leiden tot een inbreuk op de persoonlijke levenssfeer. De wetgever merkt het vergaren en vergelijken van gegevens van personen, over welke geen feiten of omstandigheden bekend zijn dat zij zich bezighouden met strafbare feiten, aan als een ingrijpende bevoegdheid<sup>66</sup>. Het feit dat deze gegevens zijn ontleend aan open bronnen doet hieraan niet af<sup>67</sup>. Verwerking van die informatie zal daarom moeten berusten op een wettelijke grondslag, anders dan die van art. 2 Politiewet 1993. Bij het kennismaken van en informatie vergaren over voornemens van burgers om een strafbaar feit te plegen zonder dat daadwerkelijk sprake is van een verdenking of vermoeden mag in beginsel geen inbreuk worden gemaakt op de privacy. Van een zodanige inbreuk is, mede vanwege de ontwikkelingen op het gebied van de privacywetgeving, echter al snel sprake. Omdat de betreffende activiteiten worden ontplooid in het kader van de strafrechtelijke handhaving van de rechtsorde, wordt de mogelijkheid van een inbreuk op de persoonlijke levenssfeer alleen maar groter. In dit kader zij nogmaals gewezen op art. 4 WPolr, op grond waarvan de verwerking van persoonsgegevens slechts is toegestaan indien dit noodzakelijk is voor de uitvoering van de politietaken. Het noodzakelijkheidsvereiste brengt met zich mee, dat de politietaken niet kan rechtvaardigen dat over een onbepaalde groep van burgers gegevens worden vergaard voor algemene politieke doeleinden, ook niet uit openbare bronnen<sup>68</sup>.

In tegenstelling tot het verkennend onderzoek van art. 126<sup>gg</sup> Sv berusten de activiteiten die in het eerste stadium van het proces van informatiegaring kunnen worden ontplooid, niet op een specifieke wettelijke grondslag<sup>69</sup>. Enerzijds is dit ook niet noodzakelijk

---

64. HR 14 oktober 1986, *NJ* 1987, 564; HR 14 oktober 1986, *NJ* 1988, 511; HR 13 oktober 1992, *NJ* 1993, 223; HR 19 december 1995, *NJ* 1996, 249.

65. *Kamerstukken II*, 1996/97, 25 403, nr. 3, p. 8.

66. *Kamerstukken II*, 1997/98, 25 880, nrs. 1-2, p. 83.

67. *Kamerstukken II*, 1996/97, 25 403, nr. 3, p. 49.

68. *Kamerstukken II*, 1998/99, 26 410, nr. 3, p. 10-11.

69. Art. 2 Politiewet 1993.

omdat in beginsel geen inbreuk op de privacy mag worden gemaakt. Anderzijds betekent dit eveneens dat de mogelijkheden voor de opsporingsautoriteiten in dit stadium zijn beperkt.



---

## 3 Het proces van informatiegaring en datamining

Voor het uitvoeren van het proces van informatiegaring staan de opsporingsautoriteiten verschillende onderzoeksmethoden ten dienste. Hoewel deze alle een waardevolle bijdrage kunnen leveren aan het proces van informatiegaring, kan daarvan het dataminingsproces als de veelbelovendste worden aangemerkt. Dit hoofdstuk handelt over de wijze waarop het dataminingsproces als opsporingsmethode een plaats kan worden gegeven binnen het proces van informatiegaring. Daartoe wordt onderscheid gemaakt tussen drie wijzen (dataminingsvarianten) waarop uitvoering aan dit proces kan worden gegeven, namelijk het ongerichte dataminingonderzoek, het gerichte dataminingonderzoek en de verificatie. Voor ieder van deze manieren wordt aangegeven, in welke fase van het proces van informatiegaring deze kunnen worden toegepast.

### 3.1 Informatiegaring en informatie-inwinning

Kenmerkend voor het proces van informatiegaring is het verwerken van informatie. Informatiegaring is essentieel voor een goede informatiepositie, welke de basis vormt voor een efficiënte rechtshandhaving. Het proces van informatiegaring (of informatie-inwinning<sup>1</sup>) ziet op het door de politie opbouwen en in stand houden van een goede informatiepositie. In sectie 2.3 zijn binnen het proces van informatiegaring de drie *juridische* stadia onderscheiden (het opbouwen en in stand houden van een zekere informatiepositie, het verkennend onderzoek en het opsporingsonderzoek). In de operationele sfeer van het informatiegaringproces worden twee *technische* stadia onderscheiden:

1. het verzamelen van gegevens;
2. het genereren van gegevens die nog niet bij de politie bekend zijn.

In het eerste stadium kunnen in beginsel uit allerlei bronnen gegevens worden verzameld. Binnen het dataminingsproces wordt dit stadium aangeduid met de term ‘data-

---

1. *Parlementaire Enquêtecommissie Opsporingsmethoden*: het begrip ‘informatie-inwinning’ ziet zowel op het vergaren als het genereren van gegevens die nog niet bij de politie bekend zijn.

warehousing': het verzamelen van de ruwe gegevens die later het onderwerp zullen vormen van het eigenlijke datamining, of het bewerken van de gegevens. Bij het verzamelen van gegevens gaat het volgens de omschrijving van de PEC niet om gegevens die elders binnen het politieapparaat aanwezig zijn. Het bewerken van de gegevens wordt gerekend tot het genereren van gegevens, het tweede technische stadium van het proces van informatiegaring. Na bewerking en analyse van de verzamelde gegevens kan kennis worden verkregen die voordien niet beschikbaar was. Er kunnen verschillende oorzaken zijn waarom gegevens (kennis) op een bepaald moment nog niet bekend zijn. Deze kunnen gefragmenteerd zijn opgeslagen, zodat het geheel daarvan voor niemand beschikbaar is. Ook kan het voorkomen dat nieuwe gegevens pas bekend worden nadat zij zijn bewerkt, waardoor feiten, verbanden of patronen aan het licht komen die zonder die bewerking niet zichtbaar waren. Op basis van de informatiepositie kunnen de vergaarde gegevens in het kader van het proces van informatiegaring verder worden bewerkt en geanalyseerd. In het rapport van de PEC wordt dit aangeduid met de term 'informatie-inwinning'. De combinatie van het verzamelen en het genereren van gegevens valt in beginsel binnen de definitie van het dataminingsproces.

Informatie-inwinning wordt gerealiseerd door de inzet van onderzoeksmethoden waarmee voor verschillende doeleinden informatie kan worden verzameld. In het hierna volgende wordt onderzocht op welke wijze het dataminingsproces als onderzoeksmethode een bijdrage kan leveren aan het proces van informatiegaring.

### 3.2 Onderzoeksmethoden

In het rapport 'Opsporing gezocht', dat de aanzet vormde voor de werkzaamheden van de PEC (per 6 december 1994), worden drie onderzoeksmethoden nader besproken, te weten het fenomeenonderzoek, het financieel rechercheren en de misdaadanalyse. Het fenomeenonderzoek is reeds in sectie 1.5 aan de orde geweest. Het financieel rechercheren is het proces van het veredelen, bewerken en analyseren van financiële gegevens, met het doel deze gegevens te gebruiken in een strafrechtelijk onderzoek naar personen, groepen of zaken<sup>2</sup>. Misdaadanalyse, ten slotte, betreft het opsporen en inzichtelijk maken van verbanden tussen criminaliteitsgegevens onderling en andere mogelijk relevante gegevens met het oog op de praktijk van politie en justitie<sup>3</sup>. Bij een fenomeenonderzoek worden

- 
2. Zie ook *Kamerstukken II*, 1998/99, 26 269, nrs. 4-5, p. 78: 'Onderscheid wordt gemaakt tussen tactisch financieel onderzoek en strategisch financieel onderzoek. Het eerste soort onderzoek is gericht op het genereren van bewijsmateriaal tegen concrete subjecten. Indien voldoende bewijsmateriaal is gevonden kan het tactisch onderzoek ook strekken tot ontneming van wederrechtelijk verkregen voordeel. Strategisch financieel onderzoek is eerder verwant aan het verkennend onderzoek en primair gericht op het verzamelen van gegevens over bepaalde groepen met als doel risicoprofielen en prioriteitstellingen te genereren.'
  3. *Rapport werkgroep Misdaadanalyse* 1991.

gegevens onderzocht die geen directe strafrechtelijke impact hebben. Dergelijk meer sociologisch of wetenschappelijk onderzoek behoort niet primair tot de taak van de politie. De methode van het financieel rechercheren vertoont een aantal overeenkomsten met het dataminingsproces. Omdat deze methode alleen betrekking heeft op financiële gegevens en derhalve slechts een beperkt deel van de opsporingstaak bestrijkt, wordt hierop verder niet ingegaan. Vanwege de verschillende raakpunten met het dataminingsproces lijkt – in het kader van dit onderzoek – de misdaadanalyse de interessantste onderzoeksmethode.

### 3.2.1 Misdaadanalyse

Reeds van oudsher wordt door de politie informatie verzameld bij het uitvoeren van de opsporingstaak. De mogelijkheden om deze zo goed mogelijk te benutten zijn met de komst van de computer enorm toegenomen. Doordat relevante informatie wordt opgeslagen in geautomatiseerde gegevensbestanden en de analysetechnieken steeds geavanceerder worden, kunnen gegevens eenvoudig worden hergebruikt, onderling vergeleken, geanalyseerd en veredeld. Deze gegevensverwerking wordt ook wel aangeduid als ‘misdaadanalyse’. Het doel van de misdaadanalyse kan van tweeërlei aard zijn: operationeel en strategisch. De operationele analyse kan gericht worden op direct-toepasbare resultaten voor de opsporings- en vervolgingspraktijk. De strategische analyse kan worden gebruikt bij het bepalen van het beleid. Wat de toepassing van het dataminingsproces betreft is met name de operationele analyse interessant. Daarbij worden de volgende vijf analysevormen onderscheiden:

1. *de zaakanalyse*: het inzichtelijk maken van informatie in een concrete zaak, waardoor tegenstrijdigheden of onvolledigheden aan het licht kunnen worden gebracht;
2. *de delictanalyse*: het vergelijken van gegevens van een aantal gelijksoortige delicten teneinde te achterhalen of deze door dezelfde dader(groep) zijn gepleegd;
3. *de dader(groep)analyse*: het structureren en vergelijken van gegevens die over een bepaalde delinquentengroep beschikbaar zijn; op deze wijze kan een criminele groep inzichtelijk worden gemaakt en kan ieders individuele aandeel bij illegale handelingen worden achterhaald;
4. *de specifieke profielanalyse*: het maken van een beschrijving van de dader(s) van een delict aan de hand van informatie afkomstig van onder meer het technisch onderzoek op de plaats delict en getuigenverklaringen in combinatie met achtergrondinformatie, zoals historische criminaliteitsgegevens of kennis uit gedragswetenschappelijke studies;
5. *de operatieanalyse*: het evalueren van de ondernomen activiteiten teneinde zicht te krijgen op het verloop van de operatie en te kunnen zoeken naar nog ongebruikte mogelijkheden voor rechercheactiviteiten; het onderwerp van deze vorm van analyse is de werkwijze van politie en justitie.

De eerste vier analysevormen vertonen verwantschap met het dataminingsproces. Een belangrijk onderscheid tussen misdaadanalyse en dataminingsonderzoek is, dat de klassieke misdaadanalyse geen neerslag behoeft in een wettelijke regeling omdat in beginsel steeds sprake is van een niet-ingrijpend middel. Bij de toepassing van dataminingsonderzoek kan niet in alle gevallen worden gesproken van een niet-ingrijpend middel. Bij de moderne geautomatiseerde misdaadanalyse is het goed denkbaar dat gebruik wordt gemaakt van ingrijpender methoden. Door het achterwege laten van de klassieke beperking van misdaadanalyse tot niet-ingrijpende middelen biedt de figuur van de misdaadanalyse interessante perspectieven voor dataminingsonderzoek en vice versa. Met het dataminingsproces lijkt invulling te kunnen worden gegeven aan de (moderne) misdaadanalyse. Met het oog hierop is het wenselijk vast te stellen wanneer en op welke wijze van misdaadanalyse gebruik kan worden gemaakt. Omdat een wettelijke regeling voor het uitvoeren van misdaadanalyse ontbreekt, zullen daarvoor de standpunten van de PEC en de wetgever worden geraadpleegd.

#### *Standpunt PEC*

De PEC geeft aan, dat in het kader van een misdaadanalyse altijd eerst gegevens worden verzameld. Deze kunnen worden verkregen uit open bronnen zoals kranten, telefoonboeken, handelsregisters en kadasters. Daarnaast kan gebruik worden gemaakt van gegevens uit persoonsregisters, politieke informatie en van informatie van buitenlandse instanties. Bij deze vorm van informatie-inwinning lijkt de politie een relatief grote vrijheid te kunnen nemen. De centrale toetsingscommissie voor bijzondere opsporingsmethoden van het OM (CTC)<sup>4</sup> heeft naar aanleiding van het Fieccom-onderzoek<sup>5</sup> het gebruik van openbare bronnen toelaatbaar geacht. Ook werd toegestaan politieregisters bij het fenomeenonderzoek te betrekken op het moment waarop de verdenking ontstond. Aangezien geen scherp onderscheid werd gemaakt tussen het fenomeenonderzoek en het opsporingsonderzoek, mag worden aangenomen dat de CTC ook geen bezwaren zal zien in het gebruik van deze registers bij een misdaadanalyse. Evenals bij het verkennend onderzoek van art. 126gg Sv, kan in het kader van misdaadanalyse ten behoeve van de opslag van gegevens gebruik worden gemaakt van een tijdelijk politieregister<sup>6</sup>. Volgens de PEC heeft het er alle schijn van dat dergelijke informatie-inwinning door de politie en bij derden, als ook het door misdaadanalyse genereren van gegevens, niet op bezwaren stuit<sup>7</sup>. In haar eindrapport constateerde de PEC echter ook, dat ten aanzien van de activiteiten in het kader van de misdaadanalyse nauwelijks tot geen controle bestaat. Als voor de klassieke

- 
4. Deze commissie is per 1 januari 1995 door het College van Procureurs-generaal ingesteld en heeft onder meer tot taak te beoordelen of, en onder welke voorwaarden, bepaalde methoden mogen worden ingezet. Zo ontstaat eenheid en duidelijkheid bij de inzet van bijzondere opsporingsmethoden.
  5. *Kamerstukken II*, 1995/196, 24 072, nr. 14, p. 231.
  6. *Kamerstukken II*, 1995/196, 24 072, nr. 14, p. 239.
  7. *Kamerstukken II*, 1995/196, 24 072, nr. 14, p. 46.

misdaadanalyse – waarbij geen sprake is van een niet-ingrijpend middel – het ontbreken van controle al onwenselijk is, zal dit nog veel sterker gelden voor de moderne misdaadanalyse. De toepassing van misdaadanalyse is volgens de PEC daarom pas mogelijk wanneer sprake is van een redelijk vermoeden van ernstige strafbare feiten, zoals omschreven in fase II<sup>8</sup>. Bovendien kan de inwinning van informatie bij derden een nadere wettelijke regeling vereisen.

#### *Standpunt wetgever*

Naar aanleiding van de bevindingen van de PEC heeft de wetgever met betrekking tot de misdaadanalyse een standpunt geformuleerd. De wetgever verenigt zich met de visie van de PEC, dat voor de toepassing van misdaadanalyse in ieder geval vereist is dat een redelijk vermoeden van ernstige strafbare feiten bestaat, zoals omschreven in fase II. Verder wordt onderschreven dat misdaadanalyse kan geschieden op basis van zowel opsporingsgegevens die zich in de politieregisters bevinden als op open bronnen. Wanneer de WPolr en het BPolr een verbetering van de informatiepositie niet in de weg staan, behoort de toepassing van misdaadanalyse tot de mogelijkheden. Deze kent geen wettelijke regeling. Het gebruik van gegevens die zich in politieregisters bevinden moet evenwel volgens de daarvoor geldende regels plaatsvinden. Wanneer gegevens worden vergeleken van en kennis wordt vergaard over personen ten aanzien van wie geen feiten of omstandigheden bekend zijn dat zij zich bezig houden met strafbare feiten, is er sprake van een ingrijpende bevoegdheid. In dat geval is een wettelijke grondslag vereist. Het noodzakelijkheidsvereiste brengt met zich mee dat de politietaak niet kan rechtvaardigen dat over een onbepaalde groep van burgers gegevens worden vergaard voor algemene politieke doeleinden, ook niet uit openbare bronnen.<sup>9</sup> Het gebruik van openbare bronnen lijkt dan ook niet mogelijk gedurende de eerste fase van het proces van informatiegaring.

#### *Misdaadanalyse en het dataminingsproces*

De wetgever stelt zich dus op het standpunt dat het voor de toepassing van misdaadanalyse in ieder geval is vereist dat er sprake is van een redelijk vermoeden van ernstige strafbare feiten, zoals omschreven in fase II van de opsporing (volgens de PEC). Hoewel dit goed lijkt te passen binnen het beleid met betrekking tot het gebruik van openbare bronnen, wordt daarmee het gebruik van misdaadanalyse zover beperkt, dat het zelfs niet is toegestaan om met behulp van de gegevens waarover men reeds beschikt een verbetering van de eigen algemene informatiepositie na te streven. Aangezien een dergelijke verbetering nu juist een essentieel onderdeel vormt van de mogelijkheden van het dataminings-

---

8. *Kamerstukken II*, 1996/97, 25 403, nr. 3, p. 123.

9. *Kamerstukken II*, 1998/99, 26 410, nr. 3, p. 10-11.

proces, is de beslissing om de toepassing van misdaadanalyse te beperken tot de tweede en derde fase van de opsporing zoals die door de PEC wordt beschreven, onbruikbaar.

Het valt te betreuren dat de wetgever onduidelijkheid laat bestaan over het moment waarop precies gebruik kan worden gemaakt van misdaadanalyse. Voor de plaats van de misdaadanalyse binnen de opsporing wordt in de MvT bij het wetsvoorstel bijzondere opsporingsbevoegdheden verwezen naar de visie op de opsporing zoals die door de PEC wordt voorgestaan. In diezelfde MvT geeft de wetgever een eigen invulling aan de opsporing, die afwijkt van die van de PEC. Verder wordt de misdaadanalyse op het ene moment in de MvT gekwalificeerd als een vorm van opsporing, terwijl in de volgende alinea wordt aangegeven dat misdaadanalyse geen opsporingsmethode is<sup>10</sup>. Deze situatie is onwenselijk. Wanneer sprake is van een opsporingsmethode<sup>11</sup> dient het gebruik ervan in beginsel gericht te zijn op een strafvorderlijke afdoening. Hiervan is enkel sprake in de laatste stadia van het proces van informatiegaring. Indien misdaadanalyse niet als opsporingsmethode wordt aangemerkt, kan het ook worden gebruikt in het eerste stadium van het proces van informatiegaring, dat niet per definitie gericht hoeft te zijn op een strafvorderlijke afdoening. Het ontbreken van een wettelijke regeling voor misdaadanalyse zorgt ervoor, dat veel vragen aangaande het gebruik ervan onbeantwoord blijven. Hoewel de misdaadanalyse als onderzoeksmethode interessante aanknopingspunten biedt voor het dataminingsproces, laat het veel mogelijkheden onbenut. De mogelijkheden van het dataminingsproces zijn talrijker dan die van de operationele analyse, die slechts vijf verschijningsvormen kent. Bovendien zal het dataminingsproces zoals hieronder zal blijken, dankzij het flexibele karakter, gedurende het gehele proces van informatiegaring worden ingezet.

### 3.2.2 Flexibiliteit dataminingsproces

In tegenstelling tot de meeste andere onderzoeksmethoden kan het dataminingsproces naar mijn mening in vrijwel elk stadium van het proces van informatiegaring worden ingezet. Deze uitzonderingspositie ten opzichte van de reguliere opsporingsmethoden is te danken aan het flexibele karakter van het dataminingsproces. Deze is te verklaren uit het feit dat dataminering geen specifieke methode is, maar een proces waaraan gedurende de opsporing op uiteenlopende manieren en op verschillende momenten invulling kan worden gegeven. Of een bepaalde dataminingsvariant al dan niet in een stadium van het proces van informatiegaring mag worden ingezet, hangt voornamelijk af van het doel van

---

10. *Kamerstukken II*, 1996/197, 25 403, nr. 3, p. 123.

11. Het *Rapport Opsporing gezocht* 1994 definieert het begrip opsporingsmethode als: 'Het verzamelen, registreren en verwerken van gegevens en informatie door overheidsorganisaties over (de voorbereiding van) crimineel handelen en criminele organisaties met het doel te komen tot vervolging dan wel tot het voorkomen of beëindigen van crimineel handelen of criminele organisaties'.

het dataminingonderzoek en de mate waarin met het onderzoek een inbreuk op de persoonlijke levenssfeer wordt gemaakt.

*Doelstelling van het dataminingonderzoek*

Het gebruik van opsporingsbevoegdheden draagt bij aan de verbetering van de informatiepositie van politie en justitie. Het flexibele karakter van het dataminingonderzoek maakt een tweeledige doelstelling mogelijk, namelijk een algemene verbetering van de informatiepositie en een strafrechtelijke afdoening. Wanneer de toepassing van dataminingonderzoek kan worden aangemerkt als een niet-ingrijpend middel, behoeft de doelstelling van het gebruik ervan niet primair te zijn gericht op een strafrechtelijke afdoening. Dit is anders wanneer gebruik wordt gemaakt van dataminingonderzoek gedurende het opsporingsonderzoek, waaraan ingrijpendere middelen (opsporingsmethoden) zijn voorbehouden. Dit houdt tevens in dat die middelen alleen zijn toegestaan in het kader van onderzoek dat gericht is op strafrechtelijke afdoening. Het is ongewenst dat ingrijpende onderzoeksmethoden worden ingezet voor onderzoek waaraan nog geen concrete verdenking, dan wel een redelijk vermoeden van georganiseerde criminaliteit, ten grondslag ligt en dat niet dient ter voorbereiding van een strafvorderlijke beslissing<sup>12</sup>. In het verlengde hiervan moeten activiteiten die plaatsvinden in de fase van het opsporingsonderzoek, gericht zijn op het nemen van strafvorderlijke beslissingen<sup>13</sup>. De inzet van zware opsporingsbevoegdheden als geregeld in Boek I, Titel V Sv is niet meer toegestaan wanneer de afdoening van strafbare feiten niet het achterliggende doel is, maar het opbouwen van een goede informatiepositie een doel op zichzelf is geworden<sup>14</sup>. Dat deze meer ingrijpende methoden uitsluitend gebruikt mogen worden ten behoeve van de strafrechtelijke afdoening van delicten en niet ter verbetering van de informatiepositie van politie en justitie in het algemeen, is niet verwonderlijk. Bij het gebruik van deze zware opsporingsmethoden is de verbetering van de informatiepositie een tussengelegen doel, terwijl het primair gaat om een strafvorderlijke afdoening. Wanneer dit andersom was zou de legitimiteit van het gebruik van dergelijke opsporingsmethoden ter discussie komen te staan. Het gebruik van ingrijpende opsporingsmethoden is gebonden aan bepaalde stadia binnen het proces van informatiegaring. Het doel waarvoor deze methoden mogen worden gebruikt is statisch van aard, aangezien zij alleen voor dat doel mogen worden gebruikt. Omdat die doelstelling weer is gelieerd aan bepaalde stadia binnen het proces van informatiegaring, geldt voor de meeste onderzoeksmethoden, dat het gebruik ervan in meerdere stadia van dit proces tegelijkertijd in beginsel is uitgesloten.

---

12. *Kamerstukken II*, 1996/197, 25 403, nr. 3, p. 8-9.

13. *Kamerstukken II*, 1996/197, 25 403, nr. 3, p. 7.

14. *Kamerstukken II*, 1997/198, 25 403, nr. 7, p. 43.

*Ernst van de inbreuk*

Naarmate een onderzoeksmethode ingrijpender van aard is, worden aan het gebruik daarvan hogere eisen gesteld. Dataminingonderzoek dat niet-ingrijpend van aard is kan in beginsel in elk stadium van het proces van informatiegaring worden gebruikt. Hiervoor is geen specifieke wettelijke grondslag vereist, althans geen andere dan die van art. 2 Politiewet 1993. Wanneer er echter sprake is van een ingrijpend middel zijn de aan het gebruik van dat onderzoek gestelde eisen zwaarder. In de praktijk betekent dit, dat de toepassing van meer ingrijpende varianten van het dataminingsproces alleen mogelijk is in de latere stadia van het proces van informatiegaring.

*Van generalis naar specialis*

De verbetering van de informatiepositie en de gerichtheid op een strafrechtelijke afdoening zijn bij het dataminingsproces zeer nauw met elkaar verweven. Wanneer het doel het verkrijgen van een zo goed mogelijke informatiepositie is, dient dit streven uiteindelijk ook een hoger doel, namelijk de afdoening van strafbare feiten. Dit doel wordt ondersteund door de werking van het proces van datamining: van generalis naar specialis. Met het gebruik van dataminingonderzoek wordt in eerste instantie gestreefd naar een optimale informatiepositie die aan de basis ligt van een efficiënte uitvoering van de opsporingstaak. Wanneer uit dat dataminingonderzoek concrete aanwijzingen naar voren komen, kunnen die de aanleiding vormen tot nader onderzoek. Naarmate het onderzoek gericht van aard wordt, verschuift het doel van een verbetering van de algemene informatiepositie in de richting van een strafrechtelijke afdoening. Het doel is dus afhankelijk van het stadium van het proces van informatiegaring waarin het dataminingonderzoek wordt toegepast. Als regel kan worden aangehouden dat, naarmate de aard van de inbreuk die met het verrichten van het dataminingonderzoek gepaard gaat groter is, het doel van het dataminingonderzoek verschuift – althans, dient te verschuiven – van een verbetering van de informatiepositie in de richting van een strafrechtelijke afdoening.

**3.3 Uitgangspunten toepassing dataminingonderzoek**

In de voorgaande sectie is duidelijk gemaakt, dat het dataminingsproces in beginsel in elk stadium van het proces van informatiegaring kan worden toegepast. Alvorens in te gaan op de wijze waarop dit gebeurt, wordt in deze sectie stilgestaan bij de bestaande opvattingen met betrekking tot de invulling van het dataminingonderzoek.

*Wettelijke regeling*

In de huidige situatie is nog geen sprake van een specifieke wettelijke regeling die voorziet in de toepassing van dataminingonderzoek als opsporingsmethode. Met het oog op het verleden<sup>15</sup> dient er met betrekking tot het gebruik van nieuwe onderzoeksmethoden

---

15. In het bijzonder de IRT-affaire.

van uit te worden gegaan, dat het ontbreken van een wettelijke regeling niet impliceert dat het gebruik ervan is toegestaan tot op het moment waarop een wettelijke regeling dat gebruik begrenst. Een opsporingsmethode dient een wettelijke grondslag te hebben wanneer bij de toepassing van die methode sprake is van een inbreuk op de privacy. Een algemene bevoegdheid zoals die van art. 2 Politiewet 1993 volstaat dan niet meer. Wanneer de wijze waarop invulling aan het dataminingsproces wordt gegeven niet (meer) als een niet-ingrijpend middel kan worden aangemerkt, is het gebruik ervan niet zonder meer mogelijk. In dat geval is een nadere legitimatie vereist in de vorm van een wettelijke regeling. Daarbij kunnen beperkingen worden gesteld met betrekking tot de doelgroep of het soort delict. Dit garandeert dat burgers gevrijwaard blijven van politieke bemoeienis indien hun persoon hiertoe geen aanleiding geeft. Het belang van een afbakening van het dataminingsproces door middel van een wettelijke regeling wordt ook onderstreept door de overwegingen hieromtrent van de HR<sup>16</sup>. Naarmate een opsporingsmethode ingrijpender van aard is, worden logischerwijs zwaardere eisen gesteld aan het gebruik ervan. Dit betekent dat ingrijpende methoden, mits gebaseerd op een afdoende formeelwettelijke basis, pas in de latere fasen van de opsporing mogen worden aangewend.

### Onbepaald en bepaald

Voor iedere onderzoeksmethode geldt dat deze dient te passen binnen en dient ter uitvoering van de strafrechtelijke handhaving van de rechtsorde. Tevens moet worden voldaan aan de eisen van proportionaliteit en subsidiariteit. Voor de toepassing van dataminingsonderzoek is in de Nota WES afzonderlijk nog een aantal uitgangspunten neergelegd. Onder datamining verstaat de wetgever het geautomatiseerd doorzoeken van zeer grote gegevensbestanden op specifieke kenmerken en het combineren van gegevens die verspreid in bestanden zijn opgeslagen. Het betreft een analyse van gegevens in een database met speciale programmatuur die naar anomalieën, trends of bepaalde kenmerken zoekt<sup>17</sup>. Voor het gebruik van dataminingsonderzoek als onderzoeksmethode wordt bepaald, dat in de wetgeving aangaande het bevragen van bestanden steeds een onderscheid dient te worden gemaakt tussen:

1. het bevragen op een bepaalde persoon, en
2. het bevragen op een op voorhand onbepaalde groep van personen (hetgeen wordt aangeduid met de term datamining)<sup>18</sup>.

Uit de definitie van datamining in de Nota WES kan worden opgemaakt, dat de Nederlandse wetgever datamining ziet als een verwerking (en niet alleen maar als een bewerking) van gegevens. In combinatie met het voorgaande lijkt de wetgever het data-

16. Dit betreft de brede toepassingsmogelijkheden die kenmerkend zijn voor nieuwe opsporingsmethoden en -technieken als het dataminingsproces.

17. *Kamerstukken II*, 1997/98, 25 880, nrs. 1-2, p. 30 en 42.

18. *Kamerstukken II*, 1997/98, 25 880, nrs. 1-2, p. 83.

miningsproces uit te leggen als het bevragen van een op voorhand onbepaalde groep van personen. Dit betekent dat het bevragen van bestanden op één bepaalde persoon of een bepaalde groep van personen volgens de letter van de Nota WES niet als dataminingsonderzoek wordt aangemerkt. Praktisch gezien is het denkbaar dat deze twee vormen van bevragen echter wel tot de mogelijkheden van het dataminingsproces worden gerekend; daarnaast is het ook technisch mogelijk een dergelijk dataminingsonderzoek uit te voeren. Met het oog op de perspectieven die deze vormen van bevragen de opsporingspraktijk kunnen bieden is het de vraag of het standpunt in de Nota WES met betrekking tot de invulling van het dataminingsbegrip niet te beperkend is. Voor een antwoord daarop is het raadzaam te onderzoeken welke motivering de Nota WES ten grondslag legt aan deze stellingname.

De beslissing om het bevragen op een bepaalde persoon of een bepaalde groep van personen niet als datamining te kwalificeren kan zowel op technische als op juridische gronden zijn genomen. In dit geval blijkt een juridische motivering ten grondslag te liggen aan het onderscheid dat wordt gemaakt tussen het bevragen van een op voorhand onbepaalde groep van personen en het bevragen op één bepaalde persoon. Volgens de Nota WES is dit onderscheid onder meer van belang, omdat aan datamining ten aanzien van een op voorhand onbepaalde groep van personen veel verdergaande beperkingen aan het zoeken dienen te worden gesteld dan wanneer het een enkele persoon betreft<sup>19</sup>. Omdat het mogelijk wordt gegevens te vergelijken en kennis te vergaren van (grote groepen) personen ten aanzien waarvan geen feiten of omstandigheden bekend zijn dat zij zich bezighouden met strafbare feiten, gaat het om een ingrijpende bevoegdheid. Bovendien zou een dergelijke bevoegdheid, meer dan individuele bevestigingen, afbreuk doen aan het beginsel dat registers slechts voor een specifiek doel worden aangelegd en in stand gehouden (de doelbinding). Het onderscheid dat in de Nota WES wordt gemaakt is dus gebaseerd op de mate van inbreuk die het bevragen (het doen van dataminingsonderzoek) met zich meebrengt op de fundamentele rechten van de burger. Om het belang van de bescherming van die rechten te onderstrepen, worden twee verschillende vormen van bevragen onderscheiden. Hiermee wil men duidelijk maken dat in het ene geval strengere eisen aan het gebruik van datamining dienen te worden gesteld dan in het andere. Met het oog op de voortschrijdende technologische ontwikkelingen en de daarmee gepaard gaande mogelijkheden om inbreuk te maken op de fundamentele rechten van de burger acht de regering dit noodzakelijk, teneinde een aanvaardbaar niveau van rechtsbescherming te kunnen waarborgen.

Vanuit deze optiek behoeft het onderscheid dat in de Nota WES wordt gemaakt niet per definitie een begrenzing te betekenen van het aantal mogelijke toepassingsvarianten van

---

19. *Kamerstukken II, 1997/98, 25 880, nrs. 1-2, p. 83.*

het dataminingsproces. In plaats daarvan kan het worden uitgelegd als een beperking van de situaties waarbij het gebruik van die varianten mogelijk is. Nu het dataminingsproces bevragingen ten aanzien van één bepaalde persoon of bepaalde groepen van personen in praktische en in technische zin niet uitsluit, kan in beginsel de mogelijkheid worden opengelaten om deze vormen van bevragen ook in juridische zin als dataminingsvarianten aan te merken. Wanneer daarbij wordt uitgegaan van het standpunt dat op de verschillende vormen van bevragen<sup>20</sup> verschillende voorwaarden van toepassing dienen te zijn, wordt in beginsel geen afbreuk gedaan aan hetgeen wordt gesteld in de Nota WES.

Voor een uitputtend onderzoek van het dataminingsproces bleek het gewenst aan het begrip datamining een ruimere betekenis toe te kennen dan in de Nota WES wordt voorgestaan; daarbij wordt tevens rekening gehouden met de stand van de techniek. Later in het onderzoek wordt ingegaan op de vraag, of het bevragen van bestanden op een bepaalde persoon of groep van personen ook daadwerkelijk als dataminingsonderzoek in juridische zin dient te worden aangemerkt.

#### *Datamining als opsporingsmiddel*

Voor het gebruik van datamining als opsporingsmiddel stelt de Nota WES dat onderzoek naar en verwerken van gegevens in dat kader slechts toelaatbaar is bij een verdenking of een verkennend onderzoek, danwel bij een onderzoek naar georganiseerde criminaliteit zonder dat er sprake is van een concrete verdenking<sup>21</sup>. Dataminingsonderzoek als opsporingsmethode is ingrijpend van aard en dient te zijn gericht op een strafvorderlijke afdoening. Dit sluit niet uit dat de toepassing daarvan ook in het eerste stadium van het proces van informatiegaring mogelijk is. In dat geval wordt het niet bestempeld als opsporingsmiddel maar als onderzoeksmethode, waarbij het onderzoek niet gericht hoeft te zijn op een strafvorderlijke afdoening. Een dataminingsonderzoek behoeft immers niet per definitie een ingrijpend middel te zijn.

### **3.4 Van dataminingsproces naar onderzoeksmethode**

De essentie van het dataminingsproces is het ontdekken (het minen) van nieuwe kennis. Uit het proces van informatiegaring blijkt, dat dit tevens de essentie is van het opsporen als geheel. In het kader van de opsporingstaak wordt door politie en justitie steeds gestreefd naar een gegevensoptimalisering. In het kader daarvan kunnen gedurende de drie stadia van het proces van informatiegaring allerhande onderzoeksmethoden worden gehanteerd. Daarbij kan het onder meer gaan om het ondervragen van verdachten of om het onderzoek op de plaats delict. De inzet van deze methoden heeft tot gemeenschappe-

---

20. Of de verschillende manieren waarop uitvoering aan het dataminingsproces kan worden gegeven.

21. *Kamerstukken II, 1997/198, 25 880, nrs. 1-2, p. 197.*

lijk doel het vergaren van nieuwe kennis ten behoeve van de opsporing. Het dataminingsproces zelf omvat geen specifieke onderzoeksmethode. Pas op het moment dat concreet invulling aan dit proces wordt gegeven, kan worden gesproken van een onderzoeksmethode. Voor een juridische inkadering van het dataminingsproces wordt de overgang van het dataminingsproces naar datamining als onderzoeksmethode beschreven, waarbij een moeilijk grijpbaar technisch begrip als datamining terug moest worden gebracht tot juridisch bruikbare stadia. Daartoe worden de manieren (dataminingvarianten) waarop uitvoering aan het proces kan worden gegeven onderscheiden. Het dataminingsproces kan worden onderverdeeld in drie varianten, namelijk het ongericht dataminingonderzoek, het gericht dataminingonderzoek en de verificatie<sup>22</sup>. Bij een dataminingonderzoek in het kader van de opsporing zal in beginsel steeds een bewerking plaatsvinden van generalis naar specialis. Uit input wordt output gegenereerd; de output kan worden gebruikt voor een eventueel vervolgonderzoek, waarbij de volgorde van ongericht onderzoek naar verificatie de meest logische is. In het navolgende wordt stilgestaan bij elk van de drie verschillende dataminingvarianten.

#### *3.4.1 Het ongerichte dataminingonderzoek*

Dataminingonderzoek kan worden gebruikt ter verbetering van de informatiepositie. Dit maakt het mogelijk om gegevens uit een bepaald register, gegevens binnen een politiekorps of zelfs de gegevensverzamelingen van de verschillende landelijke politiekorpsen zo optimaal mogelijk (uitputtend) te benutten. Gefragmenteerde of onvolledige gegevens kunnen worden gecombineerd en aangevuld en uit het geheel van gegevens kan met behulp van dataminingonderzoek verborgen kennis in de vorm van bijvoorbeeld patronen en verbanden zichtbaar worden gemaakt. In de praktijk kan hierbij onderscheid worden gemaakt tussen een verbetering van de algemene informatiepositie en een verbetering van de informatiepositie in een bepaald geval. Indien het gaat om een verbetering van de algemene informatiepositie kan gebruik worden gemaakt van ongericht dataminingonderzoek.

Bij een ongericht dataminingonderzoek bestaat nog geen verdenking van een strafbaar feit en ook niet een redelijk vermoeden van het beramen of plegen van ernstige misdrijven in georganiseerd verband. Er is nog geen sprake van opsporing; het ongerichte dataminingonderzoek vindt plaats in het kader van de strafrechtelijke handhaving van de rechtsorde. In tegenstelling tot de hierna te bespreken gerichte dataminingvariant ligt de nadruk bij dit onderzoek op gegevens die al binnen het politieapparaat aanwezig zijn en niet op operationele<sup>23</sup> gegevens. De uitkomsten van ongericht dataminingonderzoek

---

22. Verificatie is niet zozeer een afzonderlijke variant van het dataminingproces maar geeft aan wanneer dit proces eindigt.

23. Operationele gegevens hebben betrekking op een lopende zaak.

kunnen de aanzet vormen tot of bijdragen aan nieuw, respectievelijk lopend onderzoek. In het eerste geval zal het vervolgonderzoek in beginsel een gericht karakter hebben. Ook het omgekeerde is denkbaar, waarbij het resultaat van gericht dataminingonderzoek wordt gebruikt ten behoeve van ongericht dataminingonderzoek. De mogelijkheid tot dergelijk (her)gebruik is afhankelijk van de wettelijke beperkingen die daarop van toepassing (dienen te) zijn. In het hiernavolgende worden de kenmerken van een ongericht dataminingonderzoek aan de orde gesteld.

#### **Algemene doelstelling**

Het ongerichte dataminingonderzoek kan worden gebruikt ten behoeve van een verbetering van de algemene informatiepositie. Het verkrijgen en het handhaven van een goede informatiepositie vormen de basis voor een succesvolle uitvoering van de opsporingstaak. Een ongericht dataminingonderzoek is, zoals de naam aangeeft, in beginsel ongericht en algemeen van aard. Er wordt niet gezocht naar aanleiding van een bepaalde zaak of persoon. Het doel van het onderzoek in deze fase van het dataminingsproces is gericht op een algemene verbetering van de informatiepositie van één of meer (politie)registers.

#### **Inbreuk op de privacy**

Het opbouwen en in stand houden van een zekere informatiepositie door middel van een ongericht dataminingonderzoek is alleen toegestaan wanneer dit dient ter uitvoering van de politietask en wordt voldaan aan eisen van proportionaliteit en subsidiariteit<sup>24</sup>. Overeenkomstig het standpunt hieromtrent in de Nota WES<sup>25</sup> dient het gebruik van ongericht dataminingonderzoek aan strengere voorwaarden te worden gebonden dan de overige toepassingsvarianten van het dataminingsproces. De reden daarvan is dat in beginsel gebruik kan worden gemaakt van een onbeperkte hoeveelheid bronnen die betrekking kunnen hebben op een onbepaalde groep van personen. Bij een ongericht dataminingonderzoek is nog geen sprake van een verdenking van een strafbaar feit, noch van een vermoeden van het beramen of plegen van ernstige misdrijven in georganiseerd verband. Dit brengt beperkingen met zich mee voor het doen van een ongericht dataminingonderzoek. Omdat het onderzoek plaatsvindt in het kader van een verbetering van de algemene informatiepositie voordat er sprake is van opsporing, dient te worden voorkomen dat opsporingsinstanties actief onschuldige burgers onderwerp maken van onderzoek zonder dat daarvoor een directe aanleiding bestaat. Handelingen die plaatsvinden in het kader van een ongericht dataminingonderzoek mogen in beginsel niet leiden tot een ontoelaatbare inbreuk op de privacy. Daarom is het gebruik van dwangmiddelen in het kader van een ongericht dataminingonderzoek niet toegestaan.

---

24. *Kamerstukken II*, 1996/97, 25 403, nr. 3, p. 9.

25. *Kamerstukken II*, 1997/98, 25 880, nrs. 1-2, p. 83.

De mogelijkheden voor opsporingsautoriteiten bij het doen van een ongericht dataminingonderzoek betreffen in beginsel het opslaan, bewerken, gebruiken en analyseren van (al aanwezige) gegevens, of het vergaren van gegevens door de toepassing van niet-ingrijpende middelen. Registratie in een politieregister rechtvaardigt in beginsel dat deze gegevens worden gebruikt ten behoeve van (onggericht) dataminingonderzoek binnen het opsporingsapparaat. Hoewel een verwerking van deze gegevens uit een reeds bestaand politieregister een inbreuk op de persoonlijke levenssfeer met zich meebrengt, is deze in beginsel steeds toelaatbaar. Het gebruik van niet-ingrijpende middelen is toegestaan wanneer daarmee geen ontoelaatbare inbreuk op de privacy wordt gemaakt en dit past binnen en dient ter uitvoering van de politietaak met betrekking tot de strafrechtelijke handhaving van de rechtsorde. Wanneer het gebruik van dataminingonderzoek als een niet-ingrijpend middel kan worden aangemerkt, behoeft het doel niet primair gericht te zijn op een strafrechtelijke afdoening<sup>26</sup>. Als leidraad kan worden aangehouden dat sprake is van een niet-ingrijpend middel wanneer de toepassing ervan past binnen de reikwijdte van art. 2 Politiewet 1993. Wanneer een wettelijke regeling aan de toepassing van een middel ten grondslag ligt, kan niet worden gesproken van een niet-ingrijpend middel. Het feit dat de wetgever een wettelijke verankering nodig heeft geacht, geeft al aan dat het daarbij in beginsel steeds gaat om een ingrijpende bevoegdheid. De beperking tot niet-ingrijpende middelen garandeert dat burgers gevrijwaard blijven van politieke bemoeienis indien hun persoon daartoe geen aanleiding geeft<sup>27</sup>. Opgemerkt zij dat, in het geval de toepassing van een ingrijpend middel is gebaseerd op een wettelijke grondslag, dit niet per definitie betekent dat sprake is van een ontoelaatbare inbreuk op de persoonlijke levenssfeer. Hoewel het gebruik van een ingrijpend middel in bepaalde gevallen daarom ook in het kader van ongericht dataminingonderzoek mogelijk zal zijn, is het gebruik ervan over het algemeen voorbehouden aan de latere stadia van het proces van informatiegaring. Dit hangt onder meer samen met het doel van de ongerichte dataminingvariant, waarbij zo breed mogelijk wordt gezocht zonder dat daarbij wordt uitgegaan van een concrete aanwijzing of verdenking.

### Duur van het onderzoek

Het ongerichte dataminingonderzoek wordt gebruikt ter verbetering en instandhouding van de informatiepositie in het algemeen. De noodzaak van een zo goed mogelijke informatiepositie is constant aanwezig en ligt aan de basis van een succesvolle opsporing. Met het oog hierop heeft deze variant van het dataminingsproces een permanent karakter. Het is niet alleen van belang om een goede informatiepositie te verkrijgen, maar evenzeer om deze te handhaven.

---

26. Dit lijdt uitzondering indien het dataminingonderzoek wordt toegepast gedurende het opsporingsonderzoek. Het is in dat geval echter onwaarschijnlijk dat het nog om een niet-ingrijpend middel gaat.

27. *Kamerstukken II*, 1996/97, 25 403, nr. 3, p. 8.

### **Gebruik externe gegevens**

Bij een ongericht dataminingonderzoek dient terughoudend te worden omgegaan met het gebruik van externe gegevens. Dit geldt voor de gegevens die afkomstig zijn van buiten het politieke apparaat en in mindere mate ook voor de gegevens die al (elders) binnen het politieapparaat aanwezig zijn. In tegenstelling tot de gerichte dataminingvariant ligt de nadruk op gegevens die al binnen het politieapparaat aanwezig zijn en niet op operationele gegevens. Uitgangspunt is een zo goed mogelijke benutting van de aanwezige gegevens. Hoewel externe gegevens daaraan een bijdrage kunnen leveren, is het gebruik ervan geen hoofdzaak. Aan deze terughoudende opstelling liggen verschillende redenen ten grondslag. De belangrijkste is de bescherming van de persoonlijke levenssfeer, zoals hierboven is uiteengezet. Met het gebruik van externe gegevens mag geen ontoelaatbare inbreuk op de persoonlijke levenssfeer worden gemaakt. Bij een ongericht dataminingonderzoek wordt in beginsel nog niet specifiek in een bepaalde richting gezocht, waardoor geen mogelijkheid bestaat van een gericht gebruik van externe gegevens. Verder zal (mede vanwege de voorgaande reden) niet steeds kunnen worden gesproken van een noodzaak<sup>28</sup> om bepaalde externe gegevens te gebruiken; die noodzaak is daarvoor evenwel een minimumvoorwaarde.

### **Resumerend**

Uit het voorgaande blijkt dat met betrekking tot een ongericht dataminingonderzoek een aantal kenmerken kan worden onderscheiden:

- het doel is algemeen en ongericht van aard;
- er vindt geen ontoelaatbare inbreuk op de privacy plaats;
- gegevensvergaring door middel van niet-ingrijpende middelen vindt alleen plaats voor zover daarmee geen inbreuk op de privacy wordt gemaakt;
- het dataminingonderzoek is in beginsel permanent van aard;
- er is een terughoudende<sup>29</sup> opstelling bij het zoeken naar en het gebruiken van externe gegevens;
- het onderzoek richt zich primair op al aanwezige gegevens.

#### *3.4.2 Het gerichte dataminingonderzoek*

Met behulp van dataminingonderzoek kan ook worden gestreefd naar een specifieke verbetering van de informatiepositie. In dat geval is sprake van een gericht dataminingonderzoek. Het gaat om een gerichte verbetering van de informatiepositie, waarbij het onderzoek betrekking heeft op een bepaalde zaak of een bepaalde groep van personen. Het kan bijvoorbeeld gaan om het oplossen van een moordzaak of de opsporing en

---

28. Art. 4 WPolr.

29. Proportionaliteit en subsidiariteit.

bestrijding van een bepaald crimineel verband van personen. In dat kader kan eveneens worden gesproken van ‘de politietaak in een bepaald geval’, zoals bedoeld in art. 1 lid 1 onder *j* WPolr. Een gericht dataminingonderzoek vindt plaats in het kader van de strafrechtelijke handhaving van de rechtsorde. Het verschil met de ongerichte dataminingvariant is, dat in het laatste geval wel sprake kan zijn van opsporing. Bij een gericht dataminingonderzoek ligt de nadruk niet zozeer meer op een verbetering van de informatiepositie in het algemeen, maar is het zwaartepunt verschoven naar een strafvorderlijke afdoening. De aanleiding tot het doen van een gericht dataminingonderzoek kan voortkomen uit het resultaat van ongericht dataminingonderzoek, maar evenzeer uit een binnengekomen tip. In het hiernavolgende wordt nader ingegaan op de kenmerken van een gericht dataminingonderzoek.

### **Gerichte doelstelling**

Deze variant van het dataminingsproces kan als gericht worden aangemerkt, omdat er sprake is van een verdenking of aanwijzing die aan het onderzoek ten grondslag ligt. Het onderzoek is toegespitst op een situatie of groep van personen ten aanzien waarvan een bepaalde mate van verdenking is gerezen en is bedoeld om daaromtrent meer inzicht of bijzonderheden te verschaffen. Een gericht dataminingonderzoek kan, naast een verbetering van de informatiepositie, ook zien op een strafvorderlijke afdoening. Kenmerkend voor het dataminingsproces is dat het doel van het onderzoek zich in de latere fasen van het dataminingsproces verlegt van een algemene verbetering van de informatiepositie naar een strafrechtelijke afdoening.

### **Inbreuk op de privacy**

In het kader van een gericht dataminingonderzoek is theoretisch een grotere inbreuk op de rechten van de burger toegestaan dan bij de ongerichte dataminingvariant. Afhankelijk van de omstandigheden behoort daarbij ook het gebruik van zwaardere opsporingsmethoden tot de mogelijkheden. Naarmate het onderzoek vordert, zal de ingezette dataminingvariant ingrijpender van aard (kunnen) zijn. De inbreuk op de persoonlijke levenssfeer die dit met zich meebrengt, wordt in beginsel steeds gelegitimeerd door een wettelijke grondslag. Naarmate een middel ingrijpender van aard is, stelt de wet striktere voorwaarden aan het gebruik ervan. Omdat bij een gericht dataminingonderzoek al sprake is van een bepaalde mate van verdenking, is een grotere inbreuk op de privacy toegestaan. Hoe groot deze inbreuk precies mag zijn, is afhankelijk van de mate van verdenking. De wettelijke beperking van het gebruik van ingrijpende middelen resulteert voor de toepassing van de gerichte dataminingvariant in een afbakening van het onderzoeksgebied en de doelgroep.

Toepassing van een bijzondere opsporingsbevoegdheid is alleen toegestaan in het belang van het onderzoek en dient gericht te zijn op het nemen van strafvorderlijke beslissingen. Dit sluit niet uit dat zeer veel gebruik van opsporingsbevoegdheden mede bijdraagt tot

een verbetering van de informatiepositie van politie en justitie. Het verbeteren van de informatiepositie als tussengelegen doel wordt in Titel V Sv ook erkend. Dit onderzoek is gericht op het in kaart brengen van het georganiseerd verband, teneinde de feiten en verdachten te kunnen selecteren die moeten worden vervolgd. Het uiteindelijke doel van dit in kaart brengen is het berechten van personen die strafbare feiten hebben gepleegd. Zeker in de aanvang van dit onderzoek kan dat doel echter nog ver verwijderd zijn. De grens wordt overschreden wanneer de afdoening van strafbare feiten niet het achterliggende doel is, maar dat het opbouwen van een informatiepositie doel in zichzelf is<sup>30</sup>.

#### **Duur van het onderzoek**

Een gericht dataminingonderzoek wordt uitgevoerd ten behoeve van een concrete zaak, ofwel de operationele opsporing, en heeft in beginsel steeds een tijdelijk karakter. Op het moment dat het doel van het onderzoek wordt bereikt, loopt het daarmee tevens ten einde.

#### **Gebruik van externe gegevens**

Een gericht dataminingonderzoek ziet in beginsel niet op de verbetering van de algemene informatiepositie (van een register) waarover men reeds beschikt. Het betreft een nieuw onderzoek waaraan men in beginsel met een schone lei begint. Bij dit onderzoek, gericht op het verkrijgen van meer inzicht in een bepaalde zaak of omtrent een bepaalde groep van personen, ligt de nadruk in eerste instantie op het vergaren van zoveel mogelijk gegevens die een positieve bijdrage kunnen leveren aan het onderzoek. Daarbij kan het gaan om gegevens die al in de politieregisters aanwezig zijn, maar ook om gegevens die zich buiten de politieke sfeer bevinden. De mogelijkheden daartoe zijn bij een gericht dataminingonderzoek veel ruimer dan bij een ongericht dataminingonderzoek omdat er al sprake is van vermoedens, c.q. een bepaalde mate van verdenking. Omdat bij aanvang van een gericht dataminingonderzoek nog nauwelijks of geen informatie voorhanden is, ligt de nadruk op het gebruik van externe gegevens. Naarmate het gerichte dataminingonderzoek vordert en wanneer voldoende informatie is verzameld, gaat dit zwaartepunt een andere richting uit; aan de hand van een bewerking van de verzamelde gegevens wordt dan namelijk getracht het doel van het gerichte dataminingonderzoek te bereiken. Op dat moment concentreert het onderzoek zich vooral op de tot dan toe verzamelde informatie en is de noodzaak tot het verzamelen van nieuwe gegevens minder prominent aanwezig.

#### **Resumerend**

Gezien het voorgaande kunnen met betrekking tot een gericht dataminingonderzoek de volgende kenmerken worden onderscheiden:

---

30. *Kamerstukken II, 1997/198, 25 403, nr. 7, p. 43.*

- het doel is gericht van aard;
- er vindt geen ontoelaatbare inbreuk op de privacy plaats;
- de mogelijkheden tot gegevensvergaring zijn ruimer<sup>31</sup> nu het gerichte karakter een verdergaande inbreuk op de privacy rechtvaardigt;
- het dataminingonderzoek is in beginsel tijdelijk van aard;
- er kan actief gebruik worden gemaakt van externe gegevens;
- het onderzoek richt zich in eerste instantie op externe gegevens.

### 3.4.3 Verificatie

De derde variant die binnen het dataminingsproces kan worden onderscheiden is die van verificatie. Strikt genomen betreft verificatie eigenlijk de begrenzing van het dataminingsproces en kan als zodanig niet als onderzoek worden aangemerkt. Van dataminingonderzoek is namelijk alleen sprake indien wordt gezocht naar nieuwe kennis; op het moment van verificatie is die kennis echter al gevonden. Niet het ontdekken van nieuwe kennis staat centraal, maar het verifiëren van al gevonden kennis. Bij de verificatie wordt bijvoorbeeld gezocht naar bevestigende informatie in verschillende geautomatiseerde bestanden of kan het gevonden resultaat worden getoetst door het plegen van huiszoeking bij de betreffende verdachte. Van verificatie is in beginsel sprake wanneer wordt gezocht op een specifieke naam. Voor het onderscheid tussen het gerichte dataminingonderzoek en verificatie is het van belang vast te stellen, wat in een bepaald geval de aanleiding is tot het bevragen van bestanden op een specifiek criterium. Uitgaande van een omstandigheid waarin het criterium waarop wordt gezocht een bepaalde naam is zijn twee situaties denkbaar, namelijk die van verificatie en die van gericht dataminingonderzoek.

Voor het eerstgenoemde criterium suggereert de term verificatie een voorafgaand onderzoek. In dit geval kan het bevragen van bestanden op één specifieke naam worden aangemerkt als een vervolg op het dataminingonderzoek, waarbij (meestal naar aanleiding van de tijdens het gerichte dataminingonderzoek gevonden resultaten) gericht verder wordt gezocht. Omdat de gevonden naam dus het resultaat is van eerder (datamining)onderzoek is er sprake van een door feiten onderbouwde verdenking tegen deze persoon. Daarom wordt niet meer gezocht naar nieuwe feiten en wordt dus afgeweken van het gebruikelijke patroon ‘van generalis naar specialis’; wanneer wordt gezocht op een bepaalde naam is het uitgangspunt immers al een specialis. Het onderzoek is gericht op het verkrijgen van zekerheid over het tot dan toe gevonden resultaat, de verificatie.

Het tweede criterium kan betrekking hebben op een situatie, waarbij de aanleiding tot het bevragen van bestanden op een bepaalde persoon niet het resultaat is van vooraf-

---

31. In vergelijking met het ongerichte dataminingonderzoek.

gaand dataminingonderzoek. Daarvan kan bijvoorbeeld sprake zijn wanneer bij de politie een tip binnenkomt betreffende een bepaalde persoon. In de meeste gevallen zal dan de behoefte bestaan om eerst uitvoeriger onderzoek te doen teneinde meer informatie en aanknopingspunten te verzamelen. Hiervoor kan mogelijk gebruik<sup>32</sup> worden gemaakt van (on)gericht dataminingonderzoek. In plaats van naar een specialis toe te werken wordt vanuit een specialis (een bepaalde persoon) toegewerkt naar een generalis. Om de verdenking tegen deze persoon te staven is additionele informatie nodig, welke kan worden verkregen door het verrichten van (on)gericht dataminingonderzoek. Behalve voor het verkrijgen van aanvullende informatie in deze situatie kan de stap naar het gerichte dataminingonderzoek ook worden gemaakt om bijvoorbeeld een vermeend crimineel netwerk rond een bepaalde persoon bloot te leggen. Alvorens mag worden overgegaan tot verificatie en het daarmee gepaard gaande gebruik van zwaardere opsporingsmethoden dient sprake te zijn van een redelijke verdenking. Deze kan worden verkregen uit het resultaat van een gericht dataminingonderzoek.

Een stap terug in het dataminingsproces doet in zekere zin ook in een vorm van verificatie belanden, namelijk de verificatie van aanwijzingen die nog geen concrete verdenking vormen. Het karakter van de informatie die in dat geval wordt geverifieerd wijkt echter af van dat van de informatie, die onderwerp uitmaakt van verificatie als variant van het dataminingsproces. Verificatie van dergelijke aanwijzingen vindt plaats met het oog op het verkrijgen van kennis. De verificatie waarmee de derde toepassingsvariant van het dataminingsproces wordt aangeduid vindt plaats met het oog op een verificatie van al gevonden kennis. Die kennis is inmiddels zodanig gericht van aard dat voldoende grondslag wordt geboden voor een concrete verdenking. Dit betekent dat mogelijk ook het gebruik van zwaardere opsporingsmethoden is toegestaan, terwijl dit bij de verificatie van aanwijzingen die nog geen concrete verdenking vormen in beginsel niet het geval is. Om dit onderscheid in de mate van verdenking en de daarmee samenhangende bevoegdheden duidelijk te maken, wordt bij het verifiëren van aanwijzingen gesproken van ‘gericht dataminingonderzoek’ en niet van ‘verificatie’.

In conclusie dient het bevragen van bestanden op een bepaalde persoon te worden aange-merkt als (on)gericht dataminingonderzoek wanneer een stap wordt teruggedaan in het dataminingsproces. Wanneer nader onderzoek niet nodig is kan worden gesproken van verificatie. Bij de vaststelling van het type variant is de mate van verdenking in beginsel doorslaggevend. De verdenking is over het algemeen sterker wanneer deze voortvloeit uit voorafgaand dataminingonderzoek.

---

32. Opgemerkt zij dat een enkele tip niet per definitie een gericht dataminingonderzoek rechtvaardigt. Zie hiervoor ook *Kamerstukken II*, 1996/97, 25 398, nr. 3, p. 19-20.

#### 3.4.4 Schema van de drie stadia van het dataminingsproces als opsporingsmethode

Om aan te geven op welke wijze het dataminingsproces kan worden gehanteerd als opsporingsmethode is het onderverdeeld in drie stadia. Bij het maken van onderscheid is de mate van verdenking die op een bepaald moment bestaat een bepalende factor gebleken. In onderstaand schema (schema 3) is weergegeven hoe het dataminingsproces zich verhoudt tot de behoefte aan nadere informatie. Kenmerkend voor een ongericht dataminingsonderzoek is dat in beginsel nog geen sprake is van een verdenking of zelfs van aanwijzingen. Bij een gericht dataminingsonderzoek dient in ieder geval sprake te zijn van een bepaalde mate van verdenking. Op het moment van verificatie is er sprake van een concrete verdenking jegens een bepaalde persoon.

	Ontdekken		Toetsing
<b>Dataminingsproces</b>	Onggericht dataminingsonderzoek	Gericht dataminingsonderzoek	Verificatie
<b>Aanknopingspunten</b>	Geen verdenking	⇐ Overgang* ⇒	Verdachte

\* De wet spreekt van aanwijzingen en redelijk vermoeden.

#### Schema 3 Het dataminingsproces

Nu het dataminingsproces in een juridisch werkbaar kader is geplaatst zal in de volgende sectie worden ingegaan op de vraag hoe de verschillende fasen van het dataminingsproces zich verhouden tot het proces van informatiegaring. Zo kan worden vastgesteld wanneer en op welke wijze opsporingsautoriteiten ten behoeve van de opsporingstaak gebruik kunnen maken van dataminingsonderzoek.

### 3.5 De toepassingsvarianten van het dataminingsproces en het proces van informatiegaring

Het proces van politieke informatiegaring is onderverdeeld in drie verschillende juridische stadia, te weten het stadium waarin sprake is van het opbouwen en in stand houden van een zekere informatiepositie, het verkennend onderzoek en het opsporingsonderzoek. Het dataminingsproces als geheel kan in ieder stadium van het proces van informatiegaring worden gebruikt. Met betrekking tot de afzonderlijke dataminingsvarianten is dit niet het geval. Voor een compleet beeld van het gebruik van dataminingsonderzoek binnen het proces van informatiegaring wordt onderzocht hoe de drie varianten van het dataminingsproces zich verhouden ten opzichte van de drie stadia van het proces van informatiegaring. Zo kan, vooruitlopend op een wettelijke regeling voor het politieke gebruik van het dataminingsproces, worden vastgesteld in welk stadium van welke variant gebruik kan worden gemaakt. Daarbij neemt het legitimiteitsvraagstuk met betrekking tot de methoden die kunnen worden ingezet ter verbetering van de informatiepositie van politie en justitie een centrale plaats in.

### *3.5.1 Het ongerichte dataminingonderzoek*

In sectie 3.4.1 zijn de kenmerken beschreven van een ongericht dataminingonderzoek. Deze dataminingvariant kenmerkt zich onder meer door een sterk informatief karakter, waardoor het goede diensten kan bewijzen bij het opbouwen en verbeteren van de informatiepositie van politie en justitie. De (on)mogelijkheden van een ongericht dataminingonderzoek worden grotendeels bepaald door het spanningsveld tussen het opsporings- en het privacybelang. Aan een ongericht dataminingonderzoek ligt nog geen concrete verdenking ten grondslag, hetgeen betekent dat niet specifiek in een bepaalde richting wordt gezocht. Met het oog hierop dient te worden voorkomen dat burgers onderwerp van politieke activiteiten worden zonder dat zij daartoe aanleiding hebben gegeven. Het mag niet zo zijn dat ten behoeve van de algemene verbetering van de informatiepositie een inbreuk wordt gemaakt op fundamentele rechten van de burger, zonder dat daarvoor wettelijke grondslag aanwezig is. In het kader van een ongericht dataminingonderzoek mag geen sprake zijn van het actief verzamelen van externe gegevens (verzamelingen) met het doel deze te analyseren op allerlei mogelijke criminele gedragingen. Opsporingsinstanties zullen zich met een ongericht dataminingonderzoek vooral dienen te richten op de reeds aanwezige informatie, waarbij de nadruk ligt op verbetering van de algemene informatiepositie.

#### *3.5.1.1 Terugkoppeling naar het proces van informatiegaring*

Het eerste type onderzoek dat binnen het proces van informatiegaring wordt onderscheiden omvat het opbouwen en in stand houden van een zekere informatiepositie door het opslaan, bewerken, gebruiken en analyseren van gegevens of het vergaren van gegevens door de toepassing van niet-ingrijpende middelen. Met het oog op de kenmerken van een ongericht dataminingonderzoek lijkt dit type een goede basis te bieden voor de toepassing van deze dataminingvariant. Het in het belang van de strafrechtelijke handhaving van de rechtsorde opbouwen en in stand houden van een goede informatiepositie ligt ten grondslag aan het proces van informatiegaring. Net als bij de toepassing van de ongerichte dataminingvariant ligt de nadruk in het eerste stadium van de opsporing op een verbetering van de algemene informatiepositie door middel van een zo optimaal mogelijk gebruik van de voorhanden zijnde informatie. Hierbij wordt nog niet gezocht naar aanleiding van een concrete verdenking of een bepaalde zaak. Hoewel passief gebruik kan worden gemaakt van externe gegevens mag dit niet resulteren in een ontoelaatbare inbreuk op de persoonlijke levenssfeer. Samenvattend blijkt een ongericht dataminingonderzoek een goede manier om uitvoering te geven aan het eerste stadium van het proces van informatiegaring.

#### *3.5.1.2 Verkennend onderzoek en opsporingsonderzoek*

De mogelijkheid tot het verrichten van ongericht dataminingonderzoek blijft in beginsel beperkt tot het eerste stadium van het proces van informatiegaring. De toepassing van een ongericht dataminingonderzoek gedurende het stadium van het verkennend onder-

zoek of het opsporingsonderzoek lijkt niet mogelijk. Het karakter van een ongericht dataminingonderzoek gaat niet samen met het gerichte karakter dat kenmerkend is voor zowel het verkennend onderzoek als het opsporingsonderzoek. Ook dienen activiteiten die plaatsvinden in het kader van het opsporingsonderzoek te zijn gericht op een strafvorderlijke afdoening. Het is onwaarschijnlijk dat hiervan sprake is bij de toepassing van een ongericht dataminingonderzoek. In het kader van een ongericht dataminingonderzoek kan in beginsel geen gebruik worden gemaakt van zwaardere opsporingsmethoden, terwijl hieraan wel degelijk behoefte kan bestaan in het kader van een verkennend onderzoek in de zin van art. 126<sup>gg</sup> Sv of een opsporingsonderzoek overeenkomstig art. 132<sup>a</sup> Sv.

### Resumerend

De toepassing van ongericht dataminingonderzoek is in beginsel alleen mogelijk gedurende het eerste stadium van de politieke informatiegaring. Het onderzoek is niet beperkt tot bepaalde strafbare gedragingen, maar kan bijdragen aan een verbetering van de informatiepositie in de meest ruime zin. Het onderzoek zal betrekking hebben op personen en gegevens die al bij de opsporingsinstanties bekend zijn. Het resultaat van een ongericht dataminingonderzoek kan aanleiding zijn voor het doen van verder onderzoek. Dat vervolgonderzoek zal gericht van aard zijn, zodat kan worden gesproken van een gericht dataminingonderzoek.

#### *3.5.2 Het gerichte dataminingonderzoek*

De kenmerken van een gericht dataminingonderzoek zijn in sectie 3.4.2 behandeld. In het geval van een concrete verdenking of aanwijzing zal de te gebruiken dataminingvariant steeds gericht van aard zijn. Deze vorm van datamining is bij uitstek geschikt voor gebruik ten behoeve van operationele zaken. Vanwege het ingrijpender karakter van een gericht dataminingonderzoek vindt het plaats in de latere stadia van het proces van informatiegaring. Al naar gelang de gebruikte dataminingvariant ingrijpender van aard is, dienen strengere voorwaarden te worden gesteld aan het gebruik ervan. Met betrekking tot het doen van gericht dataminingonderzoek wordt dit gerealiseerd, door nadere beperkingen te stellen aan de aard van de gegevens die in het kader van dit onderzoek mogen worden verwerkt en de groep van personen op wie deze gegevens betrekking hebben. Het is bijvoorbeeld disproportioneel om ten behoeve van het opsporen van relatief kleine vergrijpen (grote groepen) onschuldige burgers voorwerp van onderzoek te maken<sup>33</sup>.

Verder mogen opsporingsdiensten alleen van bepaalde gegevens(verzamelingen) gebruik maken voor zover dat noodzakelijk is voor het betreffende onderzoek. Het gebruik van

---

33. Op deze beperkingen wordt in hoofdstuk 4 nader ingegaan.

gegevens in het kader van een gericht dataminingonderzoek is alleen toegestaan wanneer deze betrekking hebben op een bepaald delict en/of een bepaalde groep van personen. Daar staat tegenover dat ook gebruik kan worden gemaakt van gegevens die betrekking kunnen hebben op onschuldige burgers. Een mogelijke inbreuk op de rechten van het subject van onderzoek dient te worden afgewogen tegen de ernst van het (mogelijk) gepleegde vergrijp. Over het algemeen geldt dat, naarmate een delict ernstiger van aard is, het minder bezwaarlijk is wanneer gebruik wordt gemaakt van ingrijpendere onderzoeksmethoden. Het bestaan van (wettelijke) beperkingen aan het onderzoek naar delict en subject maakt duidelijk, dat geen sprake meer is van een ongericht dataminingonderzoek. Het onderzoek wordt opgestart vanuit een bepaalde veronderstelling, een bepaalde aanname, die om nader onderzoek vraagt.

Ter illustratie van het onderscheid tussen het gebruik van een ongericht en een gericht dataminingonderzoek kan worden gedacht aan een situatie waarbij de behoefte bestaat om op het internet onderzoek te doen naar eventuele verspreiding van kinderpornografie. Een dergelijk onderzoek kan niet worden uitgevoerd in het kader van een ongericht dataminingonderzoek; wanneer ongericht wordt gezocht is het onderzoek immers niet beperkt tot het opsporen van kinderporno (in een bepaald geval). Dat zou betekenen dat een schier onbeperkt aantal onschuldige burgers onderwerp wordt van een verwerking in het kader van de opsporing zonder dat zij daartoe aanleiding hebben gegeven. Onderzoek in die zin is wel toegestaan in het kader van gerichte datamining. In dat geval wordt specifiek gezocht naar kinderporno. Daarbij geldt tevens de beperking dat de groep personen die zich, al dan niet met medeweten, onderzoeksactiviteiten moeten laten welgevallen beperkt dient te blijven. Opsporingsautoriteiten kunnen niet onder het mom van het zoeken naar kinderporno enorme hoeveelheden willekeurig internetverkeer analyseren, indien dat technisch al mogelijk zou zijn. Om te kunnen spreken van een gericht onderzoek dient het zoeken naar kinderporno te worden beperkt binnen een afgebakende groep van nieuwsgroepen, chatkanalen of webpagina's waarvan het vermoeden bestaat dat die voor deze strafbare gedragingen worden gebruikt. Dit voorbeeld illustreert de begrenzing naar gedragingen en personen met betrekking waartoe een gericht onderzoek kan worden geïnitieerd.

#### *3.5.2.1 Terugkoppeling naar het proces van informatiegaring*

Het eerste stadium van het proces van informatiegaring is gericht op een algemene verbetering van de informatiepositie. Dit gaat niet samen met de aard van een gericht dataminingonderzoek dat wordt aangewend ten behoeve van een bepaalde zaak of een bepaald geval, waarbij het onderzoek primair is gericht op een specifieke, gerichte verbetering van de informatiepositie; het nastreven van een algemene verbetering van de informatiepositie is in gevallen als deze een bijkomstigheid. Voorts zijn de mogelijkheden van een dataminingonderzoek in het eerste stadium van de opsporing beperkt, terwijl in het kader van een gericht onderzoek reeds behoefte zal bestaan aan ruimere mogelijkheden

tot het maken van een inbreuk op de persoonlijke levenssfeer. Dit geldt vooral met betrekking tot het gebruik van externe gegevens. Met het oog hierop zal gedurende het eerste stadium van het proces van informatiegaring in beginsel geen gebruik kunnen worden gemaakt van de gerichte dataminingvariant.

### 3.5.2.2 *Het verkennend onderzoek*

Met behulp van een gericht dataminingonderzoek kan uitvoering worden gegeven aan een verkennend onderzoek zoals bedoeld in art. 126gg Sv. Een verkennend onderzoek dient ter voorbereiding van de opsporing en heeft daarmee een strafvorderlijk doel<sup>34</sup>. Voor de toepassing van een verkennend onderzoek dienen feiten of omstandigheden aanwezig zijn waaruit aanwijzingen voortvloeien, dat binnen een verzameling van personen strafbare feiten worden gepleegd of beraamd. Een verkennend onderzoek heeft een gericht karakter, hetgeen ten eerste blijkt uit de eis dat sprake dient te zijn van aanwijzingen en ten tweede uit de omstandigheid dat het moet gaan om een (bepaalde) groep van personen. Hoewel vaak al voldoende feiten en omstandigheden bekend zijn die aanleiding geven voor een vermoeden dat misdrijven zijn gepleegd of worden beraamd, wordt nog niet direct een opsporingsonderzoek gestart. De reden is een behoefte aan nadere informatie<sup>35</sup>. Deze kan worden verkregen door middel van een gericht dataminingonderzoek, uitgevoerd in het kader van een verkennend onderzoek. Daarbij kan informatie worden verwerkt uit onder meer (politie)registers, open bronnen en lopende onderzoeken. De opslag van deze informatie vindt plaats in een bijzonder tijdelijk politieregister als bedoeld in art. 1 sub *j* WPolr.

In het kader van een gericht dataminingonderzoek dat wordt uitgevoerd in het kader van een verkennend onderzoek, kunnen ook gegevens worden verwerkt omtrent onverdachte personen; dit in tegenstelling tot ongericht dataminingonderzoek. Aangezien gegevens mogen worden verwerkt betreffende onverdachte personen is een gericht dataminingonderzoek ingrijpender van aard. Bij het gebruik van het dataminingsproces in het kader van de opsporingstaak is het onvermijdelijk dat in enig stadium gebruik wordt gemaakt van tot individuele personen herleidbare gegevens. Dergelijk onderzoek zal weinig opleveren wanneer het gevonden resultaat niet aan individualiseerbare personen kan worden gekoppeld. Bovendien wordt ten aanzien van art. 126gg Sv expliciet de eis gesteld dat het onderzoek gericht moet zijn op een zo precies mogelijk omschreven<sup>36</sup> verzameling van personen<sup>37</sup>, hetgeen een individualiseerbaar karakter van de gegevens onderstreept. Nu

---

34. *Kamerstukken II*, 1996/197, 25 403, nr. 3, p. 125.

35. *Kamerstukken II*, 1996/197, 25 403, nr. 3, p. 49.

36. Zie ook Sietsma 2004 en *Sib.* 2004, 105: in het kader van een verkennend onderzoek kan in beginsel niet worden beschikt over NAW-gegevens, hetgeen de mogelijkheden van een verkennend onderzoek ernstig beperkt.

37. *Handboek voor de opsporingspraktijk* 2000, Model Verkennend onderzoek.

hierbij sprake kan zijn van inbreuken op de privacy, heeft het verkennend onderzoek een wettelijke grondslag. Omdat een verkennend onderzoek geen opsporingsonderzoek betreft, mogen geen opsporingsbevoegdheden of dwangmiddelen worden gebruikt. Slechts wanneer er sprake is van op feiten en omstandigheden gebaseerde concrete aanwijzingen tegen bepaalde personen, kunnen tegen hen gerichte opsporingsactiviteiten plaatsvinden op basis van art. 2 Politiewet 1993, dan wel soortgelijke taakstellende bepalingen in bijzondere wetten. Bij zwaardere verdenking, dus na de vervulling van de verdengkingscriteria van de art. 27 en/of 132a Sv, kunnen ook bijzondere opsporingsbevoegdheden en dwangmiddelen worden toegepast. In dat geval is echter geen sprake meer van een verkennend onderzoek, maar van een opsporingsonderzoek. Gedurende het opsporingsonderzoek zijn de mogelijkheden tot het maken van een inbreuk op de rechten van de burger ruimer en is het spanningsveld tussen privacy en opsporing minder prominent aanwezig. Met het oog op de bescherming van de persoonlijke levenssfeer is het van belang dat een duidelijk onderscheid bestaat tussen een verkennend onderzoek en een opsporingsonderzoek. Wanneer naar aanleiding van het verkennend onderzoek een concrete verdenking rijst, dient in beginsel worden overgegaan tot een opsporingsonderzoek.

#### *3.5.2.3 Het opsporingsonderzoek*

Een gericht dataminingonderzoek kan, behalve in het kader van een verkennend onderzoek, worden verricht gedurende het opsporingsonderzoek in de zin van art. 132a Sv. Ook het opsporingsonderzoek heeft daarmee een gericht karakter. Het verkennend onderzoek en het opsporingsonderzoek hebben met elkaar gemeen, dat in beide gevallen sprake dient te zijn van feiten of omstandigheden waaruit een bepaalde verdenking of een bepaald vermoeden voortvloeit, dan wel aanwijzingen voortvloeden. Tijdens het opsporingsonderzoek is deze verdenking het sterkst en kan gebruik worden gemaakt van zwaardere onderzoeksmethoden dan bij het verkennend onderzoek. Een dataminingonderzoek dat plaatsvindt in het stadium van het opsporingsonderzoek dient te zijn gericht op een strafvorderlijke afdoening. Wanneer in het kader van een opsporingsonderzoek gebruik wordt gemaakt van een gericht dataminingonderzoek kan een onderscheid worden gemaakt tussen het opsporingsonderzoek naar aanleiding van een verdenking van een strafbaar feit en onderzoek dat is gebaseerd op een redelijk vermoeden dat in georganiseerd verband ernstige misdrijven worden beraamd of gepleegd.

Bij een redelijk vermoeden van een strafbaar feit kan het gaan om allerlei feitelijk gepleegde strafbare feiten van meer of minder ernstige aard. Eventueel onderzoek naar feiten die nog gepleegd kunnen worden valt hier niet onder. Bij de beschrijving van de opsporing maakt de PEC terecht een onderscheid tussen de situatie waarbij sprake is van een redelijk vermoeden van een gepleegd strafbaar feit (verdenking) en die waarin een redelijk vermoeden bestaat van schuld aan een gepleegd strafbaar feit (verdenking en verdachte). Indien enkel sprake is van een verdenking zal, teneinde een verdachte te vinden,

behoefte bestaan aan nadere informatie. Hiervoor kan gebruik worden gemaakt van een gericht dataminingonderzoek. In dit geval wordt het gerichte dataminingonderzoek uitgevoerd in het kader van het opsporingsonderzoek. Indien wordt voldaan aan de voorwaarden die de wet daaraan stelt, kan daarbij ook gebruik worden gemaakt van bijzondere opsporingsmethoden conform Titel IVa Sv, alwaar de bevoegdheden ter opheldering van concrete strafbare feiten zijn geregeld<sup>38</sup>.

Ingeval er (ook) al sprake is van een verdachte bestaat geen directe behoefte meer aan aanvullende informatie. Het streven naar een specifieke verbetering van de informatiepositie is dan vervangen door een behoefte aan verificatie van de beschikbare informatie.

Een opsporingsonderzoek is eveneens mogelijk naar aanleiding van een redelijk vermoeden dat in georganiseerd verband ernstige misdrijven worden beraamd of gepleegd. Deze fase werd door de PEC ook wel aangeduid als 'de pro-actieve fase'. Hierbij is nog geen sprake van een concrete verdenking en onderzoek heeft betrekking op meerdere personen en meerdere misdrijven. Het doel van het onderzoek is niet de opheldering van een concreet misdrijf (beraamd of gepleegd), maar het in kaart brengen van het georganiseerde verband dat die misdrijven beraamt of pleegt<sup>39</sup>. Daarbij kan gebruik worden gemaakt van de in Titel V Sv geregelde bijzondere bevoegdheden. Bij een succesvol verloop van het onderzoek kan het doel daarvan worden verlegd naar het vaststellen van de waarheid over de inmiddels getraceerde misdrijven. In dat geval ligt het in de rede om gebruik te maken van de opsporingsbevoegdheden die zijn geregeld in Titel IVa Sv. Ook in het kader van een opsporingsonderzoek naar aanleiding van een redelijk vermoeden dat in georganiseerd verband ernstige misdrijven worden beraamd of gepleegd kan in beginsel gebruik worden gemaakt van gericht dataminingonderzoek. Er bestaat behoefte aan een verbetering van de informatiepositie waarbij gericht wordt gezocht. Ook wanneer het doel van het onderzoek naar aanleiding van het resultaat wordt verlegd naar het vaststellen van de waarheid omtrent inmiddels getraceerde misdrijven, blijft er sprake van gericht dataminingonderzoek; er is namelijk nog geen sprake van een verdachte of van verdachten. Op het moment waarop dat wel het geval is, verschuift het zwaartepunt van dataminingonderzoek naar verificatie. Verder onderzoek zal dan gericht zijn op verificatie van het gevonden resultaat.

### Resumerend

Een gericht dataminingonderzoek kan, afhankelijk van het stadium van de opsporing, zowel in het kader van een verkennend onderzoek als ten behoeve van een opsporingsonderzoek worden gebruikt.

---

38. *Kamerstukken II*, 1996/97, 25 403, nr. 3, p. 56.

39. *Kamerstukken II*, 1996/97, 25 403, nr. 3, p. 26.

### Verkenkend onderzoek

Bij een gericht dataminingonderzoek in het kader van een verkennend onderzoek mogen ook gegevens over onverdachte personen worden verwerkt. Daarmee is weliswaar sprake van een vergaande inbreuk op de persoonlijke levenssfeer, maar daar staat tegenover dat deze vorm van onderzoek een aantal beperkingen kent. Zo zullen er al aanwijzingen moeten zijn van strafbare gedragingen<sup>40</sup> en dient het onderzoek zich te beperken tot een groep van personen die (slechts) als collectief aanleiding geven tot onderzoek. De daadwerkelijke reikwijdte van een verkennend onderzoek is erg ruim. Het kan zich richten op bepaalde groepen, branches of sectoren in de samenleving. De aard van dit onderzoek brengt met zich mee dat de te onderzoeken verzameling van personen op tal van kenmerken kan worden uitgezocht<sup>41</sup>, bijvoorbeeld via analyse van een groot aantal online veilingssites om na te gaan of deze worden gebruikt voor het verkopen van gestolen goederen. Een verkennend onderzoek kan betrekking hebben op zowel toekomstige, als op reeds gepleegde strafbare feiten. Overigens kan het daarbij alleen gaan om misdrijven als omschreven in art. 67 lid 1 Sv en die, gezien hun aard of de samenhang met andere misdrijven die binnen die verzamelingen van personen worden beraamd of gepleegd, een ernstige inbreuk op de rechtsorde opleveren. Hoewel gegevens omtrent onverdachte personen mogen worden verwerkt blijft er sprake van een lichte vorm van onderzoek, waarvoor geen strafvorderlijke bevoegdheden mogen worden gebruikt.

### Opsporingsonderzoek

De meest ingrijpende vorm van dataminingonderzoek betreft het, in het kader van de opsporing, gerichte onderzoek; daarbij mogen namelijk gegevens betreffende onverdachte personen worden verwerkt en kunnen opsporingsautoriteiten beschikken over vergaande opsporingsbevoegdheden. Een dataminingonderzoek in het kader van een opsporingsonderzoek naar aanleiding van een redelijk vermoeden van een strafbaar feit kan betrekking hebben op iedere, al gepleegde, strafbare gedraging<sup>42</sup>. Het bestaan van een redelijk vermoeden rechtvaardigt de mogelijkheid van vergaande inbreuk op de persoonlijke levenssfeer.

Daarbij moet wel worden voldaan aan de voorwaarde, dat gericht onderzoek vanwege de aanwezigheid van een verdenking reeds gaande is. Of gebruik kan worden gemaakt van zware opsporingsbevoegdheden hangt af van de vraag, of is voldaan aan de voorwaarden die de wet hieraan stelt. In art. 132a Sv wordt gesproken van een 'redelijk vermoeden van een gepleegd strafbaar feit'. In dat kader is bij toepassing van dataminingonderzoek

---

40. Een vermoeden (van opsporingsambtenaren) volstaat daarvoor niet.

41. *Kamerstukken II*, 1997/198, 25 403, nr. 7, p. 75.

42. Ook bij nog te plegen ernstige delicten welke niet door criminele organisaties worden voorbereid, kan in bepaalde gevallen worden gesproken van (pro-actieve) opsporing. Zie sectie 2.4.

aan te bevelen om, in navolging van de PEC, onderscheid te maken tussen een situatie waarin sprake is van een verdenking en een waarbij sprake is van een klassieke verdachte. Ingeval van enkel een strafbaar feit zal in beginsel altijd behoefte bestaan aan nadere informatie voor het vaststellen van de identiteit van een verdachte. Daarbij kan gebruik worden gemaakt van gericht dataminingonderzoek. Wanneer reeds een verdachte kan worden aangewezen zal met name behoefte bestaan aan controle van de verdenking en dus aan verificatie in plaats van gericht dataminingonderzoek.

Een gericht dataminingonderzoek kan ook worden uitgevoerd in het kader van een opsporingsonderzoek dat is gebaseerd op een redelijk vermoeden, dat in georganiseerd verband ernstige misdrijven worden beraamd of gepleegd. In dergelijke gevallen kan ook worden gesproken van pro-actieve opsporing. De aanwezigheid van een georganiseerd verband in combinatie met het belang van een effectieve bestrijding van de zware criminaliteit rechtvaardigt een vergaande inbreuk op de persoonlijke levenssfeer. Het preventief bestrijden van strafbare gedragingen met behulp van een gericht dataminingonderzoek, waarmee een zo vergaande inbreuk op de persoonlijke levenssfeer kan worden gemaakt, is enkel mogelijk met betrekking tot de misdrijven waarop art. 132a Sv ziet. De vraag of er sprake is van dataminingonderzoek of van verificatie zal in deze gevallen niet aan de orde komen; het opsporingsonderzoek zal steeds gericht van aard zijn vanwege een bestaand verband van personen c.q. misdrijven. Pas wanneer een min of meer volledig beeld is verkregen van de criminele organisatie, de misdrijven die worden beraamd en gepleegd en de rol die de verschillende betrokkenen daarbij spelen kan een verantwoorde beslissing worden genomen over de vraag, welke verdachten voor welke misdrijven moeten worden vervolgd. Alleen op deze wijze kan het opsporingsonderzoek doeltreffend worden opgezet<sup>43</sup>.

De activiteiten in de pro-actieve fase hebben betrekking op het opsporingsonderzoek. Dit betekent dat zij, in tegenstelling tot die van het verkennend onderzoek, ter terechtzitting toetsbaar zijn. Alle gebruikte opsporingsbevoegdheden, en daarmee ook de methoden die in de pro-actieve fase worden ingezet, dienen in beginsel in het openbaar te worden verantwoord. Deze verantwoordingsplicht is ook van toepassing op een eventueel gebruik van dataminingonderzoek in deze fase.

### *3.5.3 De verificatie*

Hoewel de verificatie als derde fase van het dataminingsproces wordt onderscheiden, is in dit stadium geen sprake meer van dataminingonderzoek. De nadruk ligt niet meer op het ontdekken van nieuwe gegevens, maar op het verifiëren van het gevonden resultaat. Tijdens het proces van informatiegaring heeft op enig moment niet meer te worden

---

43. *Kamerstukken II*, 1996/97, 25 403, nr. 3, p. 4.

gezocht naar onbekende verbanden en kennis die de aanleiding kunnen vormen voor een mogelijke strafrechtelijke sanctie. Een dergelijke aanleiding kan zijn gebaseerd op een uit een dataminingsonderzoek resulterende concrete verdenking. Wanneer eenmaal sprake is van is van een concrete verdachte, bestaat geen behoefte meer aan (het verzamelen van) nadere gegevens over die persoon, aangezien die gegevens immers reeds ten grondslag zullen (c.q. dienen te) liggen aan de verdenking jegens hem. Vanaf dat moment vindt toetsing plaats van de gevonden kennis.<sup>44</sup> Bij zwaardere verdenking en vervulling van de verdengkingscriteria van de art. 27 en/of 132a Sv kunnen in beginsel ook bijzondere opsporingsbevoegdheden en dwangmiddelen worden toegepast.<sup>45</sup>

In conclusie kan binnen het proces van informatiegaring alleen van verificatie worden gesproken als het onderdeel uitmaakt van het stadium van het opsporingsonderzoek. Verificatie heeft geen (primaire) informatief karakter, maar dient gericht te zijn op een strafvorderlijke afdoening. Verificatie is niet beperkt tot bepaalde vormen van strafbaar handelen. De toepassing ervan wordt slechts beperkt door de mate van verdenking en de daarmee samenhangende behoefte aan nadere informatiewinning. Kenmerkend is dat bij verificatie steeds sprake is van een individualiseerbare persoon<sup>46</sup>.

### 3.6 Het juridische kader

Het dataminingsproces kan als onderzoeksmethode worden ingezet gedurende het proces van informatiegaring. Al naar gelang de het primaire doel van het dataminingsproces (of het onderzoek ten behoeve waarvan het gebruikt wordt) verschuift van een verbetering van de informatiepositie naar een strafrechtelijke afdoening, verandert ook de opsporingsfase waarin het dataminingsproces zich afspeelt. Naarmate de toepassing van het dataminingsproces ingrijpender van aard is, wordt de behoefte aan een wettelijke grondslag groter teneinde te voorzien in de beperkingen die in dat geval aan het dataminingsonderzoek dienen te worden gesteld. De manier waarop het dataminingsproces zich verhoudt ten opzichte van het proces van informatiegaring, en de verschillende wijzen waarop aan dat proces uitvoering kan worden gegeven, zijn in schema weergegeven (schema 4). Dit model vormt het juridische kader waarbinnen de toepassing van het dataminingsproces als onderzoeksmethode binnen het proces van informatiegaring (de opsporing) dient plaats te vinden.

---

44. Aldus ook *Kamerstukken II*, 1997/198, 25 403, nr. 7, p. 9, waar omtrent afspraken met criminelen wordt opgemerkt: 'Ten derde strekken de gemaakte afspraken niet tot het verzamelen van gegevens om vast te stellen of sprake is van verdenking van door de verdachte gepleegde strafbare feiten, doch als gebruik als bewijsmiddel ter staving van een reeds bestaande verdenking. Zij worden derhalve niet gebruikt in de voorfase van het opsporingsonderzoek.'

45. *Handboek voor de opsporingspraktijk* 2000, Model Verkennend onderzoek.

46. Hoewel het onderzoek zich ook kan richten op een groep van verdachte personen wordt hier, gezien het individuele karakter van het Nederlandse strafrecht, gesproken van een individuele verdachte.

	Ontdekken		Toetsing
<b>Toepassingsvarianten dataminingsproces</b>	Ongericht dataminingsonderzoek	Gericht dataminingsonderzoek	Verificatie
<b>Het proces van informatiegaring</b>	Opbouwen en instandhouden van de informatiepositie	Het verkennend onderzoek	Het opsporingsonderzoek
<b>Aanknopingspunten</b>	Geen verdenking	← Overgang ⇒	Verdachte

Schema 4 De relatie tussen de drie dataminingsvarianten en de stadia van het proces van informatiegaring

Schema 5 toont hoe de drie varianten van het dataminingsproces leiden naar een logische overgang van het ongerichte dataminingsonderzoek naar verificatie. Het resultaat van een ongericht dataminingsonderzoek kan de aanleiding vormen voor verder, gericht onderzoek dat kan leiden tot concretere uitkomsten. Wanneer dit resulteert in een voldoende onderbouwde verdenking jegens één of meer personen, kan worden overgegaan tot de derde toepassingsvariant van het dataminingsproces, de verificatie.

	Proces van informatiegaring		
	Informatiepositie	Verkennend onderzoek	Opsporingsonderzoek
<b>Toepassingsvariant dataminingsproces</b>	Ongericht	Gericht	Gericht/verificatie
<b>Aanknopingspunten</b>	Geen verdenking	← Overgang ⇒	Verdachte
<b>Voorwaarden gebruik</b>	Geen specifieke beperkingen	Aanwijzing misdrijven binnen verzamelingen van personen	Verdenking/pro-actief aanpak georganiseerde criminaliteit
<b>Inzet bijzondere opsporingsmethoden</b>	Nee	Nee	Ja
<b>Is er sprake van opsporing?</b>	Nee	Nee	Ja
<b>Verhouding tot visie van de PEC</b>	Fase I	(Fase II)	Fase II/Fase III

Schema 5 Overzicht aandachtspunten met betrekking tot het gebruik van dataminingsonderzoek als onderzoeksmethode ten behoeve van het proces van informatiegaring

---

## 4 De Wet Politierregisters en het Besluit Politierregisters

Zowel het proces van informatiegaring als het dataminingsproces staan in het teken van het verwerken van gegevens. De voortschrijdende digitalisering<sup>1</sup> zorgt vandaag de dag voor talloze informatiebronnen waarvan politie en justitie gebruik kunnen maken bij het vervullen van de opsporingstaak. Hoewel in theorie een schat aan (digitale) informatie voorhanden is, zijn de verwerkingsmogelijkheden ten behoeve van de opsporingstaak rechteens begrensd; het spanningsveld tussen het recht als instrument voor de overheid en het recht als bescherming van de burger tegen diezelfde overheid is in het eerste hoofdstuk besproken. Omdat een verwerking van (persoons)gegevens kan leiden tot vergaande inbreuken op de persoonlijke levenssfeer, dienen opsporingsinstanties zich te houden aan de wettelijke beperkingen die aan het verzamelen, opslaan en bewerken van informatie zijn gesteld. Deze beperkingen kunnen ook gevolgen hebben voor de inrichting van een computerprogramma (bijvoorbeeld een geavanceerd dataminingsprogramma) dat de politie ondersteunt bij haar taken. Volgens de wetgever dient een programmeur zich te richten naar de wettelijke regels<sup>2</sup>. Naar aanleiding van onder meer de bevindingen en aanbevelingen van de PEC zijn de wettelijke regels waaraan de opsporingsdiensten zich bij het verzamelen, opslaan en bewerken van gegevens dienen te houden aangescherpt<sup>3</sup>. Op het moment van schrijven (2005) staan vooral de mogelijkheden van gegevensvergaring in het kader van de opsporingstaak in de belangstelling naar aanleiding van het rapport van de commissie Mevis.<sup>4</sup> In

- 
1. *Kamerstukken II*, 1997/198, 25 880, nrs. 1-2, p. 49. Digitalisering van informatie wordt in het kader van de informatiemaatschappij ook wel aangeduid met de term 'dematerialisering'. Kennis, diensten en informatie die niet in een tastbare vorm zijn neergelegd vormen de motor van de economie. Bij digitale vastlegging is informatie niet meer gebonden aan een bepaalde fysieke drager of plaats. Digitaal vastgelegde informatie is voorts onuitputtelijk, want zij kan oneindig worden gekopieerd zonder dat dit leidt tot kwaliteitsverlies of vernietiging.
  2. *Kamerstukken II*, 1988/189, 19 589, nr. 6, p. 7 (*Stb.* 2001, 337).
  3. Onder meer door middel van wijziging van het Besluit beheer regionale politiekorpsen (*Stb.* 1999, 501), het Wetboek van Strafvordering (de Wet bijzondere opsporingsbevoegdheden; *Stb.* 1999, 245), de Wet Politierregisters (de Wet bijzondere politierregisters; *Stb.* 1999, 244) en de Regeling criminele inlichtingen eenheden (*Stb.* 2000, 198) die de CID-regeling 1995 vervangt.
  4. *Kamerstukken II*, 2003/104, 29 441, nr. 3.

onderhavig onderzoek ligt de nadruk niet zozeer op de gegevensvergaring maar op de wijze waarop gegevens verwerkt (mogen) worden.

In dit hoofdstuk wordt ingegaan op de bestaande wet- en regelgeving, zowel nationaal als internationaal, die (mogelijk) relevant is voor het verwerken van gegevens in het kader van het dataminingsproces ten behoeve van de opsporing alsmede de invloed daarvan op de voorwaarden waaronder opsporingsinstanties van die gegevens gebruik mogen maken.

### Gegevensverwerking

Met betrekking tot de gegevens die in het kader van een dataminingsonderzoek worden verwerkt, kan onderscheid worden gemaakt tussen twee categorieën. De eerste categorie betreft de gegevens die al binnen het politieke apparaat aanwezig zijn. Dit zijn de gegevens die vallen onder het regime van de WPoI en liggen opgeslagen in de door de politie onderhouden registers waarop de Wbp van toepassing is<sup>5</sup>, alsmede de voor de opsporing en vervolging van belang zijnde informatie die ligt opgeslagen in de registers van de bijzondere opsporingsdiensten. Ook tapgegevens, observatierapporten, dagjournaals en mondeling overgedragen bevindingen kunnen tot de politieke gegevens worden gerekend (ook wel aangemerkt als 'interne informatiebronnen')<sup>6</sup>.

De tweede categorie betreft gegevens uit bronnen buiten de politieke sfeer. Hierbij kan worden gedacht aan open bronnen uit zowel de private als de (semi-)publieke sector als bibliotheken, kranten, het internet en persoonsregistraties van het bedrijfsleven, zoals registraties van banken, de Kamers van Koophandel en verzekerings- en creditcardmaatschappijen. Voorts kunnen persoonsregistraties van de overheid, zijnde geen politieregisters, tot deze externe informatiebronnen worden gerekend: het bevolkingsregister, de registraties van de geprivatiseerde opsporingsdiensten, zoals eenheden binnen bedrijfsverenigingen, BUMA/STEMRA en registraties bij de reguliere politie die vallen buiten het kader van de in art. 2 Politiewet 1993 omschreven taak, zoals de vuurwapen-, horeca- en vreemdelingenregistraties.

#### 4.1 Bescherming van de persoonlijke levenssfeer

Strafvordering heeft op grond van art. 1 Sv alleen plaats op de wijze bij de wet voorzien. Strafvorderlijke bevoegdheden, in het bijzonder die welke een inbreuk kunnen maken op vrijheden of grondrechten van burgers, dienen een basis te hebben in de wet in formele zin. Bij strafforderlijke gegevensvergaring kan vooral het recht op bescherming van de persoonlijke levenssfeer in het geding komen. Bij het verwerken van gegevens die raken

---

5. Per 1 september 2001 is de Wpr vervangen door de Wbp (*Stb.* 2000, 302).

6. Met het oog op de wijze waarop een dataminingsonderzoek plaatsvindt, wordt hier echter niet het onderscheid tussen interne en externe gegevens gehanteerd. Alle gegevens die in het kader van een dataminingsonderzoek worden verzameld en verwerkt en welke niet de aanleiding zijn geweest om het betreffende onderzoek te starten, worden als externe gegevens aangemerkt.

aan de persoonlijke levenssfeer dienen opsporingsinstanties zich te conformeren aan de beperkingen die nationale en internationale wet- en regelgeving daaraan stelt. In deze sectie wordt stilgestaan bij de beperkingen die dit met zich meebrengt voor de toepassing van dataminingonderzoek ten behoeve van de opsporingstaak.

#### Art. 8 EVRM

Het recht van de burger op de eerbiediging van zijn of haar persoonlijke levenssfeer wordt onder meer gewaarborgd door art. 8 (recht op eerbiediging van privé-, familie- en gezinsleven) van het Europees verdrag voor de rechten van de mens en de fundamentele vrijheden en art. 17 van het Internationaal Verdrag inzake burgerrechten en politieke rechten (IVBPR). Het begrip ‘privé-leven’ in de genoemde verdragen heeft dezelfde betekenis als het begrip ‘persoonlijke levenssfeer’ in de Nederlandse Grondwet (Gw). Op grond van art. 8 lid 2 EVRM kan een inbreuk op de persoonlijke levenssfeer worden gemaakt wanneer daarin bij de wet is voorzien en voor zover dit in een democratische samenleving noodzakelijk is in het belang van ’s lands veiligheid, de openbare veiligheid of het economische welzijn van het land, de bescherming van de openbare orde en het voorkomen van strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen. Met het oog op de uitzonderingen die in dit artikel worden genoemd, lijkt een gegevensverwerking ten behoeve van de opsporing een inbreuk op de persoonlijke levenssfeer te rechtvaardigen. Daar dient dan, zoals reeds vermeld, wel een wettelijke grondslag voor te zijn die voor de burger voldoende toegankelijk en voorzienbaar is. Indien de regeling is gebaseerd op een wet in formele zin (zoals art. 10 Gw verlangt) is aan deze eis voldaan. De eis van voorzienbaarheid betekent dat de regeling voldoende precies dient te zijn geformuleerd, zodat de burger vooraf kan weten onder welke omstandigheden en voorwaarden de bevoegdheid mag worden toegepast. De regeling moet verder waarborgen bieden tegen willekeurige inmenging van de overheid in het persoonlijke leven van de burger en tegen misbruik van bevoegdheid<sup>7</sup>. In het kader van de verwerking van persoonsgegevens<sup>8</sup> kunnen ook het Databeschermingsverdrag en de Europese richtlijn betreffende de bescherming van persoonsgegevens (Privacyrichtlijn)<sup>9</sup> worden genoemd.

7. Zie ook Kruslin & Huvig, EHRM 24 april 1990, *NJ* 1991, nr. 523.

8. Dontje, 2000. Persoonsgegevens zijn alle gegevens betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. ‘Geïdentificeerd’ houdt in dat de naam van de persoon op wie de gegevens betrekking hebben, bekend is. ‘Identificeerbaar’ betekent dat de naam van een natuurlijk persoon op wie de gegevens betrekking hebben, redelijkerwijs kan worden achterhaald.

9. Richtlijn nr. 95/46/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* L 281. Voor de gegevens die beschikbaar zijn bij aanbieders van telecommunicatie geldt Richtlijn nr. 97/66/EG van het Europees Parlement en de Raad van 15 december 1997 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de telecommunicatiesector, *PbEG* L 24.

*Databeschermingsverdrag*

Een verwerking van persoonsgegevens ten behoeve van de opsporing impliceert in beginsel, dat gegevens voor een ander doel worden gebruikt dan waarvoor zij zijn vastgelegd<sup>10</sup>. Het Databeschermingsverdrag vormt in dat geval een belangrijk toetsingskader. Op grond van art. 9 van dat verdrag is een verwerking voor een ander doel mogelijk indien dit bij wet is voorzien en noodzakelijk is in een democratische samenleving in het belang van het bestrijden van strafbare feiten (het noodzakelijkheids criterium)<sup>11</sup>.

*Privacyrichtlijn*

De Europese richtlijn inzake de bescherming van persoonsgegevens is aangenomen op 15 juni 1995 en vastgesteld op 24 oktober. Hoewel deze richtlijn betrekking heeft op de verwerking van persoonsgegevens, is de betekenis daarvan voor opsporingsinstanties gering. Op grond van art. 13 van de richtlijn mogen staten namelijk uitzonderingen maken op het regime van de richtlijn indien dit noodzakelijk is in het kader van bepaalde algemene belangen, zoals de staatsveiligheid en de opsporing en vervolging van strafbare feiten. Het dataminingsproces dat wordt ingezet ten behoeve van de opsporing valt onder de uitzonderingen die in art. 13 van de richtlijn worden genoemd. Daarenboven geldt dat de privacyrichtlijn het domein van de politie en het strafrecht uitsluit van haar toepassingsgebied<sup>12</sup>. Met de komst van de Wbp is de richtlijn in ons recht geïmplementeerd.

*Richtlijn betreffende privacy en elektronische communicatie*

In het kader van het dataminingsproces is ook de richtlijn over privacy en elektronische communicatie, die sinds 12 juli 2002 van kracht is<sup>13</sup>, van belang. Het betreft een lex specialis van de Privacyrichtlijn. De richtlijn schept waarborgen die de burger dienen te beschermen tegen zaken als af luisteren, aftappen, opslaan of anderszins onderscheppen of controleren van de communicatie en de daarmee verband houdende verkeersgegevens door anderen dan de gebruikers, voor zover de gebruikers daar geen toestemming voor

---

10. *Kamerstukken II*, 2001/02, 28 059, nr. 3, p. 5.

11. Ook dient de vergaring van gegevens rechtmatig te zijn en niet bovenmatig. De art. 6 lid 1 jo art. 13 lid 1 onder *d* van de Richtlijn nr. 95/46/EG, evenals het regime van de daarop gebaseerde Wbp komen hiermee overeen.

12. Ingevolge art. 3 lid 2 van de richtlijn is zij niet van toepassing verklaard op de verwerking van persoonsgegevens die met het oog op de uitoefening van niet binnen het Gemeenschapsrecht vallende activiteiten geschiedt. Hieronder vallen activiteiten zoals bedoeld in de Titels V en VI waarin de samenwerking op het gebied van politie en justitie is geregeld. De richtlijn heeft in ieder geval geen betrekking op verwerkingen die zien op de openbare veiligheid, defensie, veiligheid van de staat en activiteiten van de staat op strafrechtelijk gebied.

13. Richtlijn nr. 2002/58/EG van het Europees Parlement en de Raad van de Europese Unie van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie, *PbEG* L 201.

hebben verleend. Het vertrouwelijke karakter van de communicatie staat centraal. De richtlijn biedt lidstaten de mogelijkheid<sup>14</sup> om in bepaalde gevallen ten behoeve van inlichtingendiensten, politie en justitie een inbreuk te maken op het vertrouwelijk karakter van de communicatie. Daarbij wordt voor lidstaten de mogelijkheid opengelaten voor het treffen van maatregelen om persoonlijke verkeersgegevens een beperkte tijd te bewaren indien dat noodzakelijk, redelijk en proportioneel is ter waarborging van de nationale veiligheid of het opsporen en voorkomen van strafbare feiten.<sup>15</sup>

#### *Art. 10 Gw*

De eerbiediging en bescherming van de persoonlijke levenssfeer is op nationaal niveau (richtinggevend) geregeld in art. 10 Gw. Dit artikel bepaalt dat eenieder, behoudens bij of krachtens de wet te stellen beperkingen, recht heeft op eerbiediging van zijn persoonlijke levenssfeer. In het tweede lid wordt aangegeven dat de wet regels stelt ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens. Tevens dient de wet, volgens het derde lid, regels te stellen 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. Het bepaalde in art. 10 Gw is richtinggevend. De nadere uitwerking van de bescherming van de persoonlijke levenssfeer, waaronder het vastleggen van persoonsgegevens, dient te worden geregeld in een formele wet. Daarbij dient rekening te worden gehouden met de eisen die het internationale recht met betrekking tot deze materie stelt. De bescherming van de persoonlijke levenssfeer is geregeld in de Wet Bescherming persoonsgegevens<sup>16</sup>.

#### *Wbp en WPolr*

De Privacyrichtlijn is uitgewerkt in de Wet bescherming persoonsgegevens, die per 1 september 2001 de Wet persoonsregistratie (Wpr) heeft vervangen. De Wbp ziet op de

---

14. Art. 15 lid 1 Richtlijn betreffende privacy en elektronische communicatie. De lidstaten kunnen wettelijke maatregelen treffen ter beperking van de reikwijdte van de in de art. 5 en 6, art. 8 lid 1, 2, 3 en 4, en art. 9 van deze richtlijn bedoelde rechten en plichten, indien dat in een democratische samenleving noodzakelijk, redelijk en proportioneel is ter waarborging van de nationale, d.w.z. de staatsveiligheid, de landsverdediging, de openbare veiligheid, of het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten of van onbevoegd gebruik van het elektronische-communicatiesysteem als bedoeld in art. 13 lid 1 van de Privacyrichtlijn. Daartoe kunnen de lidstaten o.a. wetgevingsmaatregelen treffen om gegevens gedurende een beperkte periode te bewaren om de redenen die in dit lid worden genoemd. Alle in dit lid bedoelde maatregelen dienen in overeenstemming te zijn met de algemene beginselen van het Gemeenschapsrecht, met inbegrip van de beginselen als bedoeld in art. 6 lid 1 en 2 van het Verdrag betreffende de EU.

15. Zie ook Ministerie van Justitie 2003.

16. Wet van 6 juli 2000, *Stb. 2000, 302*.

verwerking van persoonsgegevens<sup>17</sup>. Persoonsgegevens zijn alle gegevens betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. In het geval van opsporing van ernstige strafbare feiten is het mogelijk, dat persoonsgegevens worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen. Dit uitgangspunt is overgenomen in art. 43 Wbp, waarin de opsporing en vervolging van strafbare feiten als uitzonderingsgronden zijn opgenomen voor het doelbindingsbeginsel<sup>18</sup>.

Op grond van art. 2 lid 2 sub *c* Wbp is de Wbp niet van toepassing op de verwerking van persoonsgegevens ten behoeve van de uitvoering van de politietaak, zoals omschreven in art. 2 van de Politiewet 1993<sup>19</sup>. In dat geval is een aparte wettelijke regeling van toepassing, te weten de Wet Politierregisters.<sup>20</sup> De wetgever heeft met de WPolr en de daarbij behorende uitvoeringswetgeving de bedoeling gehad, de privacybescherming met betrekking tot de politierregisters uitputtend te regelen. Verstrekking- of gebruiksbepalingen in andere wetgeving dienen daarom in beginsel een corresponderende bepaling te hebben in de WPolr<sup>21</sup>. Er is een aantal redenen waarom met betrekking tot de verwerking van persoonsgegevens door de politie in het kader van de politietaak is gekozen voor een aparte wettelijke regeling. Ten eerste gaat het bij het verzamelen van persoonsgegevens in het kader van de politietaak vaak om gegevens die de geregistreerde niet vrijwillig heeft geleverd of die zelfs niet van hem afkomstig zijn. Een tweede beweegreden is gelegen in de bescherming van de persoonlijke levenssfeer met het oog op de bijzondere positie die de politie inneemt in de verhouding tussen overheid en burger. Ten derde biedt een aparte wettelijke regeling betere mogelijkheden om het verstrekkingenregime nauwkeurig te kunnen vastleggen, waardoor de persoonlijke levenssfeer van de geregistreerde beter kan worden beschermd.<sup>22</sup>

17. Hieronder verstaat de Wbp: 'elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, evenals het afschermen, uitwissen of vernietigen van gegevens' (art.1 onder *b* Wbp).

18. Commissie Mevis 2001, p. 47-48.

19. Ook art. 2 lid 3 sub *b* Wpr bepaalde destijds dat de Wpr niet van toepassing was op persoonsregistraties aangelegd ten dienste van de uitvoering van de politietaak als omschreven in art. 2 Politiewet 1993.

20. Voorschriften over het verwerken van gegevens door de politie zijn in de regel niet opgenomen in het Wetboek van Strafvordering maar in de Wet politierregisters. Een uitzondering hierop is gemaakt voor gegevens die worden verkregen door registratie door een technisch hulpmiddel bij toepassing van de bevoegdheden tot stelselmatige observatie of het opnemen van vertrouwelijke communicatie of telecommunicatie (art. 126cc). Voor andere opsporingsbevoegdheden bevat het Wetboek van Strafvordering geen voorschriften voor het verwerken van gegevens. *Kamerstukken I*, 2004 /05, 29 441, nr. C, p. 2.

21. *Kamerstukken II*, 1988 /89, 19 589, nr. 11, p. 31.

22. *Kamerstukken II*, 1985 /86, 19 589, nr. 3, p. 2.

Nu art. 2 sub *c* Wbp de Wbp niet van toepassing verklaart op de verwerking van persoonsgegevens in het kader van de politietaak, lijkt deze wet niet of nauwelijks een rol te spelen bij de verwerking van persoonsgegevens in het kader van het dataminingsproces. De invloed van de Wbp is echter groter dan art. 2 sub *c* Wbp doet vermoeden. De WPolr is namelijk gebaseerd op de uitgangspunten van de oude Wpr. De vervanging van de Wpr door de Wbp heeft daarmee ook gevolgen voor de WPolr. In tegenstelling tot de Wpr heeft de Wbp het begrip ‘gegevensverwerking’ als aangrijppunt<sup>23</sup>; het object van regelgeving is niet langer de ‘persoonsregistratie’ maar de ‘verwerking van persoonsgegevens’ in al haar stadia<sup>24</sup>. Onder de terminologie ‘handelingen met betrekking tot persoonsgegevens’ uit de begripsomschrijving van de Wbp dienen te worden verstaan alle verwerkingen waaraan persoonsgegevens kunnen worden onderworpen. Nader onderscheid op basis van het doel of de methode van verwerking speelt geen rol. Ook verwerkingen van persoonsgegevens die niet zijn gericht op individuele personen vallen onder de begripsomschrijving<sup>25</sup>. Op het moment van schrijven is de WPolr op een aantal punten aangepast aan de Wbp. Daarmee is echter nog niet volledig voorzien in de (nieuwe) benadering van de bescherming van de persoonlijke levenssfeer zoals die door de Wbp wordt voorgestaan. De aparte wettelijke regeling in de WPolr voor de verwerking van persoonsgegevens in het kader van de politietaak dient gebaseerd te zijn op, c.q. overeen te stemmen met, de nationale en internationale uitgangspunten inzake de bescherming van de persoonlijke levenssfeer. Daarom zal bij de bespreking van de WPolr waar nodig steeds rekening worden gehouden met de indirecte invloed van de Wbp.

#### *Resumerend*

Een verwerking van persoonsgegevens in het kader van de opsporingstaak gaat in beginsel gepaard met een inbreuk op de persoonlijke levenssfeer. Een dergelijke verwerking dient in overeenstemming te zijn met de nationale en internationale wet- en regelgeving. Dit heeft (beperkende) gevolgen voor de toepassing van het dataminingsproces, nu daarbij sprake is van een verwerking van persoonsgegevens waarbij een inbreuk op de persoonlijke levenssfeer van de burger in enig stadium onvermijdelijk is. Bovendien zal er vaak sprake zijn van een verwerking van gegevens voor een ander doel dan waarvoor zij zijn vastgelegd. Een dergelijke verwerking dient te berusten op een wettelijke grondslag.

In art. 10 Gw wordt niet aangegeven onder welke omstandigheden een verwerking van persoonsgegevens is toegestaan. Bij een verwerking in het kader van de opsporingstaak dient hiervoor indirect te worden gekeken naar de Wbp en direct naar de WPolr en het bijbehorende BPolr, welke samen een (uitputtende) regeling vormen voor de verwerking

---

23. *Kamerstukken II*, 1997/198, 25 892, nr. 3, p. 7.

24. *Kamerstukken II*, 1997/198, 25 892, nr. 3, p. 16.

25. *Kamerstukken II*, 1997/198, 25 892, nr. 3, p. 51.

van (persoons)gegevens door opsporingsautoriteiten in het kader van de politietaak. Zo bevat art. 4 WPolr een dubbel noodzakelijkheids criterium met betrekking tot (1) de aanleg van een politieregister en (2) de persoonsgegevens die erin worden opgenomen. De aanleg van een register dient te worden gerechtvaardigd door een zwaarwegend maatschappelijk belang en in overeenstemming te zijn met de eisen van proportionaliteit en subsidiariteit. Dit betekent dat de aanleg van een register in verhouding moet staan tot het doel dat ermee wordt nagestreefd (proportionaliteit) en dat niet op een minder ingrijpende wijze kan worden bereikt (subsidiariteit). Hoewel het vergaren van gegevens niet wordt geregeld door de WPolr en het BPolr, vormen deze voor een belangrijk deel het juridische kader waarbinnen het dataminingsproces zich dient af te spelen. Hierna wordt onderzocht welke bepalingen in de WPolr en het bijbehorende BPolr direct dan wel indirect van invloed zijn op de toepassing van het dataminingsproces ten behoeve van de opsporingstaak.

#### 4.2 De Wet Politiregisters

De voortschrijdende automatisering van de politieregisters en het feit dat deze uiterst gevoelige informatie bevatten deden de behoefte ontstaan aan een wettelijke regeling, hetgeen heeft geresulteerd in de WPolr. De uitvoeringsbepalingen ter completering van de WPolr zijn te vinden in het BPolr. Volgens de WPolr is een (politie)register ‘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 ten dienste van de uitvoering van de politietaak’<sup>26</sup>. De politietaak ziet op de taakstelling zoals beschreven in art. 2 Politiewet 1993. In overeenstemming met de terminologie van de Wbp spreekt de WPolr niet langer over ‘een persoonsregistratie’ maar over ‘persoonsgegevens’<sup>27</sup>. Voor de definiëring van het begrip ‘persoonsgegevens’ wordt verwezen naar wat daaronder in de Wbp wordt verstaan<sup>28</sup>. Op het moment van schrijven (2005) bestaat geen wettelijke regeling die specifiek voorziet in de toepassing van dataminingsonderzoek. In plaats van het techniekafhankelijke begrip ‘datamining’ kan vanuit een functionele benadering van de materie worden gesproken van ‘een verwerking van gegevens ten behoeve van de politietaak’.<sup>29</sup> Dit is immers wat er feitelijk gebeurt in het kader van een dataminingsonderzoek. De WPolr en het BPolr voorzien gedeeltelijk reeds in een zodanige verwerking.

---

26. Art. 1 lid 1 sub *b* WPolr.

27. *Kamerstukken II*, 2000/01, 26 410, nr. 150, p. 3. Met het oog op de Wbp is art. 1 WPolr herzien. Verwijzingen naar de Wpr zijn vervangen door een verwijzing naar de Wbp. Dit betekent onder meer dat als ‘persoonsgegeven’ wordt aangemerkt wat daaronder wordt verstaan in de Wbp.

28. Art. 1 lid 1 sub *i* WPolr.

29. Het in hoofdstuk 13 te bespreken wetsvoorstel inzake de verwerking van politiegegevens (Wet politiegegevens) dat strekt ter vervanging van de WPolr gaat in navolging van de Wbp uit van het ‘verwerken’ van gegevens.

Deze wettelijke regeling kan richtinggevend en mogelijk ook richtingbepalend zijn voor de toepassing van het dataminingsproces ten behoeve van de opsporingstaak. Onderstaand de uitkomsten van het onderzoek naar de vraag, in hoeverre dat daadwerkelijk het geval is.

#### *4.2.1 Algemene voorwaarden dataminingsonderzoek*

Een dataminingsonderzoek neemt een aanvang met de aanleg van het datawarehouse. Wanneer in dit onderzoek wordt gesproken over ‘het datawarehouse’ wordt daarmee aangegeven het geheel van gegevens dat in het kader van het dataminingsonderzoek zal worden bewerkt. Een datawarehouse kan worden aangemerkt als een politieregister in de zin van art. 1 lid 1 sub *b* WPolr. Dit betekent dat de regels die gelden voor de aanleg en onderhoud van een politieregister ook van toepassing zijn bij de aanleg van een datawarehouse. In deze sectie wordt onderzocht welke algemene voorwaarden de WPolr en het BPolr stellen aan de aanleg van een politieregister en daarmee aan een datawarehouse. In het hierna volgende hoofdstuk wordt dieper ingegaan op de juridische aspecten van het datawarehouse.

##### *4.2.1.1 Aanleg en inhoud politieregister*

De WPolr bevat geen uitputtende regeling met betrekking tot de inhoud van de politieregisters. Wel stelt art. 4 WPolr beperkingen aan de aanleg van een politieregister en de gegevens die erin mogen worden opgenomen. De aanleg van een politieregister is slechts toegestaan voor een bepaald doel en voor zover dat noodzakelijk is voor een goede uitvoering van de politietaak. Dit betekent dat niet onbeperkt registers kunnen worden aangelegd en dat bestaande registers hun grond moeten vinden in de politietaak. Voorts mag een register alleen persoonsgegevens bevatten die rechtmatig zijn verkregen en die noodzakelijk zijn voor het doel waarvoor het register is aangelegd. Dit noodzakelijkheidscriterium geldt niet alleen met betrekking tot nieuw aan te leggen registers maar ook voor het opnemen van gegevens in een eenmaal aangelegd register. Voor het dataminingsproces betekent art. 4 WPolr dat bij de aanleg van een datawarehouse dient te zijn voldaan aan het daar geregelde dubbele noodzakelijkheidscriterium.

De aanleg van een datawarehouse vindt, als onmisbaar onderdeel<sup>30</sup> van het dataminingsproces, plaats met het doel een bijdrage te leveren aan de opsporingstaak. Dit kan op twee manieren. Ten eerste kan het proces van dataminingsbijdragen aan de verbetering van de politieke informatiepositie als geheel. In dat geval wordt gebruik gemaakt van de ongerichte dataminingsvariant. In de tweede plaats kan door de toegevoegde (informatie)waarde van het dataminingsonderzoek in een bepaalde zaak een gerichte verbetering

---

30. Namelijk het voorbereidende stadium van het dataminingsproces; zie sectie 5.1.1 voor enige relativerende opmerkingen hieromtrent.

van de informatiepositie worden bewerkstelligd. Hiervan is sprake wanneer gebruik wordt gemaakt van gericht dataminingonderzoek.<sup>31</sup> Om de politietaak, in dit geval de strafrechtelijke handhaving van de rechtsorde, op een zo efficiënt mogelijke manier te kunnen uitvoeren, is het verkrijgen en handhaven van een goede informatiepositie onontbeerlijk. In dat licht wordt met de aanleg van een datawarehouse in beginsel voldaan aan art. 4 WPolr. Zonder een goede informatiepositie is het voor de opsporingsautoriteiten vrijwel onmogelijk om hun taak naar behoren uit te voeren, ongeacht of het daarbij gaat om een individueel geval of om de opsporingstaak in het algemeen. De mogelijkheden van het dataminingsproces, en daarmee de aanleg van een datawarehouse, zijn onontbeerlijk voor een goede uitvoering van de opsporingstaak. Verder dienen de gegevens in het datawarehouse noodzakelijk te zijn voor het doel dat wordt nagestreefd met het dataminingonderzoek in het kader waarvan het datawarehouse is aangelegd. Met het oog op het bepaalde in art. 8 EVRM dient bij de aanleg van een datawarehouse rekening te worden gehouden met de beginselen van proportionaliteit en subsidiariteit. De aanleg van een register dient in een juiste verhouding te staan tot het doel waarvoor het register wordt aangelegd (proportionaliteit).<sup>32</sup> Daarnaast mag dit doel niet op een minder ingrijpende wijze kunnen worden bereikt (subsidiariteit).<sup>33</sup>

#### 4.2.1.2 *Het reglement*

Voor elk register dient een reglement te worden vastgesteld na overleg met het gezag dat verantwoordelijk is voor de uitvoering van de politietaak ten dienste waarvan het register wordt aangelegd. Een register treedt pas in werking nadat een reglement is opgesteld.<sup>34</sup> Dit is alleen anders in het geval van een tijdelijk register, dat kan worden aangelegd voor

---

31. En in zekere zin bij verificatie.

32. Het verkrijgen en handhaven van een goede informatiepositie is van essentieel belang voor de opsporing. Dit belang zal in bepaalde gevallen prevaleren boven het belang van de burger op niet-inmenging in zijn persoonlijke levenssfeer door de overheid. Om de overheid de mogelijkheid te geven de opsporingstaak met succes ten uitvoer te brengen, dient de burger tot op zekere hoogte concessies te doen met betrekking tot de bescherming van zijn fundamentele rechten. Het gebruik van persoonsgegevens ten behoeve van de opsporing is slechts toegestaan en proportioneel in de zin van art. 8 EVRM, wanneer dat gebruik door regels wordt beperkt en met voldoende waarborgen is omkleed.

33. Aan de subsidiariteitseis van art. 8 EVRM wordt voldaan wanneer het doel van het dataminingonderzoek niet op een minder ingrijpende wijze kan worden bereikt. De behoefte om gebruik te maken van de mogelijkheden van dataminingonderzoek ontstaat voornamelijk door de toenemende omvang en automatisering van gegevens die bij de politie aanwezig zijn of waarover men op een andere wijze kan beschikken. Zonder gebruikmaking van een technisch hulpmiddel als datamining is het zeer moeilijk, zometeen onmogelijk, om al deze gegevens op een vergelijkbare efficiënte wijze te benutten. Een datawarehouse wordt aangelegd in het kader van een dataminingonderzoek. Omdat de verbetering van de informatiepositie die met behulp van het dataminingsproces kan worden bewerkstelligd niet op een andere, minder ingrijpende manier kan worden bereikt, zal zijn voldaan aan de eis van subsidiariteit.

34. Art. 9 lid 5 WPolr.

de uitvoering van de opsporingstaak in een bepaald geval.<sup>35</sup> Het reglement heeft zowel een voorlichtende als een normerende functie. Alvorens het in werking treedt, dient een exemplaar aan het College bescherming persoonsgegevens (CBP) te worden toegezonden.<sup>36</sup> Het CBP houdt toezicht op de werking van de politieregisters in overeenstemming met het bij of krachtens de WPolr bepaalde. Daarnaast ziet zij toe op de bescherming van de persoonlijke levenssfeer in het algemeen. Uit de formulering van de WPolr blijkt, dat het CBP in deze hoedanigheid een controlerende functie vervult<sup>37</sup>. In het reglement dient de werking van het register te zijn beschreven en dienen de volgende onderwerpen te worden geregeld:

- a. het doel van het register;
- b. de categorieën van personen over wie gegevens worden opgenomen en de soorten van de over hen op te nemen gegevens;
- c. de gevallen waarin opgenomen gegevens worden verwijderd;
- d. de vernietiging, zodra dit mogelijk is, van verwijderde gegevens;
- e. eventuele verbanden tussen het register en enige andere gegevensverzameling;
- f. de wijze waarop geregistreerde personen of hun wettelijke vertegenwoordigers kennisgeving en verbetering van de over hen opgenomen gegevens kunnen verkrijgen;
- g. de bevoegdheid tot het invoeren en wijzigen van gegevens in, alsmede het verwijderen van gegevens uit het register;
- h. de aanwijzing van degene die onder verantwoordelijkheid van de beheerder is belast met de zeggenschap over het register en de omschrijving van de daaruit voortvloeiende bevoegdheden;
- i. de aanwijzing van degene of degenen belast met de dagelijkse leiding van het register.

In de reglementen wordt de korpschef standaard aangewezen als registerbeheerder. De autorisatie voor toegang tot het register, de registratie en verwijdering van gegevens, evenals de aanduiding van de betrouwbaarheid van gevoelige gegevens, wordt gedelegeerd aan degene die de dagelijkse leiding heeft.<sup>38</sup>

#### *4.2.1.3 Datawarehouse en reglement*

Alvorens een datawarehouse operationeel kan worden, dient op grond van art. 9 lid 5 WPolr een reglement voor dat register te worden opgesteld. Omdat een datawarehouse een onmisbaar onderdeel van het dataminingsproces vormt, kan het dataminingsonder-

---

35. Art. 13 WPolr.

36. Met de inwerkingtreding van de Wbp op 1 september 2001 is de naam van de Registratiekamer veranderd in College bescherming persoonsgegevens (CBP).

37. Zie bijvoorbeeld art. 5 lid 3, art. 6 lid 2, tweede volzin, art. 9 lid 4, en art. 21 lid 3, tweede volzin, WPolr.

38. *Parlementaire Enquêtecommissie Opsporingsmethoden*, beheer van registers, sturing en controle, bijlage V.

zoek in beginsel geen doorgang vinden wanneer geen reglement aanwezig is. Voorafgaand aan het in werking treden van het reglement dient een exemplaar daarvan te worden toegezonden aan het CBP.<sup>39</sup> De aard van het reglement van een datawarehouse wordt mede bepaald door de variant van het dataminingsproces in het kader waarvan het datawarehouse is aangelegd. Afhankelijk daarvan heeft het datawarehouse een tijdelijk of een permanent karakter. Aangezien een ongericht dataminingsonderzoek permanent van aard is, heeft ook het datawarehouse dat in het kader daarvan wordt aangelegd een permanent karakter. Aan het doel van het onderzoek, te weten de verbetering van de informatiepositie in het algemeen, kan moeilijk een maximumtermijn worden gesteld. Hoewel het datawarehouse weliswaar voortdurend wordt bijgewerkt waarbij oude gegevens worden verwijderd en nieuwe toegevoegd, blijft het in de kern gaan om hetzelfde register en blijft het bijbehorende reglement onveranderd. Een gericht dataminingsonderzoek is tijdelijk van aard en eindigt op het moment waarop het doel van het onderzoek is bereikt. Het bijbehorende datawarehouse dient dan vernietigd te worden. Evenals het register is ook het reglement daarvan tijdelijk van aard. Een gericht dataminingsonderzoek kan voor zeer uiteenlopende doeleinden worden gebruikt. Daarom zal een datawarehouse dat in het kader daarvan wordt aangelegd, steeds andere gegevens bevatten.

#### 4.2.1.4 *Het modelreglement*

Op twee manieren kan worden voldaan aan de verplichting van art. 9 lid 5 WPolr om een reglement op te stellen. Ten eerste kan voor ieder register afzonderlijk een reglement worden opgesteld. In de praktijk betekent dit dat, alvorens een register in werking kan treden, steeds een nieuw reglement dient te worden gemaakt dat evenzovele malen moet worden voorgelegd<sup>40</sup> aan het CBP. Wanneer opsporingsdiensten voor elk afzonderlijk onderzoek opnieuw het wiel, in dit geval het reglement, moeten uitvinden, komt dat de efficiëntie van de opsporing allerminst ten goede. Aan de reglementplicht kan echter ook worden voldaan door gebruik te maken van een modelreglement.<sup>41</sup> In dat geval dient de beheerder aan het CBP mede te delen, overeenkomstig welk model het reglement is vastgesteld. Het voordeel hiervan is, dat hij niet over de afzonderlijke bepalingen in het reglement vooraf het CBP hoeft te horen en deze instantie evenmin een exemplaar van

---

39. In beginsel dient een reglement steeds te worden voorgelegd aan het CBP. Wanneer zich in de adviezen van het CBP een algemene lijn gaat aftekenen, kan die in de vorm van nadere regels in een AMvB worden vastgelegd. Zo kan voor de verschillende varianten van het dataminingsproces een goede afweging worden gemaakt met betrekking tot de wijze waarop en de voorwaarden waaronder toepassing kan plaatsvinden. Wanneer de opvattingen hieromtrent zowel politiek als juridisch voldoende zijn uitgekristalliseerd, kan het resultaat worden neergelegd in een modelreglement. Op deze wijze wordt, naast de gangbare zaken die in een reglement plegen te worden geregeld, ook voorzien in specifieke eisen die aan een datawarehouse gesteld dienen te worden.

40. Zie art. 9 WPolr.

41. Zie art. 12 WPolr.

het reglement behoeft te sturen. Het gebruik van dergelijke modelregelingen bevordert de uniformiteit en zorgvuldigheid in de omgang met de veelal ‘zachte’ en gevoelige gegevens. Wanneer bepaalde registers frequent worden gebruikt, verdient een modelreglement vanuit het oogpunt van efficiëntie de voorkeur. Voor verschillende opsporingsregisters bestaan inmiddels modelreglementen, bijvoorbeeld de modelreglementen ‘register zware criminaliteit’, ‘voorlopig register’ en ‘informantenregister’<sup>42</sup>. Het CBP is nauw betrokken bij het opstellen van modelreglementen. Wanneer overeenstemming is bereikt over de inhoud van een bepaald modelreglement voor politieregisters kan het CBP een verklaring afgeven dat het model naar haar oordeel in overeenstemming is met het bepaalde bij of krachtens de WPolr. Na afgifte van deze verklaring wordt het model in de *Staatscourant* gepubliceerd.

### Voordelen modelreglement

Wanneer in het geval van een datawarehouse wordt gekozen voor een modelreglement kan daarmee worden voorzien in de benodigde waarborgen ter bescherming van de persoonlijke levenssfeer van de burger. Zo kunnen in het reglement nadere regels worden gesteld met betrekking tot de doelstelling van het register, het beheer, het verstrekkingenregime en de mogelijkheid om te koppelen met andere registers. Ook de betrokkenheid van het CBP bij het opstellen van een modelreglement is een positieve factor. Omdat de gegevens die in aanmerking komen voor de opslag in een datawarehouse in beginsel een gevoelig karakter hebben is het noodzakelijk, dat daar zeer zorgvuldig mee wordt omgegaan. Een intensieve betrokkenheid van het CBP bij de regulering van het gebruik van een datawarehouse is daarom gewenst. Verder draagt een modelreglement bij aan een uniforme werkwijze welke van belang is voor het welslagen van een onderzoek. Het schept duidelijkheid en voorkomt onnodige vertragingen. Bij een proces als datamining, waarbij een goede samenwerking van essentieel belang is, dient te worden voorkomen dat eenieder zelf bepaalt op welke wijze invulling wordt gegeven aan het dataminingsproces. Die invulling vindt nu voor een groot deel al plaats bij het vaststellen van het modelreglement. De frequentie waarmee een bepaald dataminingonderzoek wordt uitgevoerd, is mede bepalend voor de keuze van het reglement. In het geval van een gericht dataminingonderzoek zijn het datawarehouse en het reglement tijdelijk van aard. Voor ieder afzonderlijk geval dient een apart reglement te worden opgesteld. Omdat deze dataminingvariant in de praktijk veelvuldig zal voorkomen, is het onwenselijk dat voor ieder onderzoek het traject van art. 9 lid 5 WPolr moet worden doorlopen. Voor dataminingonderzoek met een hoge gebruiksfrequentie is daarom het gebruik van een modelreglement te prefereren. Hoewel ook in het geval van een ongericht datamining-

---

42. Deze modelreglementen bevatten onder meer bepalingen over het beheer, de verwijdering en vernietiging van gegevens en de rechten van de geregistreerde. Het CBP verklaart dat deze modelreglementen in overeenstemming zijn met het bepaalde bij en krachtens de WPolr. *Stcrt.* 13 oktober 2000, 198, p. 17.

onderzoek gebruik kan worden gemaakt van een modelreglement is de noodzaak daartoe minder groot. Een ongericht dataminingonderzoek heeft in beginsel een permanent karakter, zodat een eenmaal opgesteld reglement ook voor de toekomst volstaat. Een modelreglement is vooral bedoeld voor situaties waarbij telkenmale opnieuw een reglement dient te worden opgesteld. Ten slotte wordt met de keuze voor een modelreglement rekenschap afgelegd voor het feit dat een register dat is aangelegd in het kader van het dataminingsproces op een aantal punten afwijkt van de overige politieregisters. Daarbij betreft het met name verschillen met betrekking tot het doel, het verstrekkingenregime en de gebruiksfrequentie van de registers.

Samenvattend lijkt het vooral in het geval van een gericht dataminingonderzoek wenselijk om gebruik te maken van een modelreglement. Het gebruik van een modelreglement heeft voor een datawarehouse de volgende voordelen:

1. voorzien kan worden in een afdoende bescherming van de persoonlijke levenssfeer;
2. rekening kan worden gehouden met de specifieke kenmerken van het dataminingsproces als geheel, maar ook met die van de verschillende dataminingvarianten afzonderlijk;
3. het CBP is direct betrokken bij de totstandkoming van een modelreglement;
4. het bevordert een uniform gebruik van het dataminingsproces in het algemeen en van de aanleg van een datawarehouse in het bijzonder;
5. het draagt bij aan een efficiënte toepassing van het dataminingsproces, welk effect het sterkst merkbaar zal zijn bij dataminingonderzoek met een hoge gebruiksfrequentie.

#### *4.2.2 Voorwaarden voor het verwerken van gegevens*

De in de vorige sectie besproken voorwaarden zien vooral op de aanvang van het dataminingonderzoek en het in het kader daarvan te realiseren datawarehouse. In deze sectie wordt ingegaan op de invloed van de WPolr en het BPolr op de verwerking van gegevens in het kader van het dataminingonderzoek. Opgemerkt zij dat de WPolr en het BPolr geen bepalingen c.q. bevoegdheden bevatten betreffende het vergaren van gegevens. Er wordt 'slechts' geregeld op welke manier de politie met gegevens dient om te gaan. Omdat deze regeling ook van betekenis is voor de samenstelling van het datawarehouse, zijn de WPolr en het BPolr medebepalend voor de gegevens die in het kader van een dataminingonderzoek mogen worden verwerkt.

##### *4.2.2.1 Het gebruik van persoonsgegevens*

Bij de aanleg van een datawarehouse in het kader van de opsporingstaak worden onvermijdelijk ook persoonsgegevens verwerkt. Omdat het dataminingonderzoek plaatsvindt in het kader van de opsporing is het noodzakelijk dat de informatie die daarbij wordt verwerkt, teneinde tot een eventuele strafrechtelijke sanctie te kunnen komen, op enig

moment herleidbaar is tot een individu. Wanneer dat niet het geval is kan de verkregen kennis alleen ten behoeve van fenomeenonderzoek worden gebruikt; daarbij verkregen resultaten zijn groepsgericht met als uiteindelijk doel profilering, terwijl het strafrecht juist op het individu is gericht.

Ter bescherming van de persoonlijke levenssfeer stelt de WPolr beperkingen aan het gebruik van persoonsgegevens. Zo mag een politieregister, en daarmee een datawarehouse, op grond van art. 4 lid 2 WPolr slechts persoonsgegevens bevatten die rechtmatig zijn verkregen. Verder dient het gebruik ervan noodzakelijk te zijn voor het doel waarvoor het politieregister is aangelegd. Voor de opslag van persoonsgegevens in een datawarehouse betekent dit expliciet, dat het gebruik daarvan noodzakelijk moet zijn met het oog op het doel waarvoor het dataminingonderzoek plaatsvindt. Bij de toepassing van dataminingonderzoek in het kader van de opsporing betreft deze doelstelling in beginsel de verbetering van de informatiepositie van de opsporingsdiensten, welke de basis vormt voor een effectieve en efficiënte opsporing.

#### *4.2.2.2 Registratie op grond van bepaalde kenmerken*

De mogelijkheid om persoonsgegevens in politieregisters vast te leggen wordt ook beperkt door art. 5 WPolr. Op grond van dat artikel is de registratie van personen wegens hun godsdienst of levensovertuiging, ras, politieke gezindheid, seksualiteit, intiem levensgedrag, of op grond van medische of psychologische kenmerken niet toegestaan. Het feit dat een categorische registratie op grond van deze gevoelige persoonsgegevens niet is toegelaten betekent niet, dat dergelijke gegevens in het geheel niet in politieregisters mogen voorkomen. Het bepaalde in art. 5 WPolr ziet op de situatie waarin registratie uitsluitend plaatsvindt op grond van één der genoemde kenmerken. Wanneer aanvulling op andere persoonsgegevens en voor zover het voor het doel van het register onvermijdelijk is, is op grond van het tweede lid van art. 5 WPolr opname van de genoemde persoonsgegevens in een politieregister wel mogelijk. Ook kan bij de aanleg van een datawarehouse worden uitgegaan van één bepaald kenmerk, zolang het daarbij maar niet één van de in art. 5 lid 1 WPolr genoemde kenmerken betreft. Zo is de aanleg van een register met daarin namen van ‘beruchte’ voetbalsupporters (in het kader van het EK 2000) niet in strijd met art. 5 WPolr. Over bepalingen daaromtrent in het reglement van het register dient vooraf het CBP te worden gehoord. In art. 3 BPolr is bepaald dat het reglement uitdrukkelijk toestemming dient te geven tot de opname van gevoelige persoonsgegevens en wordt het gebruik van persoonsgegevens met betrekking tot iemands ras verder beperkt. Persoonsgegevens met betrekking tot iemands ras<sup>43</sup> mogen

---

43. Het begrip ‘ras’ heeft hier dezelfde betekenis als in art. 1 Gw en moet mede worden gezien in het licht van het Internationaal Verdrag inzake de Uitbanning van Alle Vormen van Rassendiscriminatie. Het begrip ‘ras’ omvat als gevolg van dit verdrag ook huidskleur, afkomst en nationale of etnische afstamming van de geregistreerde.

alleen worden opgenomen indien dit onvermijdelijk is met het oog op de identificatie van de betreffende persoon, voor de juiste beoordeling van een strafbaar feit en wanneer zulk een gegeven het slachtoffer of de motieven van de dader van dat feit betreft, dan wel met het oog op de hulpverlening door de politie.<sup>44</sup> Bij opname van een gegeven als bedoeld in art. 5 lid 1 WPolr dient tevens een aanduiding betreffende de betrouwbaarheid van het gegeven te worden opgenomen.

#### 4.2.2.3 *Het gebruik van zachte opsporingsinformatie*

Naast het onderscheid tussen gevoelige en niet-gevoelige gegevens kan, met betrekking tot de aard van de gegevens worden onderscheiden naar harde en zachte opsporingsgegevens. Harde gegevens hebben een betrouwbaar karakter; bij zachte gegevens is daarvan (nog) geen sprake. De term ‘zachte gegevens’ is van toepassing op gegevens waarvan de juistheid (nog) niet vaststaat.<sup>45</sup> Opsporingsinstanties zullen in bepaalde gevallen gebruik moeten maken van zachte opsporingsinformatie. Om een goed zicht te kunnen krijgen op de aard en omvang van de zware criminaliteit, in het bijzonder de georganiseerde criminaliteit, is het bijvoorbeeld noodzakelijk om allerlei gegevens over personen op te slaan, waaronder vooral zachte informatie. Er dient daarbij steeds een afweging te worden gemaakt tussen enerzijds het opsporingsbelang en anderzijds het belang van de bescherming van de persoonlijke levenssfeer van de burger. Met het oog hierop wordt het gebruik van zachte gegevens beperkt door art. 5a WPolr. Het opnemen van gegevens over onverdachte personen (ongeacht om welk strafbaar feit het gaat) in een politieregister dat is aangelegd voor de strafrechtelijke handhaving van de rechtsorde is slechts toegestaan in overeenstemming met dit artikel.

Wanneer art. 5a WPolr spreekt van ‘gegevens omtrent onverdachte personen’ wordt daarmee niet bedoeld op een wettelijke tegenpool van het verdachtebegrip van art. 27 Sv in de zin, dat daaronder alle personen die geen verdachte (als bedoeld in art. 27 Sv) zijn worden verstaan. Tot de categorie van personen als bedoeld in art. 5a lid 1 WPolr behoren slechts diegenen over wie de politie gegevens heeft verkregen of vergaard die duiden op betrokkenheid bij strafbare feiten, maar waaruit nog geen redelijk vermoeden voortvloeit dat zij bepaalde feiten hebben begaan.<sup>46</sup> In art. 5a lid 1 WPolr is de mogelijkheid opengelaten om zodanige opsporingsinformatie ook vast te leggen in een register van het Meldpunt ongebruikelijke transacties. Verder kunnen dergelijke gegevens over midden-criminaliteit (zoals straatroven en woninginbraken) tijdelijk worden vastgelegd in een

---

44. Art. 3 lid 2 BPolr.

45. *Kamerstukken II*, 1996/197, 25 398, nr. 3, p. 5.

46. Dit in tegenstelling tot het *Rapport Gegevensuitwisseling en Terrorismebestrijding* 2003, waarin de gegevens onder 13a lid 1 sub b WPolr eveneens worden aangemerkt als gegevens omtrent onverdachte personen. Deze subjecten vallen echter niet binnen de definitie van het begrip ‘onverdachte personen’ (*Kamerstukken I*, 1998/199, 25 398, nr. 63b, p. 6-7).

gewoon politieregister.<sup>47</sup> In dat geval gelden nadere beperkingen voor het gebruik van de gegevens.<sup>48</sup> Na vier maanden dient die informatie uit de gewone politieregisters te worden verwijderd. Daarmee wil de wetgever voorkomen dat tot dan toe onbevestigd gebleven lichte aanwijzingen van betrokkenheid bij een strafbaar feit na vier maanden voor elke politieagent opvraagbaar zijn, zonder dat een onderzoek is ingesteld waaruit de redelijke verdenking van het begaan van een strafbaar feit voortvloeit. De langdurige opslag van zachte opsporingsinformatie is alleen mogelijk in een bijzonder politieregister, zoals het register zware criminaliteit, of een tijdelijk register dat is aangelegd in het kader van een concreet onderzoek.<sup>49</sup> Nadat bepaalde gegevens vier maanden in een regulier politieregister opgeslagen zijn geweest, mag worden besloten tot de aanleg van een tijdelijk register ten behoeve van een voortgezette opslag van de betreffende gegevens. Het is echter zeer wel mogelijk dat gedurende de registratie van vier maanden meer informatie is verkregen waardoor de gegevens hun zachte karakter hebben verloren.<sup>50</sup>

#### **Bescherming van de persoonlijke levenssfeer versus art. 5a WPolr**

In beginsel dient een verwerking van zachte gegevens te kunnen worden gerechtvaardigd door het doel van het onderzoek waarvan zij deel uitmaken. Met betrekking tot de verwerking van zachte opsporingsinformatie is dit over het algemeen enkel het geval bij de bestrijding van de zwaardere vormen van criminaliteit. De mogelijkheid van art. 5a WPolr om zachte gegevens gedurende een termijn van vier maanden in een gewoon politieregister op te kunnen slaan, staat hiermee op gespannen voet. De ‘free flow’ van in een gewoon politieregister bewaarde informatie betekent dat het gebruik van de gegevens niet expliciet is beperkt tot de zware vormen van criminaliteit, maar dat het gehele politieapparaat er in beginsel, ongeacht het doel, gebruik van kan maken. Daarmee is de mogelijkheid gecreëerd om zachte gegevens te verwerken voor onderzoek, waarvan het doel niet opweegt tegen de inbreuk die met het gebruik daarvan gepaard gaat. Aan deze situatie komt pas na een termijn van vier maanden een einde. Het ontbreken van een wettelijk vastgelegde beperking met betrekking tot het gebruik van zachte gegevens in combinatie met het bepaalde in art. 5a WPolr houdt in de praktijk dus in, dat een afdoende bescherming van de persoonlijke levenssfeer pas na vier maanden ingaat.

Vanwege de dubbele noodzaak om zorgvuldig met de gegevens om te gaan, dienen strenge beperkingen te worden gesteld aan de verwerking ervan. Immers, de gegevens die

47. Zie ook Kruissink, Verwers & Dijkhoff 1998, “Alle korpsen bekijken het werkaanbod in termen van de bekende driedeling: veel voorkomende criminaliteit aan de ene kant, zware en georganiseerde criminaliteit aan de andere kant, met daartussen het ‘middengebied’, door de korpsen ook vaak aangeduid als de middencriminaliteit of lokaal ernstige criminaliteit”.

48. Art. 5a lid 2 WPolr.

49. In overeenstemming met het bepaalde in par. 3a WPolr.

50. CBP 2001.

mogelijk betrekking hebben op onschuldige burgers zijn niet alleen gevoelig, maar ook onbetrouwbaar van aard. In het licht daarvan lijkt het gebruik van een gewoon politieregister voor zowel een langdurige als een tijdelijke opslag van zachte opsporingsinformatie onwenselijk. Van de mogelijkheid van art. 5a WPolr zou met name gebruik moeten worden gemaakt voor de vaststelling van de aard van nieuw binnengekomen gegevens. Na deze eerste analyse kan worden bepaald of de gegevens in aanmerking komen voor (voortgezette) registratie in een politieregister en zo ja, welk register. Wanneer in het reglement van een gewoon politieregister beperkingen worden opgenomen met betrekking tot het gebruik van eventuele zachte gegevens, lijkt het in art. 5a WPolr bepaalde minder bezwaarlijk. Het is echter de vraag of die beperkingen verenigbaar zijn met de 'free flow' van informatie in reguliere politieregisters. Het is in beginsel onwenselijk dat de gegevens in dit register bestemd zijn voor operationeel gebruik. Overwogen zou kunnen worden om het gebruik van dit register te beperken tot het doel waarvoor het is aangelegd: een analyse.<sup>51</sup>

#### **Zachte opsporingsinformatie en dataminingonderzoek**

Of en in hoeverre het is toegestaan om in het kader van een dataminingonderzoek ten behoeve van de opsporing gebruik te maken van zachte opsporingsinformatie, hangt af van het doel van het onderzoek en de van toepassing zijnde dataminingvariant.

Een ongericht dataminingonderzoek moet een verbetering van de informatiepositie opleveren. Het kan daarbij gaan om een verbetering van de informatiepositie binnen het politieapparaat als geheel, maar ook om die van een bepaald politieregister. In het laatste geval maakt de beheerder van een register gebruik van dataminingonderzoek om de in zijn register opgeslagen gegevens zo optimaal mogelijk te gebruiken. Het gebruik van zachte gegevens in het kader van een ongericht dataminingonderzoek is in beginsel uitgesloten aangezien het doel daarvan de, met het gebruik van deze gegevens gepaard gaande, inbreuk op de persoonlijke levenssfeer niet rechtvaardigt. Uitzondering daarop is slechts mogelijk wanneer met het ongerichte dataminingonderzoek wordt gestreefd naar een informatieoptimalisatie van een register zware criminaliteit, een voorlopig politieregister of een ander register waarin per definitie zachte gegevens liggen opgeslagen. In die registers wordt immers al voorzien in de beperkingen die met betrekking tot een verwerking van zachte gegevens in acht dienen te worden genomen.

Een gericht dataminingonderzoek ziet in beginsel op een strafvorderlijke afdoening en niet op een verbetering van de politieke informatiepositie. Deze dataminingvariant kan worden ingezet bij de bestrijding van criminele gedragingen en is ingrijpender van aard, hetgeen onder meer blijkt uit het feit dat het gebruik van zachte opsporingsgegevens is

---

51. Zie ook sectie 9.2.

toegestaan. Teneinde een afdoende bescherming te bieden tegen al te vergaande inbreuken op de rechten van de burger is het gebruik van deze dataminingvariant evenwel aan strengere voorwaarden gebonden.

#### **Wenselijkheid verwerking zachte gegevens**

Een dataminingonderzoek is in beginsel gericht op het verkrijgen van een zo betrouwbaar mogelijk resultaat. Het gebruik van zachte, onbetrouwbare opsporingsgegevens kan de efficiëntie en betrouwbaarheid van het dataminingonderzoek negatief beïnvloeden en is derhalve in principe ongewenst. De aard van de input, het datawarehouse, is immers mede bepalend voor de output, het resultaat. Voor een zo goed mogelijk resultaat dient, waar mogelijk, gebruik te worden gemaakt van bijgewerkte, opgeschoonde en betrouwbare gegevens. Een betrouwbaar resultaat behoeft echter per definitie niet ook een optimaal resultaat te zijn. Afhankelijk van het doel dat in een bepaald geval wordt nagestreefd kan het wenselijk zijn om gebruik te maken van zachte opsporingsinformatie. Zo is het denkbaar dat verschillende kleine puzzelstukjes van op zichzelf niet honderd procent betrouwbare gegevens in onderlinge samenhang wel een betrouwbaar resultaat opleveren. Vooral bij de bestrijding van de zware criminaliteit is het vaak noodzakelijk om (ook) van zachte gegevens gebruik te maken. Wanneer uit een geheel van fragmentarische zachte gegevens harde kennis wordt verkregen komt dit ten goede aan het eindresultaat van het onderzoek. Voor elk specifiek onderzoek zal opnieuw een afweging moeten worden gemaakt of het gebruik van zachte gegevens al dan niet bijdraagt aan een optimaal resultaat. De uitkomsten van een dataminingonderzoek waarbij de gebruikte gegevens deels of volledig onbetrouwbaar zijn zullen over het algemeen niet doorslaggevend zijn, maar kunnen wel waardevolle kennis opleveren en de aanzet vormen voor verder onderzoek.

#### *4.2.2.4 Koppeling*

Een onontbeerlijk onderwerp in het kader van dit onderzoek is de koppeling van gegevens(verzamelingen) als geregeld in art. 6 WPolr. Hoewel in hoofdstuk 6 uitvoerig zal worden ingegaan op de koppeling komt hier reeds een aantal aspecten van deze regeling ter sprake. Met art. 6 WPolr is een regeling getroffen voor de koppeling van een politieregister met een ander politieregister of een andere verzameling van persoonsgegevens. Een koppeling is evenwel slechts mogelijk wanneer dit noodzakelijk is voor een goede uitvoering van de politietaak. Onder het begrip ‘koppeling’ verstaat de WPolr<sup>52</sup>: ‘het treffen van technische of organisatorische voorzieningen, waardoor verschillende verzamelingen van persoonsgegevens systematisch met elkaar kunnen worden vergeleken’. Gezien hun aard zullen dergelijke nauwe verbanden voornamelijk kunnen en worden gelegd tussen geautomatiseerde verzamelingen van persoonsgegevens. Voor de vraag of er

---

52. Art. 1 lid 1 sub *d* WPolr.

sprake is van een koppeling is het niet noodzakelijk dat de onbeperkte beschikking wordt verkregen over gegevens in een ander register. Ook de verstrekking van ‘slechts’ een namenindex kan als een koppeling worden aangemerkt. Bepalend is dat een vergelijking plaatsvindt van gegevens uit twee of meer registers ter verkrijging van informatie over een onbepaalde groep van personen welke niet aan één van de betrokken registers afzonderlijk kan worden ontleend<sup>53</sup>. Indien over een bepaalde persoon informatie uit verschillende registers wordt verzameld, is er geen sprake van een juridische koppeling in de zin van art. 6 WPolr. Ook wanneer het resultaat van het raadplegen van deze registers leidt tot het zichtbaar worden van de verlangde gegevens op hetzelfde beeldscherm, is in juridische zin sprake van raadpleging (ook al wordt in dit verband in technische zin wel gesproken van koppeling).<sup>54</sup>

### Datawarehouse

In een datawarehouse kunnen verschillende gegevensverzamelingen, hetzij politieregisters, hetzij andere verzamelingen van persoonsgegevens, worden samengebracht of gekoppeld. Het kan daarbij gaan om een koppeling van gehele gegevensbestanden, maar ook om gedeelten daarvan. De WPolr spreekt in art. 1 lid 1 sub *d* namelijk niet over een vergelijking van ‘registraties’ maar over een vergelijking van ‘verzamelingen van persoonsgegevens’. Deze keuze dient waarschijnlijk om aan te geven, dat het vergelijken van delen van registraties die geen nieuwe registraties vormen ook onder het wettelijke koppelingsbegrip zijn gebracht.<sup>55</sup> Wanneer de definities van het dataminingsproces en de koppeling van art. 6 WPolr naast elkaar worden gezet kan worden geconcludeerd, dat de koppeling betrekking heeft op het voorbereidende deel van het dataminingsproces. Het koppelen van bestanden vindt plaats met het oog op een verdere analyse van de gegevens en heeft in dat verband een voorbereidend karakter. Het aanleggen van een datawarehouse in het kader van een dataminingsonderzoek kan als een dergelijke voorbereidende handeling worden aangemerkt. Zowel in de WPolr als in het BPolr worden beperkingen gesteld aan de koppeling van gegevensverzamelingen. Gezien het voorgaande dient daar ook rekening mee te worden gehouden bij de aanleg van een datawarehouse in het kader van een dataminingsonderzoek. Uitzondering daarop is wanneer het dataminingsonderzoek zich beperkt tot één enkele gegevensverzameling; in dat geval is namelijk geen sprake van een koppeling zoals bedoeld in art. 6 WPolr. Het hiernavolgende handelt over de betekenis van de koppelingsregeling in relatie tot de aanleg van een datawarehouse.

---

53. *Kamerstukken I*, 1998 /99, 25 398, nr. 63*b*, p. 8.

54. *Kamerstukken II*, 1988 /89, 19 589, nr. 6, p. 10.

55. Verbeek e.a. 1999, p. 170-171.

### Politietask

Een koppeling is toegestaan indien dat noodzakelijk is voor een goede uitvoering van de politietask. Het datawarehouse vormt een onmisbaar onderdeel van het dataminingsproces, waarmee een belangrijke bijdrage kan worden geleverd aan de informatiepositie van de opsporingsautoriteiten. Een goede informatiepositie is een voorwaarde voor een succesvolle uitvoering van de opsporingstask. Een koppeling welke plaatsvindt ten behoeve van de aanleg van een datawarehouse in het kader van een dataminingsonderzoek kan daarom worden aangemerkt als noodzakelijk voor een goede uitvoering van de politietask.

### Reglement en de plicht tot reglement

Een koppeling van gegevensverzamelingen is in beginsel slechts toegestaan indien en voor zover de reglementen van de betreffende registers in deze mogelijkheid voorzien.<sup>56</sup> Een tijdelijk politieregister vormt hierop een uitzondering.<sup>57</sup> Over de bepalingen in een reglement dient vooraf het CBP te worden gehoord. Indien zich in het advies van het CBP een algemene lijn gaat aftekenen is het dienstig om deze in de vorm van nadere regels in een AMvB vast te leggen.<sup>58</sup> Over het algemeen is het koppelen van gegevensbestanden met een verwant doel minder bezwaarlijk dan een koppeling van gegevensbestanden die met een verschillend oogmerk zijn aangelegd.<sup>59</sup> Indien dit noodzakelijk is voor de opsporing van een misdrijf waardoor de rechtsorde ernstig is geschokt, kan de MvJ toestemming geven tot een koppeling zonder dat het reglement hierin voorziet<sup>60</sup>. In dat geval prevaleert het belang van de opsporing boven het privacybelang. Wanneer bij vergelijking van de gekoppelde registers gegevens worden aangetroffen over meerdere personen die in meer dan één register voorkomen, kan het resultaat van een koppeling een nieuwe tijdelijke registratie zijn in de zin van art. 13 WPolr. Dit register is dan aangelegd voor hetzelfde doel als waarvoor de koppeling plaatsvond. Opgemerkt zij dat een koppeling niet per definitie leidt, dan wel hoeft te leiden, tot het ontstaan van een nieuw politieregister. Er is bijvoorbeeld geen sprake van een nieuw register wanneer de vergelijking van de bij de koppeling betrokken registers leidt tot het resultaat, dat geen van de persoonsgegevens in enig register wordt teruggevonden in een ander bij de koppeling betrokken register.<sup>61</sup>

Voor het dataminingsproces betekent de reglementsplicht in beginsel, dat een gegevensverzameling of een gedeelte daarvan alleen in een datawarehouse kan worden opgeno-

---

56. Art. 6 lid 2 WPolr.

57. Art. 13 lid 3 WPolr.

58. Art. 6 lid 3 WPolr.

59. *Kamerstukken II*, 1985/86, 19 589, nr. 3, p. 8-9.

60. Art. 6 lid 4 WPolr.

61. Schuurman & Jordens 2000, p. 84.

men wanneer de reglementen van de betreffende gegevensverzamelingen uitdrukkelijk in die mogelijkheid voorzien. Gegevensverzamelingen zonder reglement of waarvan het reglement niet voorziet in de mogelijkheid tot koppeling, mogen in beginsel niet worden gebruikt ten behoeve van dataminingonderzoek. Opgemerkt zij dat deze beperking alleen betrekking heeft op gegevens(verzamelingen) die deel uitmaken van een verzameling van persoonsgegevens. Met betrekking tot op zichzelf staande gegevens die niet afkomstig zijn uit een register zijn andere factoren van belang voor de vraag, of die gegevens in aanmerking komen voor opname in een datawarehouse.

### Proces-verbaal

Van iedere koppeling wordt een proces-verbaal opgemaakt.<sup>62</sup> Op deze wijze kan controle worden uitgeoefend op een uitgevoerde koppeling, bijvoorbeeld door het CBP. In het proces-verbaal dienen de volgende zaken zo nauwkeurig mogelijk vermeld te worden<sup>63</sup>:

- a. het doel van de koppeling;
- b. de datum van de koppeling;
- c. degene in wiens opdracht de koppeling plaatsvond;
- d. de registraties die zijn gekoppeld, evenals de naam van de beheerder of de houder van die registraties;
- 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;
- g. eventuele bijzonderheden.

Voor zover dat met het oog op een goede uitvoering van de politietaak onvermijdelijk is, kan bij reglement van bovenstaande praktijk worden afgeweken.<sup>64</sup> Deze uitzondering pleegt te voorzien in de situatie waarin koppeling een zo alledaagse praktijk is, dat de vastlegging van alle hierboven staande gegevens een onevenredige administratieve werklust tot gevolg zou hebben. Dit zou het geval kunnen zijn wanneer opsporingsautoriteiten veelvuldig gebruik maken van een bepaalde dataminingvariant en de verplichting om daarvan telkenmale een proces-verbaal op te maken een efficiënte (lees: goede) uitvoering van de politietaak in de weg staat. Dit laat onverlet dat in dat geval wel op een andere manier moet worden voorzien in een mogelijkheid om, indien nodig, achteraf rekenschap af te kunnen leggen van hetgeen tijdens het dataminingonderzoek heeft plaatsgevonden. Wanneer het reglement niet in een afwijkende regeling voorziet is het

---

62. Art. 5 BPolr.

63. *Kamerstukken I*, 1998/99, 25 398, nr. 63b, p. 8.

64. Art. 5 lid 3 BPolr.

opmaken van een proces-verbaal, met daarin alle voorgeschreven elementen, verplicht.<sup>65</sup> Ook wanneer een koppeling plaatsvindt in het kader van een dataminingonderzoek, is het wenselijk dat een proces-verbaal wordt opgemaakt teneinde een eventuele toetsing achteraf mogelijk te maken. In dat geval zal het proces-verbaal bij voorkeur betrekking hebben op het dataminingonderzoek als geheel, en niet alleen op de aanleg van het datawarehouse. Daartoe bestaat op dit moment evenwel geen duidelijk omschreven wettelijke verplichting.

### **Koppeling van bijzondere politieregisters**

In beginsel is de koppeling van bijzondere politieregisters niet uitgesloten, zodat de gegevens in die registers ook kunnen worden gebruikt in het kader van een dataminingonderzoek. De art. 5a en 13d lid 3 WPolr beperken de opslag van nieuwe informatie die als gevolg van een (zodanige) koppeling is verkregen. Wanneer een koppeling tot doel heeft het opsporen van de misdrijven, waarvoor het register zware criminaliteit kan worden aangelegd, dan kan nieuw verkregen informatie ingevolge art. 13d lid 3 WPolr slechts worden vastgelegd en gebruikt overeenkomstig de regels van par. 3a WPolr. Ook wanneer de nieuw verkregen gegevens moeten worden aangemerkt als gegevens over onverdachte personen, dient rekening te worden gehouden met het bepaalde in par. 3a WPolr. Wanneer dit niet het geval is mogen de gegevens slechts voor een duur van vier maanden worden bewaard.<sup>66</sup> De koppeling van een tijdelijk met een ander register is slechts toegestaan voor zover dit noodzakelijk is voor het doel waarvoor het tijdelijk register is aangelegd.<sup>67</sup> Dit betekent dat het gebruik van gegevens uit een tijdelijk register voor dataminingonderzoek noodzakelijk moet zijn voor het realiseren van het doel waarvoor het tijdelijk register is aangelegd. De aanvullende voorwaarden die aan een koppeling van bijzondere politieregisters worden gesteld zorgen ervoor, dat de strengere regels die gelden voor de bijzondere politieregisters niet omzeild kunnen worden door deze registers te koppelen met andere registers<sup>68</sup>.

### **Beperkte koppeling op grond van BPolr**

Het BPolr stelt nadere regels voor het onderling koppelen van gegevensbestanden. Zo mag een politieregister alleen worden gekoppeld met andere politieregisters of met een verzameling van persoonsgegevens voor zover het gaat om persoonsregistraties van Rijk, provincies, gemeenten en andere openbare lichamen en de daaronder ressorterende diensten, instellingen en bedrijven. Dit betekent dat een koppeling niet mogelijk is met regi-

---

65. Schuurman & Jordens 2000, p. 85. Voor een tijdelijk politieregister als bedoeld in art. 13 WPolr betekent dit bijvoorbeeld dat, zolang er geen reglement is dat in de uitzonderingsmogelijkheid van art. 5 lid 3 WPolr voorziet, van een eventuele koppeling steeds een proces-verbaal dient te worden opgemaakt.

66. Art. 5a WPolr.

67. Zie art. 13 lid 2 WPolr en art. 4 lid 2 BPolr.

68. *Kamerstukken I*, 1998/99, 25 398, nr. 63b, p. 8.

straties van het bedrijfsleven<sup>69</sup> en evenmin met die van de semi-publieke sector op het gebied van onderwijs, gezondheidszorg en maatschappelijke dienstverlening. De koppeling van politieregisters met registers uit de niet-publieke sector voor opsporingsdoeleinden is naar huidig recht dus niet toegestaan; de PEC concludeert in haar eindrapport dat dit ook zo dient te blijven. Het ‘ruilen’ van gesloten informatie uit politieregisters met derden (bijvoorbeeld particuliere recherchebureaus) is uit den boze en dient expliciet te worden verboden.<sup>70</sup> Een uit een dergelijke handeling voortvloeiende inbreuk op de persoonlijke levenssfeer zou nog groter zijn dan dat al het geval is met betrekking tot de registraties binnen de overheid. Slechts in bijzondere gevallen kan de MvJ hierop een uitzondering maken<sup>71</sup>. Voor de koppeling van een (bijzonder) tijdelijk politieregister bevat het BPolr een aparte regeling; een koppeling van dit register met een ander register is toegestaan voor zover dat noodzakelijk is voor het doel waarvoor het tijdelijke politieregister is aangelegd.<sup>72</sup>

*Kritiek op art. 4 BPolr* – Bij de totstandkoming van de WPolr en het BPolr is het bepaalde in de Wpr als uitgangspunt genomen. Op dit moment (2005) is het BPolr op een aantal belangrijke punten evenwel nog niet in lijn gebracht met de Wbp en verwijst art. 4 BPolr nog steeds naar de inmiddels door de Wbp vervangen Wpr. Daarmee handelt het BPolr als uitgangspunt het technologieafhankelijke begrip ‘persoonsregistratie’, in plaats van het neutralere begrip ‘gegevensverwerking’ dat in de Wbp als aangrijppunt wordt genomen. In beginsel dient het bepaalde in art. 4 BPolr te worden uitgelegd conform de Wbp. Dit betekent dat de inhoud van een datawarehouse is beperkt tot gegevensverzamelingen zijnde politieregisters en door Rijk, provincies, gemeenten en andere openbare lichamen en de daaronder ressorterende diensten, instellingen en bedrijven verwerkte persoonsgegevens. Art. 4 BPolr zal beter aansluiten op de huidige uitgangspunten van de Wbp wanneer het begrip ‘persoonsregistratie’ wordt vervangen door ‘verwerkingen van persoonsgegevens’.

Ook op de inhoud van art. 4 BPolr valt enige kritiek te leveren. Deze kritiek richt zich niet op de vraag óf beperkingen moeten worden gesteld aan de mogelijkheden om gegevensverzamelingen met elkaar te koppelen, maar wel of dat de beperkingen moeten zijn die art. 4 BPolr stelt. Mede omdat het koppelingsbegrip niet alleen ziet op de koppeling van gehele gegevensbestanden maar ook op die van delen daarvan<sup>73</sup> lijkt een nuancering van art. 4 BPolr op zijn plaats.

---

69. Art. 4 lid 1 BPolr.

70. *Parlementaire Enquêtecommissie Opsporingsmethoden*, sectie 10.11 ‘Overige methoden Inwinning, opslag en gebruik van informatie’.

71. Art. 6 lid 4 WPolr, Schuurman & Jordens 2000, p. 84.

72. Zie art. 4 lid 2 BPolr.

73. Verbeek e.a. 1999, p. 170-171.

Voorts is de koppeling van politieregisters met registers uit de niet-publieke sector voor opsporingsdoeleinden naar huidig recht niet toegestaan. Daarmee wordt onder meer voorkomen, dat derden de beschikking kunnen krijgen over gesloten informatie uit politieregisters. Deze beperking maakt een dergelijke koppeling echter ook voor opsporingsinstanties onmogelijk. Daarmee worden de mogelijkheden die het dataminingsproces biedt zodanig begrensd, dat men zich kan afvragen of en in hoeverre deze situatie in het licht van de hedendaagse technologische en juridische<sup>74</sup> ontwikkelingen nog gewenst is. In bepaalde gevallen zal in het kader van een dataminingsonderzoek bij opsporingsinstanties behoefte bestaan aan gegevens in registers uit de niet-publieke sector. Gezien het doelbindingsbeginsel dient daarbij te worden gedacht aan een beperkte hoeveelheid informatie en blijft het gebruik van een volledig register uit de niet-publieke sector onwenselijk.

### Resumerend

Een koppeling is niet zonder meer mogelijk. Dit heeft indirect ook betekenis voor de samenstelling van het datawarehouse en het dataminingsonderzoek in het kader waarvan dat datawarehouse is aangelegd. Afhankelijk van de aard van de te koppelen registers dient een koppeling te worden getoetst aan de beschreven voorwaarden. Daarbij staan de volgende vragen centraal:

- mag de bevrager zijn bestand met het bestand van de verstrekker koppelen?
- mogen de gegevens worden ontvangen?
- mag de verstrekker zijn bestand met het andere bestand koppelen?
- mogen de gegevens worden verstrekt?

#### 4.2.2.5 *Het verstrekkingenregime*

Het verstrekkingenregime, uitgewerkt in de WPoI en het BPoI, is eveneens van invloed op de aanleg en inhoud van een datawarehouse. Bij of krachtens de WPoI wordt aangegeven aan wie en in welke gevallen bepaalde gegevens uit politieregisters mogen worden verstrekt. Behalve een gebied waarop vrije informatie-uitwisseling is toegestaan bestaat er ook een gebied dat van vrije informatie-uitwisseling is uitgesloten.<sup>75</sup> De WPoI hanteert een zogenaamd ‘besloten verstrekkingenregime’ dat is neergelegd in de art. 14 tot en met 18 ‘WPoI en verder wordt uitgewerkt in de art. 9 tot en met 15 BPoI. Dit regime is van toepassing op vrijwel ieder gebruik van de gegevens in de politieregisters en beperkt de wijze waarop met deze gegevens mag worden omgegaan. Het heeft onder meer betrekking op de vraag aan wie gegevens mogen worden verstrekt, de aard van de gegevens die

---

74. Zie ook Commissie Mevis 2001 en *Kamerstukken II*, 28059, 28353 en 29441.

75. Artz & Van Eijk 2000 (Sociale compartimentering).

worden verstrekt en de wijze waarop dit gebeurt<sup>76</sup>. Het besloten verstrekkingenregime reguleert voornamelijk de externe contacten.

Het verstrekken van gegevens uit een politieregister (in de zin van de WPolr) dient ruim te worden geïnterpreteerd. Het ziet op het bekendmaken of ter beschikking stellen van persoonsgegevens voor zover zulks geheel of grotendeels steunt op gegevens die in een politieregister zijn opgenomen of voor zover die persoonsgegevens door verwerking daarvan, al dan niet in verband met andere gegevens, zijn verkregen.<sup>77</sup> De wijze van verstrekken is daarbij niet van belang. Verstrekte gegevens kunnen als zodanig in de persoonsregistratie zijn opgenomen, maar het kan ook gaan om gegevens die het resultaat zijn van een verwerking waardoor nieuwe informatie wordt verkregen. Deze verwerking kan mede bestaan uit het leggen van een verband met andere gegevens. Een verstrekking betreft niet alleen het nauwkeurig weergeven van de uit de registratie verkregen informatie, maar ook het in enigszins andere vorm doorgeven van in wezen dezelfde gegevens.<sup>78</sup>

Binnen het politieapparaat is in beginsel steeds sprake van een vrij verstrekkingenregime. Uit de formulering van een groot aantal wettelijke bepalingen vloeit zelfs een verplichting tot verstrekking voort.<sup>79</sup> Opsporingsambtenaren moeten voor de opsporing van strafbare feiten aanspraak kunnen maken op gegevens uit de politieregisters, ongeacht of deze registers worden beheerd door het politiekorps waartoe zij behoren of niet. Het verplichtend regime van de WPolr wordt verklaard uit de opvatting, dat compartimentering binnen de Nederlandse politie op het terrein van de gegevensverstrekking kan leiden tot een ongewenste situatie van onderlinge concurrentie in de misdaadbestrijding met behulp van de hun ter beschikking staande gegevens. Een Nederlandse politieambtenaar dient, mits het doel dit rechtvaardigt, te kunnen beschikken over alle gegevens die binnen de Nederlandse politie aanwezig zijn. Aan opsporingsambtenaren van de politie en de Koninklijke Marechaussee dienen uit politieregisters de gegevens te worden verstrekt die zij behoeven voor de vervulling van hun taak.<sup>80</sup> Aan opsporingsambtenaren in dienst van een publiekrechtelijk lichaam (voornamelijk de bijzondere opsporingsdiensten) dienen die gegevens te worden verstrekt die zij nodig hebben voor de opsporing van strafbare feiten in een bepaald onderzoek waarbij zij zijn betrokken.<sup>81</sup> Voor de overige opsporingsambtenaren wordt, naast de voorwaarde dat het moet gaan om gegevens die zij

---

76. Op grond van art. 20 WPolr is het verstrekkingenregime van de WPolr niet van toepassing op mededelingen van de beheerder van een register aan de geregistreerde zelf.

77. Art. 1 sub *b* WPolr.

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

79. Zie bijvoorbeeld de art. 14 en 15 WPolr: 'uit een politieregisters worden (...) gegevens verstrekt aan'.

80. Art. 14 onder *a* en *b* WPolr.

81. Art. 14 onder *c* WPolr.

behoeven voor een bepaald onderzoek, de aanvullende eis gesteld dat hun voorafgaand toestemming is verleend door de OvJ (in afzonderlijke gevallen) of door de MvJ (in het algemeen).<sup>82</sup>

Aan een ambtenaar, handelend in de uitvoering van zijn wettelijk opgedragen politietak, dienen – geregelde uitzonderingen daargelaten – de gevraagde gegevens uit een politieregister in beginsel te worden verstrekt. Deze verplichting tot het verstrekken van informatie kan alleen worden beperkt bij AMvB op grond van art. 17 WPolr<sup>83</sup>. Over het algemeen is een beheerder van een register bij een verzoek om informatie niet bevoegd om ten gronde te beoordelen of de gevraagde gegevens inderdaad nodig of noodzakelijk zijn in verband met de uitoefening van de taak of de werkzaamheden waarvoor deze gevraagd worden.<sup>84</sup> Enkel wanneer het evident is dat de gevraagde gegevens niet benodigd, noodzakelijk of onvermijdelijk zijn in verband met de uitoefening van de taak waarvoor ze zijn gevraagd, kan de beheerder verstrekking weigeren.<sup>85</sup> Voor de bijzondere politieregisters, die in de volgende sectie ter sprake komen, geldt een beperkt verstrekkingenregime. De beperkingen van de WPolr worden uitgewerkt in het BPolr. De beheerder van een politieregister is bevoegd om de verstrekking van gegevens betreffende politie-informanten en gegevens die bij verstrekking direct gevaar kunnen opleveren voor de geregistreerde of voor derden, aan alle bovengenoemde opsporingsambtenaren te weigeren. Een verstrekking kan eveneens achterwege worden gelaten wanneer deze werden verkregen onder de voorwaarde, dat zij alleen voor een bepaald doel gebruikt zouden worden. Anders dan in de normale situatie is hier ruimte gecreëerd voor een belangenafweging door de verstrekker. Deze heeft daarnaast de mogelijkheid om beperkingen op te leggen aan het gebruik van de verstrekte gegevens.<sup>86</sup> De verstrekking van gevoelige gegevens aan opsporingsambtenaren vindt slechts plaats voor zover dit noodzakelijk is voor de goede uitvoering van de politietak. Art. 30 WPolr bevat een geheimhoudingsverplichting op verstrekte gegevens uit politieregisters die betrekking hebben op een derde. Voor een hulpverleningsregister en het register dat door het Meldpunt Ongebruikelijke Transacties wordt bijgehouden geldt, dat uit deze registers in beginsel alleen informatie wordt verstrekt dat betrekking heeft op het doel waarvoor deze zijn aangelegd.

### **De bijzondere politieregisters**

Naast de gewone politieregisters onderscheidt de WPolr in par. 3a de bijzondere politieregisters<sup>87</sup>. De politie dient bij het vervullen van de opsporingstaak te kunnen beschik-

---

82. Art. 14 WPolr.

83. *Kamerstukken II*, 1988 /89, 19 589, nr. 6, p. 11.

84. Zie de formulering van de art. 14 en 15 WPolr.

85. Op grond van de algemene zorgplicht van art. 7 WPolr.

86. Art. 11 lid 3 BPolr.

87. De Wet Bijzondere politieregisters is op 1 februari 2000 in werking getreden (*Stb.* 1999, 244).

ken over veel informatie, variërend van openbaar tot geheim en van vaststaand tot onbetrouwbaar. Hierbij gaat het soms, gezien het impliciete morele verwijt dat ligt besloten in strafrechtelijke gegevens, om zeer gevoelige informatie. Met het oog op de bescherming van de persoonlijke levenssfeer dient op vrij gedetailleerd niveau te worden vastgelegd, op welke wijze met de verschillende soorten informatie moet worden omgegaan. Door middel van een aparte regeling in de vorm van een bijzonder register is het mogelijk duidelijkheid te verschaffen over de mogelijkheden tot opslag en gebruik van (zachte)<sup>88</sup> gegevens die onvoldoende hard zijn om, zonder nadere restricties, te worden opgenomen in een gewoon politieregister. De WPolr onderscheidt drie bijzondere politieregisters, namelijk het tijdelijk register, het voorlopig register en het register zware criminaliteit<sup>89</sup>. Deze registers hebben met elkaar gemeen dat daarin voor een langere periode gevoelige en mogelijk onbetrouwbare opsporingsinformatie kan worden opgeslagen. De bepalingen met betrekking tot de bijzondere registers vormen een uitputtende regeling voor de opslag van dergelijke informatie. Zij onderscheiden zich vooral in de zin, dat de informatie die zij bevatten niet structureel mag worden opgeslagen in de overige politieregisters. Daarnaast ligt het onderscheid in het gebruik, het opslaan en het verstrekken van zachte opsporingsinformatie.<sup>90</sup>

*Het tijdelijke politieregister* – Een tijdelijk politieregister kan worden aangelegd met het oog op de uitvoering van de politietaak in een bepaald geval of in het kader van een verkennend onderzoek als bedoeld in art. 126gg Sv. In een tijdelijk register mogen slechts persoonsgegevens worden opgenomen die het doel dienen waarvoor dit register is aangelegd. Verstrekking uit een tijdelijk register is in beginsel toegestaan voor het doel waarvoor het is aangelegd, dan wel voor opname in een voorlopig politieregister of een register zware criminaliteit. Een verstrekking is verder mogelijk wanneer uit de gegevens zelf een redelijk vermoeden voortvloeit dat een bepaalde persoon een strafbaar feit heeft begaan.<sup>91</sup> Opmerkelijk is dat een tijdelijk register in beginsel is vrijgesteld van de reglementsplicht van art. 9 WPolr. Voor de inwerkingtreding van een tijdelijk register is het voldoende, dat het doel<sup>92</sup> en de datum waarop met de aanleg van het register wordt begonnen worden vastgelegd. Binnen een week moet het bestaan van het register ter kennis worden gebracht van het gezag en het CBP. De overige voorwaarden die normaal gesproken van toepassing zijn gelden niet voor de ingestelde termijn van zes maanden, te

88. De term ‘gevoelige gegevens’ is door de wetgever voorbehouden aan gegevens die één van de in art. 5 WPolr genoemde kenmerken bezitten.

89. Voor de komst van de Wet Bijzondere politieregisters stonden het register zware criminaliteit en het voorlopig register bekend als het CID-register respectievelijk het grijze-veld register.

90. *Kamerstukken II*, 1996/197, 25 398, nr. 3, p. 4.

91. Dit geldt zowel voor gegevens uit een tijdelijk register als voor gegevens uit een voorlopig register, zie hiervoor art. 13d lid 2b WPolr.

92. Met inbegrip van een nauwkeurige omschrijving van het bepaalde geval.

rekenen vanaf de dag dat met de aanleg van het register is begonnen<sup>93</sup>; die termijn kan namelijk door het bevoegde gezag telkens voor ten hoogste zes maanden worden verlengd, wanneer het doel waarvoor het register is aangelegd door bekendmaking en terinzagelegging van het reglement ernstig in gevaar wordt gebracht. Elke beslissing tot verlenging van de termijn dient te worden gemeld aan het CBP<sup>94</sup>. Bij overdracht of samenvoeging dient het reglement dienovereenkomstig te worden aangepast. In het geval van een overdracht kan het doel van het register niet worden gewijzigd. Bij samenvoeging is dit onder bepaalde voorwaarden wel mogelijk. Indien de termijn van een tijdelijk politieregister verstrijkt of het doel van het register is bereikt, dienen de daarin opgenomen gegevens te worden vernietigd. Dit is slechts anders indien de gegevens betekenis hebben voor een strafrechtelijk vervolgonderzoek of worden opgenomen in een register zware criminaliteit of een voorlopig register.<sup>95</sup> Deze gegevens kunnen binnen een redelijke termijn naar één van deze registers worden overgeheveld. In beginsel geldt dat gegevens ingevolge de WPolr niet langer mogen worden opgeslagen dan nodig is voor het doel waarvoor zij zijn vergaard.

*Het voorlopige politieregister* – Een voorlopig register is aangelegd met het oog op de uitvoering van de politietaak voor zover het betreft een onderzoek ter vaststelling of een geregistreerde persoon, in samenhang met andere gegevens, kan worden opgenomen in het register zware criminaliteit. Registratie van persoonsgegevens in een voorlopig register mag alleen ten behoeve van dit doel plaatsvinden. Gegevens uit een voorlopig register kunnen, evenals bij een tijdelijk politieregister, worden verstrekt indien uit de gegevens zelf een redelijk vermoeden voortvloeit dat een bepaalde persoon een strafbaar feit heeft begaan. Voor identificatie benodigde gegevens mogen enkel worden verstrekt voor het doel waarvoor het voorlopig register is aangelegd. Voorts is een verstrekking mogelijk ten behoeve van de opname in een ander bijzonder politieregister of van het Meldpunt, bedoeld in art. 2 Wet melding ongebruikelijke transacties (MOT). Persoonsgegevens dienen uit het voorlopig register verwijderd en vernietigd te worden indien zij niet langer noodzakelijk zijn voor het doel van het register, dan wel na verloop van zes maanden na de datum van eerste opname. Evenals het register zware criminaliteit valt het voorlopig register onder de verantwoordelijkheid van de criminele inlichtingeneenheden (CIE). Dat is vastgelegd in de Regeling criminele inlichtingen eenheden<sup>96</sup>, die per 1 november 2000 de CID-regeling 1995 heeft vervangen.

---

93. Art. 8 lid 3 BPolr.

94. Art. 8 BPolr.

95. *Parlementaire Enquêtecommissie Opsporingsmethoden*, bijlage V, sectie 8.2.2

‘Feitelijke toepassing politieregisters’.

96. *Stb.* 2000, 198, p. 14-16.

*Het register zware criminaliteit* – Het derde bijzondere politieregister is het register zware criminaliteit, dat is aangelegd met het oog op de uitvoering van de politietaak voor zover het betreft:

- misdrijven als omschreven in art. 67 lid 1 Sv die in georganiseerd verband worden beraamd of gepleegd en, gezien hun aard of de samenhang met andere misdrijven die in georganiseerd verband worden beraamd of gepleegd, een ernstige inbreuk op de rechtsorde opleveren;
- misdrijven waarop naar de wettelijke omschrijving een gevangenisstraf van acht jaar of meer is gesteld;
- bij algemene maatregel van bestuur (AMvB) te omschrijven misdrijven als omschreven in art. 67 lid 1 Sv die, gezien hun aard of de samenhang met andere door een betrokkene begane misdrijven, een ernstige inbreuk op de rechtsorde opleveren.

Het opnemen van persoonsgegevens in een register zware criminaliteit is toegestaan wanneer het gaat om verdachten van de hierboven genoemde misdrijven, dan wel personen ten aanzien van wie een redelijk vermoeden bestaat dat zij betrokken zijn bij het beraamen of plegen daarvan. Ook kunnen persoonsgegevens worden opgenomen van degenen die in een bepaalde relatie staan tot de genoemde personen. Hoewel het een bijzonder politieregister betreft, stelt de WPolr in beginsel<sup>97</sup> geen nadere beperkingen aan een verstrekking van gegevens uit een register zware criminaliteit. Persoonsgegevens dienen uit het register te worden verwijderd en vernietigd wanneer deze 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 de betrokkene met het oog op het doel van het register.<sup>98</sup>

#### 4.2.2.6 *Het doelbindingsbeginsel*

Het doelbindingsbeginsel is één van de nieuwe aspecten van de Wbp waarmee bij de toepassing en uitleg van de WPolr en het BPolr rekening dient te worden gehouden. In art. 9 Wbp wordt bepaald dat persoonsgegevens niet verder mogen worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor zij zijn verkregen. Voor de toepassing van dataminingsonderzoek ten behoeve van de opsporing betekent dit dat dient te worden voorkomen, dat gegevensverzamelingen die voor een ander doel zijn verkregen toch ten behoeve van de opsporing worden gebruikt. Het is bijvoorbeeld niet toegestaan om uitsluitend voor medische doeleinden opgeslagen DNA-gegevens voor opsporingsdoeleinden te gebruiken. Ook bij het opnemen van vingerafdrukken in het

---

97. Voor de laatstgenoemde categorie van gegevens geldt een beperkt verstrekkingenregime op grond van art. 13b WPolr.

98. Zie ook Corstens 2002, p. 279.

paspoort kan de doelbinding een regulerende functie vervullen. Een dergelijk besluit leidt namelijk tot een nationale, zo niet internationale, database van vingerafdrukken die, behalve voor het waarborgen van de authenticiteit van het paspoort, tevens ten behoeve van de opsporing kan worden ingezet.

Op het moment van schrijven (2005) is geen specifiek doelbindingsbeginsel voorhanden met betrekking tot het verwerken van gegevens door opsporingsautoriteiten. Het verstrekkingenregime van de WPolr kent geen voorwaarde aangaande een koppeling tussen verstrekkingen en doel van het register, ofwel de doelbinding zoals de nieuwe Wbp die voorstaat. Er bestaat een verplichting om te verstrekken indien de verstrekking past binnen de goede taakuitoefening van de vragende partij. Voor enkele registers bestaat een uitzondering op deze regel. Zowel uit een tijdelijk politieregister als uit een voorlopig bijzonder politieregister kan in beginsel slechts worden verstrekt voor het doel waarvoor deze registers zijn aangelegd. Hoewel een register zware criminaliteit geen expliciet doelbindingsbeginsel kent, zal later in dit onderzoek<sup>99</sup> blijken dat dit beginsel ook van invloed is op een verstrekking uit dit register. Het doelbindingsbeginsel is voorts wel van toepassing op de hulpverleningsregisters en het register-MOT<sup>100</sup>.

In sectie 4.2.2.4 kwam onder het kopje *Beperkte koppeling op grond van BPolr* in het kader van de koppelingsregeling de reikwijdte van art. 4 BPolr reeds ter sprake. Met dit artikel worden geen nadere beperkingen gesteld aan het gebruik (koppeling) van gegevensverzamelingen zijnde politieregisters en verzamelingen van persoonsgegevens voor zover dit betreft verwerkingen van persoonsgegevens door Rijk, provincies, gemeenten en andere openbare lichamen en de daaronder ressorterende diensten, instellingen en bedrijven. Onder de huidige privacywetgeving lijkt een koppeling met publieke gegevensverzamelingen echter niet minder bezwaarlijk dan een koppeling met niet-publieke gegevensverzamelingen. Met het oog op het doelbindingsbeginsel is het gebruik van gegevens uit de genoemde registers ten behoeve van de opsporing niet vanzelfsprekend; ook publieke gegevensverzamelingen zouden in wezen slechts dan mogen worden gekoppeld wanneer het doel waarvoor de betreffende gegevensverzameling in eerste instantie is aangelegd overeenkomt, dan wel in het verlengde ligt van het doel van het dataminingonderzoek waarvoor het wordt gebruikt. De mogelijkheid van het onbeperkt gebruik van gegevens uit publieke registers staat op gespannen voet met de huidige privacywetgeving. Deze zienswijze lijkt ondersteuning te vinden in de, in het kader van de wijziging van bepalingen met betrekking tot de verwerking van persoonsgegevens, gerealiseerde aanpassing van art. 126gg Sv<sup>101</sup>, betreffende het verkennend onderzoek. In het kader van een verkennend onderzoek is het mogelijk dat dataminingonderzoek wordt verricht. Met het

---

99. Zie sectie 7.3.4.3 onder het kopje *De doelbinding*.

100. Art. 12 lid 1 BPolr.

101. *Kamerstukken I*, 2000 /01, 26 410, nr. 150, p. 2.

oog op de komst van de Wbp is een tweede lid aan art. 126<sup>gg</sup> Sv toegevoegd. Daarin is bepaald dat de OvJ kan bepalen dat art. 9 lid 1 Wbp met betrekking tot het onderzoek niet van toepassing is op daarbij nader aan te geven openbare registers die bij wet zijn ingesteld, indien dat noodzakelijk is voor de uitvoering van het onderzoek. In het kader van dataminingsonderzoek kan mogelijk gebruik worden gemaakt van openbare registers die bij wet zijn ingesteld, dan wel van gedeelten daaruit. De omstandigheid dat een verkennend onderzoek slechts onder bepaalde voorwaarden is toegestaan, in combinatie met het feit dat het besluit om daarbij gebruik te maken van bepaalde openbare registers alleen kan worden genomen door de OvJ, geeft aan dat de bevoegdheid die het huidige art. 4 BPolr voorstaat niet onbegrensd is.

### 4.3 Afsluitend

Zowel op nationaal als op internationaal niveau worden beperkingen gesteld aan de verwerking van persoonsgegevens. In dit hoofdstuk is vastgesteld met welke wet- en regelgeving in ieder geval rekening dient te worden gehouden bij de verwerking van persoonsgegevens door opsporingsautoriteiten. Vervolgens is onderzocht in hoeverre de bepalingen uit de Politiewet 1993, de WPolr en het BPolr richtinggevend en misschien zelfs richtingbepalend zijn voor de toepassing van het dataminingsproces ten behoeve van de opsporingstaak. Met het oog op de toenemende automatisering en de daarmee gepaard gaande centrale gegevensopslag is het voor de bescherming van de privacy van belang, de gebundelde macht die daarin ligt besloten te kunnen normeren. In dit onderzoek wordt het bestaande juridische raamwerk, gevormd door nationale en internationale invloeden, als leidraad gebruikt bij de normering van het dataminingsproces. Bij de toepassing van het dataminingsproces in het kader van de opsporingstaak is het namelijk onvermijdelijk, dat daarbij in enig stadium ook persoonsgegevens worden verwerkt.

Dit onderzoek beperkt zich tot het gebruik van het dataminingsproces door de politie (en justitie) ten behoeve van de opsporingstaak. Het juridisch kader dat hierop van toepassing is blijkt grotendeels (en uitputtend) te worden gevormd door de WPolr en het bijbehorende BPolr, waarmee onze wetgever heeft voorzien in een specifieke regeling voor de verwerking van gegevens in het kader van de opsporingstaak. Op grond van de WPolr vindt de opslag van persoonsgegevens (het verwerken van persoonsgegevens onder de Wbp) ten dienste van de politietaak plaats in een politieregister. Dit is alleen toegestaan voor een bepaald doel en dient tevens noodzakelijk te zijn voor een goede uitvoering van de politietaak. De vastgelegde gegevens moeten rechtmatig zijn verkregen en noodzakelijk zijn voor het doel waarvoor het register is aangelegd. Met betrekking tot de verstrekking van gegevens uit een politieregister is sprake van een besloten regime. In de WPolr wordt een onderscheid gemaakt tussen gewone en bijzondere politieregisters. Kenmerkend voor bijzondere politieregisters is het afwijkende verstrekkingenregime en het doorgaans 'zachte' karakter van de gegevens die in die registers liggen opgeslagen. De specifieke registratie van bepaalde (gevoelige) persoonsgegevens, zoals opgesomd in art. 5

WPolr, is in beginsel uitgesloten. In art. 5a WPolr worden beperkingen gesteld aan de mogelijkheid om gegevens omtrent onverdachte personen vast te leggen. Met uitzondering van het tijdelijk politieregister dient ieder politieregister een reglement te hebben. Daarin moet onder meer (de mogelijkheid tot) het koppelen van een register met een ander register worden geregeld. Wanneer een dergelijke regeling ontbreekt is een koppeling uitgesloten. De WPolr en het BPolr stellen, al naar gelang de aard van de betrokken politieregisters, nadere voorwaarden aan een koppeling. Binnen het systeem van de WPolr vervult het CBP als ‘waakhond over de privacybelangen van de burger’ een belangrijke functie.



---

## 5 Het datawarehouse

Het verzamelen van gegevens neemt een belangrijke plaats in binnen het proces van datamining. De fase waarin dit gebeurt wordt meestal aangeduid met de term ‘datawarehousing’<sup>1</sup>. Bij de toepassing van dataminingstechnieken ten behoeve van de opsporing is het onvermijdelijk dat op enig moment gegevens (dienen te) worden opgeslagen. Een dergelijke registratie kan niet alleen nodig zijn ter voorbereiding van het eigenlijke datamining (bewerken), maar kan ook betrekking hebben op het (vastleggen van het) resultaat van het dataminingonderzoek. De verzamelde gegevens worden opgeslagen in een geautomatiseerd centraal gegevensbestand, het datawarehouse, waarna zij verder kunnen worden bewerkt. Omdat de input in grote mate bepalend is voor het resultaat van het dataminingsproces, is de fase van de datawarehousing van invloed op het verloop van het dataminingsproces. De aanleg van een datawarehouse vindt, als onmisbaar onderdeel<sup>2</sup> van het dataminingsproces, plaats met het uiteindelijke doel een bijdrage te leveren aan de opsporingstaak. Om de politietaak, in dit geval de strafrechtelijke handhaving van de rechtsorde, op een zo efficiënt mogelijke manier te kunnen uitvoeren, is het verkrijgen en handhaven van een goede informatiepositie onontbeerlijk. Zonder een goede informatiepositie is het voor de opsporingsautoriteiten vrijwel onmogelijk hun taak naar behoren uit te voeren, ongeacht of het daarbij gaat om een individueel geval of om de opsporingstaak in het algemeen. In dit licht kan de toepassing van dataminingstechnieken, en daarmee de aanleg van een datawarehouse, als noodzakelijke voorwaarde worden verondersteld voor een goede uitvoering van de opsporingstaak.

Bij toepassing van het dataminingsproces ten behoeve van de opsporingstaak kan de vraag worden gesteld of het nodig is dat daarbij een, eventueel als politieregister te kwalificeren, datawarehouse wordt aangelegd. Bij de opslag van gegevens in het kader van de politietaak dienen de nodige waarborgen te bestaan en in acht te worden genomen. Wanneer voor de opslag van gegevens geen wettelijke kaders aanwezig zijn komt dat noch de uitvoering van de politietaak, noch de bescherming van de persoonlijke levenssfeer ten goede.<sup>3</sup> Het opslaan van gegevens ten behoeve van de opsporing, waartoe ook de aanleg

- 
1. Technisch gesproken is een datawarehouse niet altijd noodzakelijk voor de toepassing van datamining, maar in de meeste gevallen wel wenselijk.
  2. Namelijk het voorbereidende stadium van het dataminingsproces.
  3. *Kamerstukken II*, 1997/98, 25 398, nr. 6, p. 8.

en het gebruik van een datawarehouse kunnen worden gerekend, is geregeld in de WPolr en het BPolr. In dit hoofdstuk wordt onderzocht op welke wijze aan het datawarehouse, aangelegd in het kader van een dataminingonderzoek ten behoeve van de opsporingstaak, vanuit juridisch oogpunt door de WPolr en het BPolr wordt vormgegeven.

### **5.1 Kenmerken van het politieregister**

Eerst wordt voor een datawarehouse, aangelegd in het kader van een dataminingonderzoek ten behoeve van de opsporingstaak, nagegaan of het kan worden aangemerkt als een politieregister in de zin van de WPolr.<sup>4</sup> Dit is het geval wanneer het datawarehouse de volgende eigenschappen bevat:

1. een samenhangende verzameling, van
2. op verschillende personen betrekking hebbende persoonsgegevens die
3. langs geautomatiseerde weg wordt gevoerd of met het oog op een doeltreffende raadpleging van die gegevens systematisch is aangelegd,
4. ten dienste van de uitvoering van de politietaak.

Een datawarehouse kan bestaan uit twee categorieën van gegevens. De eerste categorie heeft betrekking op de gegevens waarop de bewerking wordt uitgevoerd. Deze vormen in beginsel steeds een samenhangende verzameling van op (verschillende) personen betrekking hebbende gegevens. Tevens wordt deze gegevensverzameling gevoerd ten dienste van de uitvoering van de politietaak en systematisch aangelegd met het oog op een doeltreffende raadpleging van die gegevens langs geautomatiseerde weg. Een kwalificatie als politieregister lijkt dus gerechtvaardigd. Dit impliceert dat voor de juridische inkadering van het dataminingsproces bij de opslag van gegevens gedurende het dataminingonderzoek rekening dient te worden gehouden met de wettelijke bepalingen die gelden voor de politieregisters. De tweede categorie van gegevens die in een datawarehouse kunnen worden aangetroffen betreft het resultaat van het dataminingonderzoek. Een bewerking van de gegevens in het datawarehouse, resulteert in nieuwe informatie. Afhankelijk van de aard daarvan wordt die informatie (tijdelijk) in het datawarehouse opgenomen, elders vastgelegd of vernietigd. Het resultaat op zich kan niet per definitie als een politieregister worden aangemerkt<sup>5</sup>.

#### **Resultaat ongericht dataminingonderzoek**

Het resultaat van een ongericht dataminingonderzoek is ruimer en algemener dan dat van de gerichte dataminingvariant. Omdat nog niet gericht wordt gezocht kan het onderzoek resulteren in verschillende, los van elkaar staande verdenkingen, die aanlei-

---

4. Art. 1 lid 1 sub c WPolr (*Kamerstukken I*, 2000 /01, 26 410, nr. 150, p. 3).

5. Aldus ook Schuurman & Jordens 2000, p. 84.

ding kunnen vormen voor verder (gericht) dataminingonderzoek. Het resultaat kan echter ook onvoldoende worden bevonden om op een bepaald moment een vervolgonderzoek te rechtvaardigen. Het kan in dat geval eventueel opnieuw in het onderzoek worden meegenomen of apart worden bewaard. Dit is mogelijk door het permanente karakter van een ongericht dataminingonderzoek, dat immers niet teneinde loopt op het moment waarop resultaat is gegenereerd. Resultaten die vandaag niets opleveren, kunnen morgen een waardevolle aanvulling vormen op de bestaande politieregisters. Ingeval het resultaat wel deels of geheel in aanmerking komt voor opslag in een ander register kan het, mits dat niet op juridische bezwaren stuit<sup>6</sup>, wenselijk zijn dat de betreffende gegevens beschikbaar blijven voor het ongerichte dataminingonderzoek. Het bovenstaande in aanmerking genomen kan worden geconcludeerd dat bij een ongericht dataminingonderzoek, zowel de gegevens waarop het onderzoek betrekking heeft als ook het resultaat van het onderzoek, in aanmerking komt voor de kwalificatie van politieregister.

### Resultaat gericht dataminingonderzoek

Het resultaat van een gericht dataminingonderzoek zal, gezien de aard daarvan, in principe niet meer in aanmerking komen voor kwalificatie als politieregister. Dit zou echter wel denkbaar zijn ingeval het onderzoek resulteert in het blootleggen van een crimineel netwerk; daarbij is immers sprake van op verschillende personen betrekking hebbende persoonsgegevens. Overigens ontbreekt met betrekking tot het resultaat van een gericht dataminingonderzoek doorgaans de noodzaak tot kwalificatie als politieregister. Een gericht dataminingonderzoek is naar duur en doelstelling beperkt van aard. Het onderzoek eindigt wanneer het doel daarvan is bereikt.<sup>7</sup> Bij de beëindiging van een gericht dataminingonderzoek kunnen de gegevens die onderdeel van dat onderzoek uitmaakten worden opgenomen in een ander politieregister indien zij daarvoor in aanmerking komen. Wanneer het resultaat bijvoorbeeld aanleiding vormt voor een vervolgonderzoek<sup>8</sup> is het van belang, dat het wordt opgenomen in een datawarehouse dat in het kader van dat vervolgonderzoek wordt aangelegd. Uit deze gang van zaken kan worden afgeleid dat na afloop van een gericht dataminingonderzoek in beginsel geen sprake meer is van een

---

6. Wanneer het resultaat in aanmerking komt voor registratie in het register zware criminaliteit, ligt het gezien de aard van de betreffende gegevens niet voor de hand dat deze ook beschikbaar blijven voor ongericht dataminingonderzoek.

7. Het is overigens mogelijk dat als gevolg van bijvoorbeeld een verkennend onderzoek een concrete verdenking ontstaat. Dan is er niets op tegen om naar aanleiding daarvan een opsporingsonderzoek te starten, terwijl het verkennend onderzoek naar andere personen nog doorloopt (Handboek voor de opsporingspraktijk 2000, sectie 1.2 Verkennend onderzoek). Niet het genereren van een resultaat maar het bereiken van het doel van het onderzoek, doet het gerichte dataminingonderzoek eindigen.

8. Dit is ook het geval bij het verkennend onderzoek van art. 126gg Sv. Indien naar aanleiding van dit onderzoek een concrete verdenking ontstaat, resulteert dit in een opsporingsonderzoek.

verzameling van resultaten. Het resultaat wordt in een nieuw datawarehouse of een ander politieregister opgenomen. Is dit niet het geval, dan geldt als hoofdregel dat alle gegevens, voortkomende uit een gericht dataminingonderzoek, inclusief het resultaat, worden vernietigd.

#### *5.1.1 Geen verplichte aanleg politieregister*

Afhankelijk van de aard van het dataminingonderzoek kan een datawarehouse worden aangemerkt als een register in de zin van de WPolr. Uit deze constatering vloeit evenwel geen verplichting tot de aanleg van een datawarehouse voort. Wanneer een datawarehouse als politieregister wordt gekwalificeerd betekent dit, dat het moet voldoen aan de regels die de WPolr en het BPolr daaraan stellen. Noch de WPolr, noch het BPolr kent echter de verplichting tot het aanleggen van een politieregister. Ingeval de opsporingsautoriteiten de aanleg van een politieregister om enige reden gewenst achten, is met betrekking tot de vraag of dit een gewoon of een bijzonder politieregister moet zijn bepaald<sup>9</sup>, dat de aanleg van een gewoon politieregister wordt beheerst door art. 4 WPolr; de beheerder kan een gewoon register aanleggen voor een bepaald doel en voor zover dat noodzakelijk is voor de goede uitvoering van de politietaak. Deze situatie voert naar de conclusie dat de beslissing van een opsporingsautoriteit om al dan niet een (bepaald) politieregister aan te leggen bepalend is voor de vraag of met betrekking tot een gegevensverzameling al dan niet dient te worden voldaan aan de bijbehorende voorwaarden in de WPolr en het BPolr. Dit kan niet de bedoeling zijn.

Hierna wordt ingegaan op de vraag of de vrije keuzemogelijkheid voor de aanleg van een politieregister door opsporingsdiensten impliceert, dat in de praktijk kan worden volstaan met een datawarehouse dat niet als een politieregister wordt gekwalificeerd. Daarbij wordt vooral gekeken naar de rol die een datawarehouse kan vervullen bij de bescherming van de persoonlijke levenssfeer. Mogelijk bestaan er vanuit juridisch oogpunt redenen waaruit de wenselijkheid, dan wel de noodzaak voortvloeit een datawarehouse te kwalificeren.

#### *5.1.2 Status datawarehouse*

Voor het beantwoorden van de vraag of vanuit juridisch oogpunt het onderscheiden en kwalificeren van een datawarehouse noodzakelijk is, dient met een aantal factoren rekening te worden gehouden. Hieronder behandel ik vijf factoren.

---

9. *Kamerstukken II*, 1997/98, 25 398, nr. 6, p. 10-11.

### 1. Bescherming persoonlijke levenssfeer

Wanneer een datawarehouse niet als politieregister wordt gekwalificeerd kan men zich afvragen, of er nog wel sprake is van een ‘verantwoorde opslag’<sup>10</sup>. Het is onwenselijk dat opsporingsautoriteiten gegevens opslaan op een wijze die noch de uitvoering van de politietoets, noch de bescherming van de persoonlijke levenssfeer ten goede komt. De behoefte aan een verantwoorde opslag doet zich in het bijzonder voelen wanneer het gaat om gegevens uit registers waarvoor een (zeer) beperkt verstrekkingenregime geldt. Een verantwoorde opslag hangt ook samen met de beheersbaarheid van het resultaat van een dataminingonderzoek. Dat resultaat kan bestaan uit bruikbare kennis, maar ook uit nutteloze informatie. Om het een van het ander te onderscheiden dient het resultaat te worden geanalyseerd, waarna het verder kan worden bewerkt. Dit kan betekenen dat het wordt opgenomen in een ander register, vernietigd of verstrekt aan derden. Bij een juridische inkadering van het dataminingsproces is de verwerking van het resultaat minstens even belangrijk als de andere stadia van het proces.

Met uitputtende regelgeving in de WPoLr en het BPolr heeft de wetgever willen voorzien in het op een juiste manier vastleggen en verstrekken van gegevens door de politie in het kader van de opsporingstaak. Daarbij zijn de benodigde waarborgen vastgelegd ter bescherming van de persoonlijke levenssfeer van de burger. Bij een verwerking<sup>11</sup> van gegevens in het kader van de opsporingstaak dienen deze waarborgen in acht te worden genomen. De voorwaarden voor een verwerking variëren naar gelang de aard van de gegevens. Hoe gevoeliger en zachter de gegevens, hoe strenger de voorwaarden. De WPoLr en het BPolr beogen de realisering van de waarborgen door onder meer het hantieren van verschillende verstrekkingenregimes, bijvoorbeeld door onderscheid te maken tussen gewone en bijzondere politieregisters. Door een datawarehouse in het kader van een dataminingonderzoek te kwalificeren als een politieregister in de zin van de WPoLr, kunnen die waarborgen onverkort worden gehandhaafd. Dit impliceert dat, alvorens het in werking mag treden, op grond van art. 9 WPoLr ook moet worden voorzien in een reglement bij dat datawarehouse. Daarin kunnen zaken worden geregeld met betrekking tot het datawarehouse, de uitvoering van het dataminingonderzoek en de wijze waarop het resultaat wordt verwerkt. Hoewel de aanleg van een datawarehouse bij dataminingonderzoek niet verplicht is, dient een gegevensverwerking door opsporingsinstanties op juridisch verantwoorde wijze plaats te vinden. Dit is vooral van belang wanneer het gaat om de verwerking van gevoelige, dan wel zachte gegevens. De waarborgen die de WPoLr en het BPolr bieden moeten niet kunnen worden omzeild door een datawarehouse niet

---

10. *Kamerstukken II, 1997/198, 25 398, nr. 6, p. 8.*

11. Hierbij kan het gaan om de opslag van gegevens in een politieregister maar ook om het gebruik van de gegevens in het kader van een dataminingonderzoek.

als politieregister te kwalificeren en de beslissing dienaangaande over te laten aan een opsporingsambtenaar.

## 2. Doelbinding

De Wbp onderstreept het belang van het doelbindingsbeginsel bij de verwerking van (persoons)gegevens. Dat beginsel ziet op het voorkomen van het gebruik van een gegevensverzameling voor een ander doel dan waarvoor het is aangelegd. Het doel van een datawarehouse kan op dit moment nog op meer dan één wijze worden geïnterpreteerd. Zo kan worden betoogd dat het datawarehouse de strafrechtelijke handhaving van de rechtsorde tot doel heeft; een dataminingonderzoek in het kader van de opsporingstaak vindt uiteindelijk immers in dat kader plaats. In strikte zin ligt het doel evenwel in de realisatie van het dataminingonderzoek in het kader waarvan het datawarehouse is aangelegd. Deze (beperkte) interpretatie ligt volledig in lijn met het doelbindingsbeginsel en verdient met het oog op de handhaving van het verstrekkingenregime de voorkeur.

De over het algemeen binnen het politieapparaat gebruikelijke ‘free flow’ van informatie is met betrekking tot de gegevens in een gedurende het dataminingonderzoek aangelegd register ongewenst; dit vanwege de afwijkende functie van die gegevens. Een datawarehouse staat niet op zichzelf, maar maakt een vast onderdeel uit van een meeromvattend proces. In tegenstelling tot de meeste andere gegevens binnen het politieapparaat hebben de gegevens in een datawarehouse geen informatieve, maar een overwegend voorbereidende functie. Door een ruime uitleg van het doelbindingsbeginsel kunnen de gegevens in een datawarehouse voor allerlei toepassingen worden aangewend waarbij zou kunnen worden afgeweken van het verstrekkingenregime van de WPoI en het BPoI. Het is in beginsel niet noodzakelijk dat op ruime schaal kan worden beschikt over de gegevens in een datawarehouse; de bestaande wet- en regelgeving in de WPoI en het BPoI bieden voldoende alternatieve mogelijkheden voor het verkrijgen van toegang tot bepaalde informatie. Wanneer een wettelijk alternatief ontbreekt, heeft de wetgever het gebruik van de betreffende gegevens blijkbaar niet wenselijk geacht. Als gevolg daarvan ligt het in de lijn van het bestaande wettelijk stelsel dat opsporingsdiensten niet rechtstreeks informatie kunnen en mogen opvragen uit een datawarehouse. Het kan niet zo zijn dat bepaalde gegevens door middel van een bevraging van een datawarehouse alsnog kunnen worden verkregen. Slechts in een beperkt aantal, limitatief in de wet opgesomde gevallen dient een mogelijkheid te bestaan om gegevens direct uit een datawarehouse te verkrijgen. Daarbij kan worden gedacht aan gegevens die nog niet elders zijn opgeslagen, bijvoorbeeld opsporingsinformatie die gedurende een gericht dataminingonderzoek aan het licht komt en van belang kan zijn voor ander onderzoek of in aanmerking komt voor opname in een ander politieregister.

## 3. Koppeling

De koppeling speelt een belangrijke rol bij het kwalificatievraagstuk in het kader van het datawarehouse. In het voorgaande werd geconstateerd dat met betrekking tot een data-

miningonderzoek (en ook met betrekking tot het datawarehouse) geen verplichting bestaat om een datawarehouse als een politieregister aan te merken. Daarmee ontbreekt tevens de verplichting om te voorzien in een reglement en daarmee een wettelijke waarborg voor een verantwoorde gegevensverwerking. Een ongewenste situatie, temeer daar bepaalde vormen van dataminingonderzoek alleen mogelijk lijken wanneer een reglement aanwezig is.

Indien in het kader van een dataminingonderzoek sprake is van een koppeling, dient rekening te worden gehouden met het bepaalde in art. 6 WPolr. Op grond van art. 6 lid 2 WPolr is een koppeling slechts mogelijk overeenkomstig het voor het register geldende reglement. Uit de formulering van dit artikel wordt niet direct duidelijk of deze verplichting alleen geldt bij koppeling van een politieregister met een ander politieregister of een andere gegevensverzameling, of dat deze ook van toepassing is wanneer het datawarehouse niet als politieregister is gekwalificeerd. Wanneer het eerste het geval is, betekent dit dat het al dan niet kwalificeren van een datawarehouse bepalend is voor de vraag of de waarborgen die door de WPolr en het BPolr aan een koppeling worden gesteld van toepassing zijn. Die waarborgen zijn juist in het kader van een datawarehouse bijzonder belangrijk, aangezien het koppelen van gegevens(verzamelingen) een belangrijke rol speelt bij de verwerking daarvan in een datawarehouse. In dit verband lijkt de tweede uitleg waarschijnlijker. Wanneer een gegevensverzameling kan worden gekwalificeerd als een politieregister in de zin van de WPolr, dient het reglement van dat register te voorzien in een koppeling. Wanneer wordt gekoppeld met een ander politieregister dient ook het reglement van dat andere register daarin te voorzien. Geredeneerd vanuit het standpunt van het politieregister waarmee wordt gekoppeld vloeit deze verplichting immers ook voort uit art. 6 lid 2 WPolr. Wanneer er sprake is van een koppeling met een gegevensverzameling die niet als een politieregister kan worden aangemerkt, lijkt het op grond van art. 6 lid 2 WPolr niet noodzakelijk dat ook die andere gegevensverzameling beschikt over een reglement dat voorziet in een koppeling.<sup>12</sup> Uit de waarborgfunctie van art. 6 WPolr vloeit in beginsel een aanleiding tot kwalificatie van het datawarehouse voort. Indien een tijdelijk politieregister is betrokken bij een koppeling is art. 6 lid 2 WPolr niet van toepassing. In art. 13 lid 3 WPolr is naast een tijdelijke ontheffing van de reglementplicht namelijk ook voorzien in een tijdelijke ontheffing van het bepaalde in art. 6 lid 2 WPolr.

12. Met het oog op de formulering van art. 6 WPolr en *Kamerstukken II*, 1988 /89, 19 589, nr. 11, p. 13: ('een koppeling dient krachtens de regelgeving van alle in het geding zijnde registers toelaatbaar te zijn') kan hierover echter onduidelijkheid ontstaan. Wanneer gebruik wordt gemaakt van gegevens van buiten de politieke sfeer dient daarvoor in beginsel een wettelijke grondslag te zijn. Niet een eventueel reglement maar die wettelijke regeling is dan doorslaggevend bij de vraag naar een koppeling.

Omdat een reglement onlosmakelijk is verbonden met de aanwezigheid van een register, dient bij aanneming van een reglementplicht op grond van art. 6 lid 2 WPolr een politieregister aanwezig te zijn; dit wijst op een kwalificatie van het datawarehouse. In beginsel is bij een dataminingonderzoek (en ook bij de aanleg van een datawarehouse) steeds sprake van een koppeling. Ter voorbereiding van een dataminingonderzoek kunnen allehande gegevens(verzamelingen) worden samengebracht (gekoppeld) in een datawarehouse. Daarbij wordt het datawarehouse als zelfstandige gegevensverzameling gekoppeld met andere gegevens; het moet dus niet worden gezien als een zelfstandige gegevensbron, maar als een vergaarbak van gegevens uit verschillende bronnen. De reden om een datawarehouse niet als zelfstandige bron aan te merken hangt samen met het doelbindingsbeginsel, op grond waarvan de inhoud van een datawarehouse niet voor andere doeleinden dient te worden gebruikt. Mede vanwege de functionaliteit van een datawarehouse zal in het reglement steeds een voorziening dienen te worden opgenomen omtrent het koppelen van gegevens. Het is echter de vraag in hoeverre een verplichting om in het reglement van een datawarehouse aan te geven of en op welke wijze koppeling mogelijk is, noodzakelijk is. Het is voor een datawarehouse eigenlijk vanzelfsprekend dat het reglement ervan in een dergelijke regeling voorziet. In tegenstelling tot de meeste andere politieregisters, waarbij een koppeling slechts één van de mogelijke toepassingen is, wordt een datawarehouse aangelegd met als enig doel er, ter voorbereiding van een dataminingonderzoek, gegevens in op te slaan.

In beginsel bestaat op grond van art. 6 WPolr de behoefte om het datawarehouse te kwalificeren en vervolgens een reglement op te stellen waarin wordt voorzien in het koppelen van gegevens. Een situatie, waarin voor elk register apart kan worden vastgesteld of het al dan niet in aanmerking komt voor een koppeling, garandeert een goede controle. De WPolr bepaalt lid 3 dat ter bescherming van de persoonlijke levenssfeer bij AMvB nader regels omtrent koppeling kunnen worden gesteld; daarbij kan aansluiting worden gezocht bij de algemene lijn die zich in de adviezen van het CBP gaat aftekenen. Degene die het reglement vaststelt zal over het algemeen de meest-aangewezen persoon zijn om te beoordelen of en in hoeverre het gebruik van het betreffende register ten behoeve van dataminingonderzoek wenselijk is. In principe verschaft het altijd aanwezige reglement de uitvoerder van een dataminingonderzoek of de beheerder van een register duidelijkheid over de vraag, of gegevens al dan niet ontvangen respectievelijk verstrekt mogen worden. Ook kan de keuze voor het gebruik van een bepaald register beter worden afgestemd op veranderingen in de maatschappelijke opvattingen over privacy en opsporing. Daarvoor is dan immers geen ingrijpende wetswijziging nodig, maar kan worden volstaan met aanpassing van het reglement van het betreffende register. Door de gebruiksmogelijkheden per register in de reglementsbepalingen vast te stellen wordt voorzien in een flexibel regime, onder het wakend oog van het CPB als controlerende instantie.

Opgemerkt zij dat geen sprake is van koppeling ingeval dataminingonderzoek slechts betrekking heeft op één enkel register en geen gebruik wordt gemaakt van externe gegevens. In dergelijke gevallen blijft het bepaalde in art. 6 WPolr buiten beschouwing. Dat geldt eveneens voor gevallen waarin gebruik wordt gemaakt van externe gegevens die niet tot enige gegevensverzameling behoren. In beide situaties noopt het artikel noch tot een kwalificatie van het datawarehouse, noch tot het opstellen van een reglement.

#### 4. Praktische grondslag

De onderscheiding van een apart datawarehouse en een eventuele kwalificatie ervan als politieregister kan ook om meer praktische redenen in de rede liggen. In het kader van een dataminingonderzoek worden per definitie gegevens verwerkt. Om een verwerking mogelijk te maken zullen de gegevens waarop het onderzoek betrekking heeft op enigerlei wijze onderscheidbaar c.q. identificeerbaar dienen te zijn. Wanneer een datawarehouse apart wordt benoemd kan in een dergelijk onderscheidend karakter worden voorzien. Overigens zal bij een ongericht dataminingonderzoek ter verbetering van de informatiepositie van een bepaald politieregister in beginsel niet worden gewerkt met het oorspronkelijke politieregister. Nu het gaat om digitale informatie kan, zonder noemenswaardige moeite, een mirror<sup>13</sup> van het originele register worden gemaakt.<sup>14</sup> Daarmee wordt ook eventuele vervuiling van de oorspronkelijke politieregisters voorkomen en is een duidelijk onderscheid aangebracht tussen de bestaande politieregisters als zodanig en de gegevensverzameling (of mirror) die de functie van 'datawarehouse' vervult.

De aanleg van een apart datawarehouse ligt ook in de rede met het oog op de bewijsvoering en de mogelijkheid van het achteraf toetsen van een dataminingonderzoek. In geval er in het kader van een dataminingonderzoek gebruik wordt gemaakt van gegevens die afkomstig zijn van het internet, dient te worden voorzien in een registratiewijze die minder vluchtig is dan die waarop gegevens zich op het internet plegen te manifesteren: de informatie dient niet alleen op een bepaald moment beschikbaar te zijn, maar ook te blijven.

Ook de aard van het dataminingonderzoek kan pleiten voor een apart datawarehouse. Indien er sprake is van een ongericht dataminingonderzoek heeft het daartoe aangelegde datawarehouse in beginsel een permanent karakter. De gegevens die in het kader van een ongericht dataminingonderzoek worden verwerkt zijn overigens niet statisch van aard. Nieuwe gegevens dienen te worden ingevoerd en achterhaalde gegevens dienen te worden verwijderd met het oog op het waarborgen van een goed en betrouwbaar eindresul-

---

13. (Digitale) kopie.

14. Commissie Mevis 2001, p. 62, 'Het bewerken van gegevens zal veelal plaatsvinden met behulp van een kopie van de gegevens, buiten de normale bedrijfsvoering'.

taat. Eenmaal ingesteld, kan het onderzoek onbeperkt voortduren. Dit permanente karakter van een ongericht dataminingonderzoek kan een aanleiding vormen om te spreken van een apart datawarehouse als politieregister.

### 5. Bestaande wettelijke regeling

De vraag aangaande de kwalificatie van een gegevensverzameling, die tot stand komt in het kader van een gegevensverwerking met betrekking tot een verkennend onderzoek als bedoeld in art. 126gg Sv, wordt in feite al beantwoord door bestaande wet- en regelgeving: in art. 13 WPolr wordt bepaald, dat deze worden opgeslagen in een tijdelijk politieregister. Het belang dat wordt gehecht aan een duidelijke kwalificatie van de gegevens die in het kader van een verkennend onderzoek worden vastgelegd, wijst vrijwel onontkoombaar om de richting van kwalificatie van ieder datawarehouse, ongeacht het doel waarvoor het werd aangelegd.

### Resumerend

Dit onderzoek beoogt het scheppen van een juridisch kader voor de toepassing van het dataminingsproces ten behoeve van de opsporing. Behalve dat daarbij vanuit praktisch oogpunt in beginsel steeds sprake zal zijn van een aparte gegevenverzameling of datawarehouse, vormt de kwalificatie van dat datawarehouse één van de peilers van het juridische kader voor het plegen van dataminingonderzoek. Het benoemen van een datawarehouse als een aparte gegevensverzameling en de kwalificatie daarvan als politieregister zijn van groot belang voor de bescherming van de persoonlijke levensfeer. Die bescherming wordt gewaarborgd door de in de WPolr en het BPolr geregelde verbinding van politieregisters aan verschillende reglementen en afwijkende verstrekkingenregimes. Daarmee wordt een onlosmakelijke samenhang gecreëerd tussen een juiste (legitieme) verwerking van gegevens door opsporingsautoriteiten en een kwalificatie van die gegevens. Wanneer een datawarehouse wordt aangemerkt als een register in de zin van de WPolr dient ook die gegevensverzameling te worden gekwalificeerd en, alvorens het in werking mag treden, op grond van art. 9 WPolr te worden voorzien in een reglement bij dat datawarehouse. Dat reglement vervult een belangrijke functie omdat daarin regelingen kunnen worden opgenomen aangaande het datawarehouse, het dataminingonderzoek en de wijze waarop het uiteindelijke resultaat wordt verwerkt. In dit onderzoek wordt uitgegaan van het standpunt, dat de aanwezigheid van een datawarehouse en de kwalificatie daarvan in beginsel juridisch noodzakelijk zijn voor het gebruik van het dataminingsproces. Dit betekent evenwel niet per definitie dat die juridische noodzaak ook vanuit technisch oogpunt noodzakelijk is. Hoewel noch het onderscheidende vermogen van een datawarehouse, noch de aard van het dataminingonderzoek een kwalificatie van het datawarehouse als politieregister juridisch noodzakelijk maken, worden daardoor wel redenen gevormd die pleiten voor een kwalificatie als zelfstandige gegevensverzameling. De wijze waarop een kwalificatie in de praktijk tot stand kan komen wordt in het hierna volgende uiteengezet.

## 5.2 Kwalificatie datawarehouse

Voor een kwalificatie van een datawarehouse als politieregister staan verschillende mogelijkheden open. Daarbij ligt het vanuit praktisch oogpunt voor de hand, dat voor zowel de opslag van de te bewerken gegevens als het daaruit te behalen resultaat gebruik wordt gemaakt van één en hetzelfde register.<sup>15</sup> De WPolr en het BPolr voorzien in een wettelijke regeling met betrekking tot de opslag van gegevens door politie en justitie in een gewoon of in een bijzonder politieregister. In deze sectie zal voor een als politieregister aan te merken datawarehouse worden onderzocht, op welke wijze kwalificatie mogelijk is.<sup>16</sup>

### 5.2.1 Varianten dataminingonderzoek

Bij de kwalificatie van een datawarehouse dient er rekening mee te worden gehouden dat onderscheid kan worden gemaakt tussen diverse soorten van datawarehouses. Dat onderscheid is gelegen in de dataminingsvariant in het kader waarvan het datawarehouse tot stand is gebracht. De verschillende kaders waarbinnen aan het dataminingsproces uitvoering kan worden gegeven, spelen een rol bij de kwalificatie van het datawarehouse. Daarbij gaat het met name om het onderscheid tussen een ongericht en een gericht dataminingonderzoek.

#### Onggericht dataminingonderzoek

Een ongericht dataminingonderzoek dient ter verbetering van de (algemene) informatiepositie van een bepaald politieregister en kan betrekking hebben op zowel een gewoon als een bijzonder politieregister. In beide gevallen kan het betreffende politieregister worden aangemerkt als het basisregister. Dat register vormt het uitgangspunt van het onderzoek. Een ongericht dataminingonderzoek dat betrekking heeft op één bepaald politieregister kan worden uitgevoerd zonder gebruik te maken van externe gegevens. In dat geval vindt geen koppeling plaats. Het datawarehouse komt volledig overeen met het register waarop het dataminingonderzoek betrekking heeft, ofwel het basisregister. Wanneer een beheerder een dergelijk dataminingonderzoek binnen zijn politieregister uitvoert voorziet het basisregister in een kwalificatie en is geen directe juridische noodzaak aanwezig voor de aanleg van een datawarehouse. Het bij het basisregister behorende reglement vormt immers in beginsel een afdoende juridisch kader voor de verwerking van de gegevens in dat register. Het is overigens wel wenselijk om in het reglement aanvullende voorwaarden op te nemen aangaande de vorm en inhoud van het data-

15. Hierbij kunnen de functies van het politieregister dat als datawarehouse of basisregister fungeert, de mogelijkheden van het dataminingonderzoek beperken. In sectie 7.1 wordt hierop nader ingegaan.

16. Een ongericht dataminingonderzoek met betrekking tot een tijdelijk politieregister is in beginsel niet mogelijk. In sectie 9.3 wordt de achtergrond daarvan belicht. Tevens wordt uitvoerig, per register, onderzocht wat wel en wat niet mogelijk is bij een verwerking in het kader van het dataminingsproces.

miningonderzoek. Ondanks het feit dat in dit geval een directe juridische noodzaak tot kwalificatie ontbreekt, is er wel sprake van een aparte gegevensverzameling die als datawarehouse kan worden aangemerkt. Voor de goede orde zij opgemerkt, dat het dataminingonderzoek veiligheidshalve meestentijds zal worden uitgevoerd aan de hand van een kopie van het basisregister.

Bij een ongericht dataminingonderzoek waarbij meer dan één enkele gegevensverzameling betrokken is, zal in beginsel steeds een datawarehouse worden aangelegd. Gezien de bepalingen aangaande de koppeling is een juridische kwalificatie van het datawarehouse hier wel opportuun. Als uitgangspunt bij de bepaling van de kwalificatie wordt dan een basisregister aangewezen. Daarmee wordt voorkomen dat voor elk dataminingonderzoek een nieuw politieregister dient te worden aangelegd. Aangezien een basisregister op grond van art. 9 WPolr over een reglement beschikt, is dat reglement tevens van toepassing op het betreffende datawarehouse; daarmee wordt voorzien in een eventuele reglementsplicht voor dat datawarehouse. De keuze van het basisregister als uitgangspunt sluit naadloos aan op de systematiek van de WPolr en het BPolr. Het vormt een waarborg dat het dataminingonderzoek plaatsvindt conform de voorwaarden die de WPolr en het BPolr stellen aan de verwerking van gegevens die zich in de politieregister bevinden; daarnaast wordt voorkomen dat de strikte regels met betrekking de bijzondere politieregisters worden omzeild door een koppeling van die registers met andere registers.<sup>17</sup> Wanneer voor de kwalificatie van een datawarehouse aansluiting wordt gezocht bij het basisregister is het van belang dat het dataminingonderzoek steeds wordt uitgevoerd door, dan wel onder leiding van, de beheerder van dat basisregister. Bij uitvoering van het onderzoek door een derde zal er in beginsel sprake zijn van een verstrekking en zullen de waarborgen van het basisregister niet per definitie aanwezig zijn.

### **Gericht dataminingonderzoek**

In het kader van een gericht dataminingonderzoek wordt niet gestreefd naar de verbetering van de informatiepositie van een bepaald politieregister, maar naar een verbetering van de informatiepositie in een bepaald geval; er bestaat al een bepaald vermoeden of een verdenking. Dat is een belangrijk verschil met de ongerichte dataminingvariant. Een gericht dataminingonderzoek heeft in beginsel geen betrekking op een bestaand politieregister (als basisregister). De bestaande politieregisters dienen in beginsel de algemene politietaak en worden niet aangelegd met het oog op een enkel geval. Het tijdelijk politieregister vormt hierop een uitzondering. Dit bijzondere register wordt aangelegd met het oog op de uitvoering van de politietaak in een bepaald geval, of in het kader van een verkennend onderzoek als bedoeld in art. 126gg Sv.<sup>18</sup> In dat licht gezien behoort een

---

17. *Stcrt.* 12 oktober 2000, nr. 198. Zie ook art. 5a en 13d lid 3 WPolr.

18. Art.1 lid 1 sub j WPolr.

gericht dataminingonderzoek in het kader van een tijdelijk politieregister dus ook tot de mogelijkheden.<sup>19</sup> Het is echter zeer de vraag of überhaupt wel kan worden gesproken van een verbetering van de (specifieke) informatiepositie van een tijdelijk politieregister. In beginsel kan elk onderzoek dat leidt tot de aanleg van een tijdelijk politieregister worden beschouwd als een gericht dataminingonderzoek en kan dat register worden aangemerkt als het datawarehouse dat in dat kader wordt/is aangelegd. In deze optiek is een gericht dataminingonderzoek steeds een op zichzelf staand onderzoek waarbij nog geen sprake is van een basisregister. Daarmee wordt de mogelijkheid van een verbetering van de informatiepositie van een tijdelijk politieregister met behulp van een gericht dataminingonderzoek uitgesloten.

Bovenstaande interpretatie past geheel in het kader van de omstandigheden, waaronder een gericht dataminingonderzoek normaliter zal plaatsvinden. Het handelt immers om een nieuw onderzoek naar aanleiding van een bepaald geval, waarbij geen sprake is van een basisregister. Gezien de aard van een gericht dataminingonderzoek, namelijk een verwerking van externe gegevens, ligt het gebruik van externe gegevens in de rede. Daaruit volgt dat in beginsel ook rekening moet worden gehouden met de regels die gelden voor een koppeling en is kwalificatie dus noodzakelijk. Aangezien een basisregister ontbreekt moet gezocht worden naar een alternatieve wijze van kwalificatie.

### 5.2.2 *Kwalificatie datawarehouse gericht dataminingonderzoek*

Bij de kwalificatie van een datawarehouse dient rekening te worden gehouden met de kenmerken van het dataminingonderzoek in het kader waarvan het tot stand wordt gebracht. Voor de belangrijkste eigenschappen van een gericht dataminingonderzoek zij hier verwezen naar sectie 3.4.2. Voor een kwalificatie van een bij een gericht dataminingonderzoek behorend datawarehouse dient het register aan te sluiten op de genoemde kenmerken en moet derhalve voldoen aan de volgende voorwaarden:

- het register kan worden aangelegd ten behoeve van de politietaak in een bepaald geval;
- het dient inzetbaar te zijn voor uiteenlopende doeleinden;
- het biedt de mogelijkheid om er zachte gegevens in vast te leggen;
- het kent een beperkt verstrekkingenregime;
- het heeft een tijdelijk karakter.

Uitgaande van deze voorwaarden is onderzocht, welke van de bestaande politieregisters in aanmerking komt om te dienen als kwalificatie van het datawarehouse.

---

19. Volledigheidshalve zij opgemerkt, dat een gewoon politieregister ook kan worden aangelegd ten behoeve van een registratie in een bepaald geval. Daarvoor wordt echter alleen gekozen in die gevallen waarin geen behoefte bestaat aan nadere informatie, zodat een verdere verwerking van de betreffende gegevens niet nodig is.

### 5.2.2.1 Doelstelling

Een gericht dataminingonderzoek heeft betrekking op één bepaald geval. Uit de WPolr blijkt duidelijk dat, voor het registreren van gegevens ten behoeve van de politietaak in een bepaald geval, gebruik kan worden gemaakt van een tijdelijk politieregister. Tijdelijke registers kunnen ook worden gebruikt ten behoeve van misdaadanalyse en financieel rechercheren.<sup>20</sup> Het register wordt ad hoc aangelegd voor een in ruimte en tijd omgrensd doel, bijvoorbeeld de opsporing van een bepaald ernstig misdrijf.<sup>21</sup> De doelstellingen van een tijdelijk register zijn veel strikter omlijnd en minder algemeen dan die van de overige politieregisters. Het bereiken van het doel moet te voorzien zijn; bijvoorbeeld de dader van het ernstige misdrijf wordt gevonden of door het oprollen van een bende komt een einde aan een reeks brandstichtingen.<sup>22</sup> Voorts is het, in tegenstelling tot de andere bijzondere politieregisters, niet gebonden aan een bepaald doel en derhalve qua doelstelling net zo flexibel als het gerichte dataminingonderzoek zelf. Ingeval een onderzoek ziet op de bestrijding van de zware criminaliteit en het gebruik van een register zware criminaliteit voor de hand lijkt te liggen kunnen zich omstandigheden voordoen, waardoor een meer ingekaderde en op het specifieke geval gerichte registratie te prefereren is. In die omstandigheid wordt een tijdelijk register aangelegd voor de duur van het onderzoek naar dat naar tijd en ruimte omgrensde geval.<sup>23</sup>

De overige politieregisters zien niet op de politietaak in een bepaald geval en hebben een eigen, vaak veel ruimere doelstelling. Een gewoon politieregister dient in beginsel de algemene politietaak, onder meer blijkende uit het vrije verstrekkingenregime dat op deze registers van toepassing is. Het gebruik van een gewoon politieregister omvat enkel een registratie van gegevens; er bestaat geen behoefte aan nadere informatie. Bij een gericht dataminingonderzoek is per definitie juist altijd sprake van een nadere informatiebehoefte. Een register zware criminaliteit wordt aangelegd en bijgehouden ten behoeve van de bestrijding van de zware criminaliteit. De mogelijkheid tot de aanleg van dit register is begrensd door het bepaalde in art. 1 lid 1 sub k WPolr. Een gericht dataminingonderzoek is niet beperkt tot de bestrijding van de zware criminaliteit. Met het oog op de strekking en de werking van zowel het register zware criminaliteit als het als 'voorportaalregister'<sup>24</sup> hiervan fungerende voorlopige register moet worden geconcludeerd, dat een datawarehouse niet kan worden aangemerkt als en gerangschikt kan worden onder één van deze bijzondere politieregisters. Deze dienen elk een specifiek, eigen

---

20. *Kamerstukken II*, 1995/196, 24 072, nr. 14, p. 239.

21. *Kamerstukken II*, 1996/197, 25 398, nr. 3, p. 1-2.

22. *Kamerstukken II*, 1997/198, 25 398, nr. 6, p. 6.

23. *Kamerstukken II*, 1997/198, 25 398, nr. 6, p. 10.

24. *Kamerstukken II*, 1997/198, 25 398, nr. 6, p. 3. 'De opslag van gegevens in het vaststellingsregister houdt rechtstreeks verband met de wettelijke doelbinding van het register zware criminaliteit.'

belang dat niet strookt met het gebruik van deze registers voor kwalificatiedoeleinden in dit geval.

Op basis van het vorengaande kan worden geconcludeerd dat een tijdelijk politieregister het eerst aangewezen register is om te dienen als kwalificatie van het datawarehouse dat in het kader van een gericht dataminingonderzoek tot stand komt. Daaraan kan nog worden toegevoegd dat voor deze keuze ook steun wordt gevonden in het feit, dat met behulp van een gericht dataminingonderzoek uitvoering kan worden gegeven aan een verkennend onderzoek van art. 126*gg* Sv<sup>25</sup>. De gegevens die in dit kader worden verwerkt worden immers vastgelegd in een tijdelijk politieregister.

#### 5.2.2.2 *Verstrekkingenregime*

Anders dan bij een gericht dataminingonderzoek dient een ongericht dataminingonderzoek ter verbetering van de (algemene) informatiepositie van een bepaald politieregister en kan betrekking hebben op zowel een gewoon als een bijzonder politieregister. In beide gevallen kan het betreffende politieregister worden aangemerkt als het basisregister. Het gebruik van het basisregister bij een ongericht dataminingonderzoek waarborgt in beginsel, dat een verwerking die in het kader van dat onderzoek plaatsvindt in overeenstemming is met het verstrekkingenregime van de WPolr en het BPolr. Op registers waarin gevoelige dan wel zachte gegevens kunnen worden opgeslagen is een afwijkend, strenger verstrekkingenregime van toepassing dan op de registers waarin de opslag van dergelijke gegevens niet mogelijk is. Met het verstrekkingenregime wordt beoogd ontoelaatbare inbreuken op de persoonlijke levenssfeer te voorkomen. Bij een verwerking van zowel harde als zachte opsporingsinformatie dient te worden uitgegaan van de gegevens waarop het strengste regime van toepassing is.

Aangezien bij een gericht dataminingonderzoek het basisregister ontbreekt, dient voor de kwalificatie van een datawarehouse te worden uitgegaan van de gegevens die men in het kader van het onderzoek wil verwerken. Een gericht dataminingonderzoek is een flexibel instrument dat kan worden gebruikt voor allerlei onderzoek, waarbij zowel harde als zachte opsporingsinformatie wordt verwerkt. In verband hiermee dient het verstrekkingenregime van het datawarehouse overeen te komen met het regime dat normaal gesproken op grond van de WPolr en het BPolr op deze gegevens van toepassing is. Het gaat daarbij vooral om de bijzondere politieregisters van par. 3a WPolr. Kenmerkend voor deze registers is de behoefte aan een beperkt regime met betrekking tot het gebruik, de opslag en de verstrekking van de gegevens die erin worden opgeslagen. Deze behoefte hangt samen met het overwegend zachte karakter van de in de bijzondere politieregisters opgeslagen gegevens.

---

25. Zie sectie 3.5.2.2.

### Registratie van zachte gegevens

Met het oog op de bescherming van de persoonlijke levenssfeer is uitputtend geregeld voor welke doeleinden binnen de uitvoering van de politietaak zachte gegevens mogen worden vastgelegd. De (langdurige) registratie van zachte opsporingsinformatie voor operationeel gebruik is alleen gerechtvaardigd, wanneer het gaat om misdrijven die ofwel naar hun aard een ernstige inbreuk op de rechtsorde opleveren, ofwel het rechtsgevoel ernstig schokken. In die gevallen dient gebruik te worden gemaakt van een register zware criminaliteit. Voor de overige politieregisters geldt dat het een beheerder niet vrij staat om gewone politieregisters aan te leggen met betrekking tot personen ten aanzien van wie (slechts) een redelijk vermoeden bestaat dat zij zijn betrokken bij het beramen of plegen van strafbare feiten, en evenmin ten aanzien van personen waarover nog minder aanwijzingen van betrokkenheid bij strafbare feiten bestaan. Volgens de MvT<sup>26</sup> bij de bijzondere politieregisters is de registratie van zachte gegevens voor een ander doel dan de bestrijding van de zware criminaliteit alleen denkbaar in een tijdelijk of een voorlopig politieregister<sup>27</sup>. De behoefte die bij een gericht dataminingonderzoek kan bestaan aan het vastleggen van zachte gegevens wijst, met het oog op het voorgaande, niet in de richting van het gebruik van een gewoon politieregister bij de kwalificatie van het datawarehouse. In een datawarehouse mogen in principe immers geen gegevens worden vastgelegd waarop van origine een strenger verstrekkingenregime van toepassing is dan het regime van het betreffende datawarehouse.

Bij het verstrekkingenregime spelen ook de art. 5a en 13d lid 3 WPolr een rol. Daarin worden nadere regels gesteld aan de opslag van nieuwe informatie die is verkregen als gevolg van een koppeling<sup>28</sup>, dit onder meer om te voorkomen dat de strikte regels met betrekking tot de bijzondere politieregisters kunnen worden omzeild via de koppeling van die registers met andere registers. Met name in het geval van een gericht dataminingonderzoek zal vaak sprake zijn van een koppeling.

### Art. 5a WPolr

Op grond van art. 5a WPolr kunnen zachte gegevens kortstondig worden vastgelegd in een gewoon politieregister. Om te bepalen of binnengekomen tips en meldingen in aanmerking komen voor registratie in een (bijzonder) politieregister dienen zij te worden geëvalueerd. Daartoe kan gebruik worden gemaakt van een gewoon politieregister als bijvoorbeeld het BPS. Gegevens omtrent onverdachte personen (ongeacht het strafbare feit

---

26. *Kamerstukken II*, 1997/198, 25 398, nr. 6, p. 9.

27. Het is de vraag of een registratie in een voorlopig politieregister inderdaad plaatsvindt voor een ander doel dan de bestrijding van de zware criminaliteit. Een voorlopig politieregister dient, als voorportaal van het register zware criminaliteit immers ook indirect de bestrijding daarvan.

28. *Stcrt.* 12 oktober 2000, nr. 198.

waar het om gaat) mogen daar niet langer dan vier maanden worden opgeslagen. Met gegevens omtrent ‘onverdachte personen’ wordt bedoeld op diegenen over wie de politie gegevens heeft verkregen of vergaard die duiden op betrokkenheid bij strafbare feiten, maar waaruit nog geen redelijk vermoeden voortvloeit dat zij bepaalde feiten hebben begaan.<sup>29</sup> De categorie van onverdachte personen van art. 5a WPolr is daarmee beperkt. Op grond van de huidige WPolr kunnen gegevens over onverdachte personen in beginsel op vier verschillende manieren binnen de politie worden opgeslagen<sup>30</sup>, te weten in een tijdelijk politieregister, een voorlopig politieregister, een register zware criminaliteit en (kortstondig) in een gewoon politieregister. In het laatste geval blijft de status van de gegevens onveranderd, maar na vier maanden is daarop een ander (lees strenger) verstrekkingenregime van toepassing. In wezen is dus sprake van een opschorting van de bescherming van de persoonlijke levenssfeer van vier maanden. Rechtvaardiging van die situatie kan gevonden worden in het belang van een verantwoorde registratie (in een gewoon politieregister) op het moment waarop gegevens omtrent onverdachte personen bij de politie binnenkomen, teneinde te kunnen bepalen of zij in aanmerking komen voor registratie in een bijzonder politieregister. Het is echter de vraag, of art. 5a WPolr een opening biedt om een – in het kader van een gericht dataminingonderzoek tot stand gekomen – datawarehouse te kwalificeren als een gewoon politieregister. Het lijkt ongewenst en ongerechtvaardigd dat, met een beroep op dat artikel, gegevens omtrent onverdachte personen ook voor andere doeleinden in een gewoon politieregister kunnen worden vastgelegd. De wetgever heeft met art. 5a WPolr juist beoogd een grens te stellen aan het gebruik van zachte informatie in verband met de uitvoering van de politietaak in het kader van de strafrechtelijke handhaving van de rechtsorde. De aard van die gegevens is moeilijk rijmbaar met een zodanige interpretatie van art. 5a WPolr dat zachte gegevens, waarop normaal gesproken een beperkt verstrekkingenregime van toepassing is, te pas en te onpas ook in een gewoon politieregister kunnen worden opgenomen.

#### Art. 13d lid 3 WPolr

Op grond van art. 13d lid 3 WPolr<sup>31</sup> staat het een beheerder niet in alle gevallen vrij om te bepalen op welke wijze hij bepaalde gegevens registreert. Het vastleggen en koppelen (in het kader van een koppeling vindt ook een registratie van gegevens plaats) van persoonsgegevens voor de doeleinden die staan omschreven in art. 1 lid 1 onder *j*, *k* en *l*

29. Dit in tegenstelling tot het *Rapport Gegevensuitwisseling en Terrorismebestrijding* 2003 waarin ook de gegevens onder 13a lid 1 sub b WPolr worden aangemerkt als gegevens omtrent onverdachte personen. Deze subjecten vallen echter niet binnen de definitie van het begrip ‘onverdachte personen’ (*Kamerstukken I*, 1998/99, 25 398, nr. 63b, p. 6-7).

30. *Kamerstukken II*, 1997/98, 25 398, nr. 6, p. 9.

31. In art. 13d lid 3 WPolr wordt gesproken over het vastleggen en het gebruiken van persoonsgegevens’. Met het oog op de systematiek van de Wbp zou in plaats hiervan beter kunnen worden gesproken van ‘een verwerking van persoonsgegevens’.

WPolr is alleen toegestaan overeenkomstig het bepaalde in par. 3a WPolr, waaruit een tweetal conclusies kunnen worden getrokken.

1. Voor de doelstellingen waarvoor de bijzondere politieregisters kunnen worden aangelegd, mogen geen gewone politieregisters worden aangelegd. Het vastleggen van persoonsgegevens voor die doelstellingen is alleen mogelijk overeenkomstig par. 3a WPolr.
2. Voor de wijze waarop al in de bijzondere politieregisters vastgelegde gegevens verder mogen worden verwerkt (vastgelegd en gebruikt), dient het bepaalde daaromtrent in par. 3a WPolr in acht te worden genomen.

Volgens de MvT<sup>32</sup> beoogt het derde lid van art. 13d WPolr waarborgen te scheppen, zonder welke de gegeven regels binnen de WPolr en het BPolr illusoir zouden zijn. Indien het mogelijk is omtrent personen, die in aanmerking komen voor registratie in het register zware criminaliteit en het voorlopig politieregister, registers aan te leggen met een zelfde of nagenoeg dezelfde doelstelling, maar met een andere naam, dan kunnen de waarborgen die par. 3a WPolr biedt eenvoudig worden omzeild. Opmerkelijk is dat de MvT in dit verband niet het tijdelijk politieregister noemt, terwijl dat eveneens behoort tot de bijzondere politieregisters van par. 3a WPolr. Hoewel dat register voor uiteenlopende doeleinden kan worden aangelegd, betreft het steeds de politietaak in een bepaald geval. Met het oog hierop kan worden betoogd dat op grond van art. 13d lid 3 WPolr ook de registratie van gegevens in een bepaald geval slechts mogelijk is in overeenstemming met par. 3a WPolr.<sup>33</sup>

De koppeling van bijzondere politieregisters wordt in de MvA<sup>34</sup> in verband gebracht met art. 13d lid 3 WPolr. Aangegeven wordt dat nieuw verkregen informatie, voortkomende uit een koppeling met als doelstelling de opsporing van de misdrijven waarvoor het register zware criminaliteit kan worden aangelegd, ingevolge art. 13d lid 3 WPolr slechts kan worden vastgelegd en gebruikt overeenkomstig de regels van par. 3a WPolr. Gelet op de formulering van art. 13d lid 3 WPolr lijkt de interpretatie die in de MvA aan de werking van dit artikel wordt gegeven te beperkt te zijn. Volgens de wetgever dient alleen met betrekking tot het resultaat van een koppeling rekening te worden gehouden met par. 3a WPolr. De waarborgen van die sectie lijken niet van toepassing te zijn op de registratie die plaatsvindt in het kader van de koppeling zelf (in dit geval het datawarehouse). Ook bij die koppeling zelf worden echter persoonsgegevens geregistreerd in een datawarehouse. Die registratie gaat aan de bewerking vooraf en dient hetzelfde doel. Nu op grond

---

32. *Kamerstukken II*, 1996/97, 25 398, nr. 3, p. 24.

33. Meer specifiek in overeenstemming met het bepaalde in art. 13 WPolr.

34. *Kamerstukken I*, 1998/99, 25 398, nr. 63b, p. 8.

van art. 13d lid 3 WPolr iedere registratie van persoonsgegevens voor één van de doelstellingen van par. 3a WPolr dient te voldoen aan de voorwaarden van par. 3a WPolr, zal dat niet alleen gelden voor het resultaat van de koppeling maar ook voor het datawarehouse dat in het kader van de koppeling tot stand komt.

### **Doelbinding datawarehouse**

Door bij de kwalificatie van het datawarehouse uit te gaan van een register met een beperkt verstrekkingenregime wordt voorzien in de in sectie 5.1.2 beschreven doelbinding. Zoals daar uiteengezet is het wenselijk, de gegevens in een datawarehouse slechts te gebruiken voor het (doel van het) bijbehorende dataminingonderzoek. Een gewoon politieregister zal in dit verband een onbevredigende oplossing zijn. Gezien het verstrekkingenregime van een gewoon politieregister zullen de gegevens in het datawarehouse met die kwalificatie immers vrij toegankelijk zijn binnen het politieapparaat, ongeacht voor welk doel. Dit open verstrekkingenregime staat op gespannen voet met de ingrijpende aard van het dataminingonderzoek en het soort gegevens dat in het kader daarvan kan worden verwerkt. Om die reden geniet een kwalificatie als bijzonder politieregister de voorkeur. Gegevens in een als tijdelijk politieregister gekwalificeerd datawarehouse kunnen, op grond van art. 13 lid 2 WPolr, immers alleen worden gebruikt voor het doel waarvoor dat register is aangelegd.

#### *5.2.2.3 Tijdelijk karakter*

Politieregisters die de algemene politieke informatiepositie dienen zijn in beginsel steeds permanent van aard. De behoefte waarin zij voorzien is voortdurend aanwezig. Ook een voorlopig politieregister en een register zware criminaliteit zien niet op een specifieke zaak, maar vormen een bron van informatie waarvan het voortbestaan niet afhankelijk is van het bereiken van een bepaald doel. Het tijdelijk politieregister vormt hierop een uitzondering. Het wordt aangelegd voor een specifiek doel en eindigt op het moment waarop dat doel is bereikt. Een gericht dataminingonderzoek wordt, naast de gerichte doelstelling en de verwerking van zachte gegevens, gekenmerkt door de tijdelijke aard ervan. Het onderzoek eindigt wanneer het doel ervan is bereikt. Het bijbehorende datawarehouse dient, behoudens de daarvoor geldende wettelijke uitzonderingen, te worden vernietigd. Het tijdelijk politieregister sluit aan op het tijdelijke karakter van een gericht dataminingonderzoek en leent zich om die reden goed voor kwalificatie van het datawarehouse.

### **Resumerend**

Een tijdelijk register wordt aangelegd met het oog op de uitvoering van de politietaak in een bepaald geval of in het kader van een verkennend onderzoek zoals bedoeld in art. 126gg Sv. Behalve door een beperkte levensduur onderscheidt het zich van de permanente politieregisters door een concrete, vast te omlijnen doelomschrijving welke ook gevolgen heeft voor het verstrekkingenregime. Het doel van het onderzoek in het kader

waarvan een tijdelijk register wordt aangelegd behoeft niet noodzakelijkerwijs verband te houden met de ernst van de misdrijven genoemd in de doelomschrijving van het register zware criminaliteit. Het gebruik van een tijdelijk register is niet beperkt tot de zware criminaliteit, maar sluit dit ook niet uit. Het tijdelijk register kan in beginsel alle categorieën van persoonsgegevens bevatten, voor zover nodig voor het doel van het onderzoek waarvoor het register wordt aangelegd. Dit betekent dat ook de opslag van zachte gegevens in dit register mogelijk is. Kenmerkend voor gegevens die in tijdelijke registers worden opgeslagen is dat het verzamelingen van persoonsgegevens zijn die, wanneer het concrete, naar plaats en tijd gedefinieerde doel waarvoor zij zijn vastgelegd is bereikt, niet meer nodig zijn. Dit in tegenstelling tot de (permanente aard van) registers met een algemene, door de beheerder nader in te vullen doelstelling en registers met een wettelijk omschreven doelstelling zoals het register zware criminaliteit en het voorlopig register.<sup>35</sup>

De ingrijpende aard van een gericht dataminingonderzoek en het soort gegevens dat in het kader daarvan wordt verwerkt, sluiten in beginsel de mogelijkheid uit om als kwalificatie gebruik te maken van een gewoon politieregister. Ook het voorlopig politieregister en het register zware criminaliteit komen, onder meer vanwege hun specifieke doelstellingen, daarvoor niet in aanmerking. Van de bestaande politieregisters blijkt het tijdelijk politieregister van art. 13 WPolr het beste aan te sluiten op de voorwaarden die dienen te worden gesteld aan een in het kader van een gericht dataminingonderzoek aangelegd datawarehouse. Daarnaast is het toepassingsbereik van het tijdelijk register in overeenstemming met het flexibele karakter van een gericht dataminingonderzoek.

### 5.2.3 *Ontbreken reglement tijdelijk politieregister*

Op grond van art. 13 lid 3 WPolr kent een tijdelijk politieregister geen directe verplichting tot het opstellen van een reglement<sup>36</sup> gedurende een bij AMvB te bepalen termijn<sup>37</sup>. Ook is in dat artikel voor die termijn niet voorzien in een regeling in het reglement aangaande de koppeling in de zin van art. 6 WPolr. Volgens dat laatstgenoemde artikel is een koppeling normaal gesproken evenwel slechts toegestaan overeenkomstig het voor het register geldende reglement. In art. 4 lid 2 BPolr is bepaald dat een koppeling van een tijdelijk politieregister met een ander register alleen mogelijk is voor zover dat noodzakelijk is voor het doel waarvoor het tijdelijk politieregister is aangelegd. Om te kunnen nagaan of in een bepaald geval aan dat artikel wordt voldaan, dient het doel van een

---

35. *Kamerstukken II*, 1997/98, 25 398, nr. 6, p. 3-6.

36. *Kamerstukken II*, 1996/97, 25 403, nr. 3, p. 95. Ook met betrekking tot een tijdelijk register dat wordt aangelegd ten behoeve van een verkennend onderzoek volstaat een voorziening waarvoor niet de reglementeringsplicht geldt en waaraan evenmin de overige, daarmee verband houdende, voorwaarden voorafgaand aan de ingebruikneming worden gesteld.

37. De beheerder van een tijdelijk register dient binnen een week het CBP hiervan in kennis te stellen, tenzij het register dan inmiddels is vernietigd.

betreffende tijdelijke politieregister bekend te zijn. Dat doel wordt normaliter vastgelegd in het reglement van het register.<sup>38</sup> Aangezien het tijdelijk politieregister in beginsel een reglement ontbeert is onduidelijk, hoe in het geval van een koppeling uitvoering aan art. 4 lid 2 BPolr dient te worden gegeven.

De gedachte achter de uitzonderingspositie van een tijdelijk politieregister betreft vooral een noodzaak tot onmiddellijk optreden. Deze vereist een voorziening die de aanleg en in gebruikneming van een register mogelijk maakt alvorens daarvoor een reglement aan te leggen en te voldoen aan de overige daarmee verband houdende voorwaarden<sup>39</sup>. Daarnaast speelt een mogelijke belemmering van het daadwerkelijke onderzoek als gevolg van vroegtijdige publicatie van een reglement, en daarmee de doelstelling van het register, een rol. Vanwege de toegevoegde waarde van een reglement voor een dataminingonderzoek is het de vraag, of de ontheffing van de reglementplicht voor het tijdelijk politieregister in de huidige vorm moet worden gehandhaafd. De aard en de te verwachten hoge gebruiksfrequentie van met name de gerichte dataminingvariant afwegende tegen het belang van factoren als uniformiteit, zorgvuldigheid en het toezicht van het CBP, lijkt herziening raadzaam, zo niet noodzakelijk. Het ontbreken van een directe verplichting tot het opstellen van een reglement betekent niet dat dit ook niet mogelijk zou zijn. Er kan steeds vrijwillig in een reglement worden voorzien. Met het oog op het belang van de hierboven genoemde factoren verdient een minder vrijblijvende oplossing echter de voorkeur. In dit verband zij gewezen op het modelreglement<sup>40</sup> voor een tijdelijk politieregister waarvan het CBP heeft verklaard dat het Modelreglement Tijdelijk Register in overeenstemming is met de WPolr. Dit modelreglement is tot stand gekomen op grond van art. 12 lid 1 WPolr waarin, ter bevordering van de eenduidigheid van de informatiehuishouding en de vermindering van de administratieve last, de mogelijkheid is gecreëerd om een modelreglement vast te stellen voor een bepaald politieregister.

#### 5.2.3.1 Modelreglement

Een reglement waarin wordt voorzien in uniformiteit, zorgvuldigheid en het toezicht van het CBP kan worden beschouwd als aanvulling op het beperkte verstrekkingenregime van het tijdelijk politieregister. De keuze voor een tijdelijk politieregister in combinatie met een reglement vormt een waarborg voor verantwoorde gegevensverwerking. Hoewel bij een gericht dataminingonderzoek niet per definitie sprake hoeft te zijn van een noodzaak tot onmiddellijk optreden, is het om praktische redenen onwenselijk om voor elk gericht dataminingonderzoek afzonderlijk in een reglement te voorzien. Deze zijn voor-

38. Art. 10 lid 2 onder a WPolr.

39. *Kamerstukken II*, 1985/86, 19 589, nr 3, p. 19-20 en *Kamerstukken II*, 1997/98, 25 398, nr. 6, p. 6-7.

40. *Stert. 11 juli 2003, nr. 131.*

namelijk gelegen de mogelijk hoge gebruiksfrequentie van de gerichte dataminingvariant, in combinatie met het flexibele karakter van het onderzoek.

Met een modelreglement kan worden voorzien in een regeling die volledig is toegesneden op de specifieke eisen die aan een dataminingonderzoek moeten worden gesteld. Bij het opstellen van het reglement kan met het flexibele karakter van het dataminingproces rekening worden gehouden door bijvoorbeeld een ruime doelstelling te formuleren. Daarnaast kan daarbij de rol van het CBP als positieve bijkomende factor worden betrokken als een aanvullende garantie voor het legitieme karakter van het reglement voor wat betreft de gegevensverwerking in het kader van een dataminingonderzoek. Ten slotte levert het een positieve bijdrage aan het bereiken van meer eenheid in de manier waarop met het resultaat van een dataminingonderzoek wordt omgegaan.

### **5.3 Afsluitend**

In dit hoofdstuk is uiteengezet op welke wijze de gegevens kunnen worden vastgelegd die in het kader van een dataminingonderzoek worden verwerkt. Wanneer deze gegevensverzameling, die in het kader van het dataminingproces wordt aangeduid als datawarehouse, kan worden aangemerkt als een politieregister in de zin van de WPolr is het wenselijk, dat het ook als zodanig wordt gekwalificeerd. Wanneer een datawarehouse tot stand komt bij een ongericht dataminingonderzoek, kan steeds worden teruggegrepen naar het politieregister waarop het onderzoek betrekking heeft, het zogenaamde basisregister. In het verlengde daarvan is het van belang dat het onderzoek wordt uitgevoerd door, dan wel onder het gezag van, de beheerder van het desbetreffende politieregister. Wanneer dit niet het geval is, is er sprake van verstrekking en kunnen andere regels gelden. Het basisregister dient als kwalificatie van het datawarehouse en voorziet ook in een reglement. Het verdient aanbeveling dat in dergelijke reglementen wordt voorzien in de wijze, waarop uitvoering aan een dataminingonderzoek dient te worden gegeven. Aangezien ingeval van een gericht dataminingonderzoek in beginsel geen basisregister aanwezig is, dient het datawarehouse op een andere wijze te worden gekwalificeerd. Het tijdelijk politieregister blijkt daarvoor het meest geschikt. De in dit hoofdstuk neergelegde bevindingen zijn schematisch samengevat in schema 6.

Datamingvariant	Politierregister	Basisregister	Kwalificatie datawarehouse
<b>Ongericht dataminingonderzoek</b>	Gewoon politie-register	Ja	Basisregister
	Bijzonder politie-register*	Ja	Basisregister
<b>Gericht datamingonderzoek</b>	Tijdelijk politieregister	Ja	Basisregister
	Geen	Nee	Tijdelijk politieregister

\* het tijdelijk politieregister uitgezonderd

*Schema 6 Overzicht kwalificatie datawarehous*



---

## 6 Koppeling

Bij het proces van datamining speelt het deels of geheel koppelen van gegevensbestanden een belangrijke rol. Terwijl het raadplegen van gegevensbestanden en het koppelen van of met gegevensbestanden in de hedendaagse (opsporings)praktijk bijna als onderling uitwisselbare begrippen worden beschouwd, is dit vanuit juridisch perspectief zeker niet het geval. In juridische zin zijn aan koppeling voorwaarden verbonden, zoals de reglementsplicht.<sup>1</sup> Bij het vaststellen van een juridisch kader voor het gebruik van dataminingstechnieken ten behoeve van de opsporing dient daarom duidelijkheid te bestaan over de vraag, wanneer precies sprake is van een koppeling als bedoeld in art. 6 WPoI.

Met betrekking tot de koppeling of het leggen van verbanden tussen bepaalde gegevens(bestanden) kunnen zich uiteenlopende casusposities voordoen.<sup>2</sup> Koppeling is geen nader gespecificeerd begrip, hetgeen de bestempeling tot een bepaalde koppelvorm niet eenvoudig maakt. Teneinde een weg te vinden in de wirwar van termen die in dit verband worden gebruikt (koppeling, registervergelijking, bewerking, verwerking, raadpleging, verstrekking, integratie, computerprofiling, computer matching, integratie, en verificatie) is nagegaan, hoe deze zich verhouden tot de juridische koppeling van art. 6 WPoI ten behoeve van de opsporing. Ook wordt ingegaan op de reikwijdte van de juridische koppeling en de vraag of het koppelingsbegrip zoals de wetgever dat indertijd voor ogen heeft gestaan nog volstaat, gezien de huidige uitgebreide mogelijkheden van gegevensverwerking. Ten slotte is onderzocht op welke wijze de juridische koppeling van art. 6 WPoI kan worden toegepast binnen het dataminingsproces.

### 6.1 Koppelingsvormen

In de literatuur<sup>3</sup> worden vier belangrijke vormen van koppeling onderscheiden: verificatie, computer matching, computerprofiling en integratie. In deze sectie wordt ieder van deze vormen besproken teneinde deze in verband te brengen met de vraag, hoe zij zich verhouden tot het wettelijke koppelingsbegrip van art. 6 WPoI.

---

1. Art. 6 lid 2 WPoI.

2. *Kamerstukken II*, 1997/98, 25 892, nr. 3, p. 93.

3. Schreuders 2001, p. 24 en U.S. Congress, Office of Technology Assessment 1986.

### Verificatie

Verificatie<sup>4</sup> betreft het uitwisselen van gegevens met als doel, door toetsing de juistheid of volledigheid van die gegevens vast te stellen. Het gaat daarbij om gegevens van een bepaalde persoon of een bepaalde groep van personen, die door directe identificatie (op naam of nummer) bekend zijn bij de initiatiefnemer van de gegevensuitwisseling. Deze vorm van gegevensuitwisseling wordt ook wel aangeduid als ‘personal dataveillance’. Clarke<sup>5</sup> definieert dit begrip als volgt:

*‘Personal dataveillance is the systematic use of personal data systems in the investigation or monitoring of the actions or communications of an identified person. In general, a specific reason exists for the investigation or monitoring of an identified individual. It may also, however, be applied as a means of deterrence against particular actions by the person, or repression of the person’s behaviour’.*

Er is in beginsel sprake van een bepaalde aanleiding (trigger) op grond waarvan bijvoorbeeld een overheidsorgaan bepaalde gegevens zal verifiëren aan de hand van andere gegevens(bestanden). Zo kan het bij het verstrekken van een uitkering van belang zijn om vooraf te controleren of een soft-nummer<sup>6</sup> en de daarbij behorende persoonsgegevens juist zijn, zodat de bepaling op het recht van een uitkering plaatsvindt op basis van de juiste gegevens. De Belastingdienst kan daartoe een verificatie (hoort het soft-nummer bij de betreffende persoonsgegevens) of een identificatie (welk soft-nummer hoort bij de persoonsgegevens) uitvoeren. Hoewel deze vorm van vergelijken betrekking kan hebben op meerdere personen, ligt de nadruk in beginsel op het individu. Aangezien de verificatie vooral effectief is wanneer deze onmiddellijk plaatsvindt, bestaat er behoefte aan een snelle toetsing. Daarbij kan het gebruik van verwijzindexen, waarmee de benodigde informatie eenvoudig en efficiënt kan worden geraadpleegd zonder daartoe de volledige gegevensbestanden te moeten doorzoeken, uitkomst bieden. Bijkomend voordeel daarvan is, dat een (eventuele) inbreuk op de persoonlijke levenssfeer beperkt blijft. De volgende zaken zijn kenmerkend voor verificatie<sup>7</sup>:

- verificatie vindt plaats op individuele basis en kan betrekking hebben op een op voorhand bepaalde (bekende) persoon of groep van personen;
- verificatie kan betrekking hebben op één of meerdere gegevensverzamelingen;
- de toetsing gaat vooraf aan een bepaalde beslissing<sup>8</sup>;

---

4. Ook wel ‘computer assisted front-end verification’ genoemd.

5. Clarke 1995.

6. Het soft-nummer (sociaal-fiscaal nummer) wordt door veel overheids- en semi-overheidsinstanties gebruikt als uniek nummer bij de door hen geadmistreerde persoonsgegevens.

7. U.S. Congress, Office of Technology Assessment 1986, p. 68.

8. Bijvoorbeeld het verstrekken van een lening.

- het doel is gelegen in voorkomen en afschrikken en niet zozeer in signaleren en bestraffen;
- verificatie is vooral effectief wanneer deze onmiddellijk plaatsvindt<sup>9</sup>;
- het individu waarop de verificatie betrekking heeft, is over het algemeen op de hoogte van de (mogelijkheid tot) verificatie.

### Computer matching

Computer matching<sup>10</sup> is het vergelijken van twee of meer gegevensverzamelingen, ten einde aan de hand van bepaalde kenmerken of vooronderstellingen tot dan toe onbekende personen op te sporen. Deze koppelingsvorm wordt ook wel ‘mass dataveillance’<sup>11</sup> genoemd.

*‘Mass dataveillance is the systematic use of personal data systems in the investigation or monitoring of the actions or communications of groups of people. In general, the reason for investigation or monitoring is to identify individuals who belong to some particular class of interest to the surveillance organisation. It may also, however, be used for its deterrent effects of a whole population, for a reason related to some suspected but as yet unidentified portion of that population.’*

Bij computer matching kan onderscheid worden gemaakt tussen ‘structureel matchen’ (regelmatig in het kader van bijvoorbeeld een project) en ‘incidenteel matchen’ (eenmalig). Gezocht kan worden naar situaties waarin een bepaalde persoon in meer dan één bestand voorkomt wanneer dat normaal gesproken niet zo zou moeten zijn. Afhankelijk van het doel van het onderzoek kan ook worden gezocht naar personen die niet in meer dan één bestand voorkomen, terwijl dat juist wel zo zou moeten zijn. Bij computer matching gaat het vaak om zeer uitgebreide onderzoeken die betrekking hebben op een bepaalde categorie van personen en niet zozeer op die personen als individu<sup>12</sup>. Het aantal personen dat bij de vergelijking betrokken is wordt in beginsel alleen beperkt door de vraag of zij al dan niet voldoen aan de kenmerken of vooronderstellingen welke aan de computer match ten grondslag liggen. Er is sprake van een veel ruimere ‘trigger’ dan bij bijvoorbeeld verificatie het geval is. Computer matching biedt de mogelijkheid om omvangrijke gegevensbestanden te verwerken, waardoor het voor het individu steeds moeilijker wordt om te weten hoe zijn of haar persoonlijke informatie wordt gebruikt.

9. Hier kan worden gedacht aan een verwijzindex zoals het BPS.

10. “Computer matching is the comparison of machine-readable records containing personal data relating to many people, in order to detect cases of interest. The technique is called ‘computer matching’ in the United States, and ‘data matching’ in Australia and Canada.” ‘Dataveillance by governments: the technique of computer matching’, Clarke 1994, p. 46-85 en Schreuders 2001, p. 24.

11. Clarke 1995.

12. U.S. Congress, Office of Technology Assessment 1986, p. 40.

Deze situatie kan een bedreiging vormen voor de persoonlijke levenssfeer. De volgende zaken zijn kenmerkend voor computer matching:

- computer matching heeft betrekking op een op voorhand in beginsel onbepaalde (onbekende) groep of categorie van personen;
- bij computer matching zijn in de regel twee of meer gegevensbestanden betrokken;
- de toetsing vindt plaats naar aanleiding van een bepaalde vooronderstelling of een bepaald kenmerk;
- het doel ligt dichterbij signaleren en bestraffen dan bij voorkomen en afschrikken;
- personen die bij computer matching zijn betrokken, zijn daarvan vaak niet op de hoogte.

### **Computerprofiling**

Bij computerprofiling (ook wel ‘computer screening’ genoemd) kunnen twee fases worden onderscheiden. In de eerste fase wordt in een of meer geautomatiseerde gegevensbestanden gezocht naar een bepaalde combinatie van veelal complexe en gefragmenteerde gegevens-elementen, die in samenhang met elkaar een profiel vormen. Door gebruik te maken van inductieve logica kunnen karakteristieken en/of gedragspatronen worden vastgesteld die kenmerkend zijn voor het vertonen van bepaald gedrag<sup>13</sup>, op basis waarvan een profiel kan worden samengesteld. Profilering kan vooral goede diensten bewijzen bij strafbare gedragingen waarop normaal gesproken moeilijk grip is te verkrijgen. In de tweede fase wordt in grote databestanden gezocht naar (groepen van) personen, die aan het eerder gevonden profiel voldoen. Een voorbeeld daarvan is de daarop geënte methode van Rasterfahndung, waarvan de Duitse politie en veiligheidsdiensten destijds gebruik maakten voor het opsporen van RAF-terroristen. Met behulp van een combinatie van bepaalde bekende gegevens-elementen die samen een profiel opleverden van (mogelijke) RAF-terroristen, werden allerhande bestanden doorzocht op personen die aan dat profiel voldeden. Er is discussie mogelijk over de vraag of de bovengenoemde fasen beide als computerprofiling moeten worden aangemerkt, of dat computerprofiling slechts betrekking heeft op de tweede fase.

Het doel van de profilering, de aard en de bron van de informatie die wordt gebruikt, de rechten van het individu en de betrouwbaarheid van de profielschets zijn alle factoren die bijdragen aan een juiste toepassing van profiling<sup>14</sup> en, daarmee samenhangende, gedurende het gehele dataminingsproces een belangrijke rol vervullen.

---

13. U.S. Congress, Office of Technology Assessment 1986, p. 87.

14. Zie ook Clarke en U.S. Congress, Office of Technology Assessment 1986, p. 95.

1. Met betrekking tot het doel kan worden gesteld dat profilering met een specifiek doel minder bezwaarlijk is dan met een algemeen doel. Een meer gericht onderzoek rechtvaardigt namelijk een ingrijpender aanpak. Toepassing van een middel waarmee een ernstige inbreuk op de rechten van het individu kan worden gemaakt zonder dat daartoe aanleiding bestaat – bijvoorbeeld in het kader van een ongericht (data-mining)onderzoek – is ongewenst. In het verlengde daarvan is het van belang of het onderzoek (het profiel) betrekking heeft op één individu of op een bepaalde groep van personen. Voor wat betreft de aard van de gegevens die deel uitmaken van het te gebruiken profiel is het van belang, dat gevoelige informatie als bijvoorbeeld ras of religie<sup>15</sup> buiten beschouwing wordt gelaten. Daarnaast moet het gebruik van de informatie, als toegevoegde waarde, noodzakelijk zijn voor het onderzoek.<sup>16</sup>
2. Met het oog op de persoonlijke levenssfeer dient duidelijkheid te bestaan over de rechten van het, aan een profilering onderworpen, individu. Daarbij gaat het onder meer om de vraag in welk geval hij of zij daarover dient te worden geïnformeerd en, zo ja, op welke wijze men daarvan kennis moet kunnen nemen.
3. Ten slotte moet uiterste zorgvuldigheid worden betracht bij het opstellen van een profielschets; dit in verband met de inbreuk op de privacy die met een profilering gepaard kan gaan. Deze bezigheid, welke noodzakelijkerwijs aan de profilering voorafgaat, vormt immers het uitgangspunt van het onderzoek. Het profiel dient voldoende nauwkeurig te zijn om een eventuele inbreuk op de rechten van een individu te kunnen rechtvaardigen. Regulering van de wijze waarop de profilering plaatsvindt is dan ook wenselijk. Het hanteren van een standaardmethode<sup>17</sup>, waarbij wordt voorzien in afdoende waarborgen ter bescherming van het individu, kan bijdragen aan de acceptatie van een ruimer gebruik van deze koppelingsvariant.

De volgende eigenschappen zijn karakteristiek voor computerprofilering:

- computerprofilering heeft in beginsel betrekking op een onbepaalde groep van personen;
- het uitgangspunt is een specifieke combinatie van gegevenselementen, die tezamen het profiel vormen van een groep of persoon;
- profilering kan betrekking hebben op één of meer gegevensverzamelingen;
- personen die deel uitmaken van profilering zijn daarvan vaak niet op de hoogte.

---

15. Zie ook art. 5 WPoI.

16. De voorwaarde van noodzakelijkheid treffen we ook veelvuldig aan in de wet- en regelgeving met betrekking tot de politieregisters.

17. Standaardisering van bijvoorbeeld voorwaarden /reglementen en gebruikte programmatuur.

Ook de toepassing van profiling kan een gevaar opleveren voor de persoonlijke levenssfeer. Aangezien het in beginsel om onverdachte burgers gaat, dient zeer omzichtig te worden omgegaan met het gebruik van profiling. Behalve dat de personen die het onderwerp van profiling vormen daarvan over het algemeen niet steeds op de hoogte zijn, kan profiling leiden tot een, ongefundeerde, andere behandeling van geselecteerde dan van niet geselecteerde personen. Wanneer gegevens worden vergeleken van en kennis wordt vergaard over personen ten aanzien waarvan geen feiten of omstandigheden bekend zijn dat zij zich bezig houden met strafbare feiten, is er sprake van een ingrijpende bevoegdheid. Dit standpunt wordt ook verdedigd in de Nota WES. Deze Nota duidt het bevragen van een op voorhand onbepaalde groep van personen aan als datamining en geeft aan, dat bij deze vorm van bevragen (bijvoorbeeld door middel van profiling) vergaande beperkingen aan het zoeken moeten worden gesteld. Daarbij wordt de mogelijkheid opengelaten om ingeval van zeer ernstige zaken (bijvoorbeeld de georganiseerde criminaliteit) volgens passende procedures omvangrijke bestanden te bevragen en te koppelen, zelfs wanneer deze zijn aangelegd voor geheel andere doeleinden<sup>18</sup>. Bij het zoeken naar een balans tussen de rechten van het individu en het belang van de overheid kan het doelbindingsbeginsel ook bij het gebruiken van profielen een positieve rol vervullen.

#### **Integratie van bestanden**

De vierde koppelingsvariant betreft het integreren van bestanden. Er is sprake van integratie indien een koppeling van gegevensbestanden leidt tot het ontstaan van een nieuw bestand. Daarbij is het mogelijk dat de bronbestanden ophouden te bestaan. Integratie kan bijvoorbeeld worden toegepast op de overkoepelende politieregisters die dienen ter ondersteuning van de algemene politietaak, de zogenaamde bedrijfsprocessensystemen (BPS). In tegenstelling tot de overige drie koppelingsvormen heeft integratie enkel betrekking op de wijze, waarop de gegevensbestanden worden gekoppeld. Gegevensbestanden met verschillende verstrekkingenregimes kunnen in bepaalde gevallen een integratie in de weg staan. Integratie kenmerkt zich door de volgende eigenschappen:

- integratie is niet gerelateerd aan een bepaalde vorm van bevragen en kan plaatsvinden voor uiteenlopende doeleinden;
- bij integratie zijn twee of meer (delen van) bestaande gegevensbestanden betrokken;
- omdat bestaande gegevensbestanden worden samengevoegd, moet rekening worden gehouden met de voor die bestanden afzonderlijk geldende privacywaarborgen.

#### **6.2 De wettelijke koppelingsregeling**

In art. 6 WPoI wordt voorzien in de mogelijkheid van koppeling. Deze regeling is verder uitgewerkt in de art. 4 en 5 BPoI. In art. 1 lid 1 sub *d* WPoI wordt een definitie gegeven

---

18. *Kamerstukken II, 1997/98, 25 880, nrs. 1-2, p. 83.*

aan de koppeling van art. 6 WPolr. Een zodanige koppeling doet zich voor wanneer er sprake is van:

*‘het treffen van technische of organisatorische voorzieningen, waardoor verschillende verzamelingen van persoonsgegevens systematisch met elkaar kunnen worden vergeleken’.*

De wetgever heeft ervoor gekozen om, vanuit juridisch perspectief, slechts in een beperkt aantal situaties van een koppeling te spreken. Het oogmerk van een koppeling is in de regel het verkrijgen van nieuwe informatie over een in beginsel onbepaalde groep van personen, welke informatie niet kan worden ontleend aan één van de betrokken registers afzonderlijk.<sup>19</sup> Dit betekent dat een onderzoek, waarbij uit verschillende registers gegevens worden verzameld ter verkrijging van nieuwe informatie omtrent een bepaalde persoon of groep van personen, geen koppeling is als bedoeld in art. 6 WPolr.<sup>20</sup> Er wordt wel verstrekt, maar die verstrekking betreft geen koppeling. Volgens de MvA is de juiste juridische term in die gevallen ‘raadpleging’. Over de strekking van het juridische koppelingsbegrip kan onduidelijkheid ontstaan. Zo is het, wanneer men over een koppeling spreekt, niet steeds helder of daarmee wordt gerefereerd aan de bestaande koppelingsregeling in de WPolr en het BPolr of dat het gaat om koppeling in de algemene betekenis van het woord. Hoewel juridisch onjuist, worden tal van termen als synoniemen voor koppeling gehanteerd. Daarnaast zijn de voor de regeling van art. 6 WPolr kenmerkende voorwaarden niet op alle punten even duidelijk. Het effect daarvan wordt nog versterkt doordat de koppelingsregeling noch in de wet, noch in de praktijk echt is uitgewerkt.

### 6.2.1 Koppeling en registervergelijking

Het rapport van de commissie Mevis handelt over nieuwe bevoegdheden tot het voordere van gegevens ten behoeve van strafvorderlijk onderzoek. Daarin wordt een aantal methoden voor het bewerken van gegevens beschreven, waarbij geen onderscheid wordt gemaakt tussen de inhoudelijke betekenis van de termen ‘koppeling’ en ‘registervergelijking’.

*‘Onder registervergelijking verstaat de commissie het genereren van nieuwe gegevens door het koppelen of vergelijken van registers. Bij het koppelen of vergelijken van registers worden de gegevens uit het ene register als het ware gelegd naast de gegevens uit het andere register. Op die manier kunnen gegevens worden vergeleken of aangevuld, waardoor nieuwe informatie ontstaat’.*

19. Kamerstukken II, 1988 /89, 19 589, nr. 3, p. 16.

20. Kamerstukken II, 1988 /89, 19 589, nr. 6, p. 10.

Wanneer de commissie spreekt over koppeling wordt de wettelijke koppelingsregeling als uitgangspunt gehanteerd. Dit blijkt uit een verwijzing naar de WPolr en het BPolr:

*‘Voor de koppeling van registers van derden met politieregisters is een voorziening getroffen in de Wet politieregisters en het Besluit politieregisters (respectievelijk artikel 6 Wet politieregisters en artikelen 4 en 5 Besluit politieregisters)’.*

Door geen onderscheid te maken tussen het koppelen van registers en het vergelijken van registers komt de commissie tot de constatering, dat koppeling een bewerkingsmethode is.<sup>21</sup> In dat verband verstaat men onder bewerken het verkrijgen van nieuwe gegevens door een analyse, een vergelijking of een combinatie van verschillende gegevens of verschillende verzamelingen van gegevens. De nieuwe gegevens ontstaan door de bewerking en zijn zonder die bewerking niet beschikbaar. Daarvoor zal eerst nog een tweede handeling verricht moeten worden, namelijk een vergelijking. De juridische definitie van koppelen impliceert niet een zodanige vergelijking. Om met de commissie Mevis te spreken: er dient hier een onderscheid te worden gemaakt tussen bewerken en selecteren. Een koppeling in de zin van art. 6 WPolr ziet uitsluitend op het selecteren van gegevens. Volgens art. 1 onder *d* WPolr ziet koppelen op het treffen van technische of organisatorische voorzieningen, waardoor verschillende verzamelingen van persoonsgegevens systematisch met elkaar *kunnen* worden vergeleken. Hier is het koppelen een voorbereidingshandeling, voorafgaande aan een vergelijking of een bewerking; deze impliceert geen vergelijking in de zin zoals bedoeld door de commissie.

Koppeling in het kader van het dataminingonderzoek vindt aansluiting op de juridische definitie van koppelen in de WPolr. In beginsel wordt voor elk dataminingonderzoek een datawarehouse aangelegd. Het datawarehouse kan het resultaat zijn van de koppeling. Pas na bewerking van de gegevens in het datawarehouse is het dataminingonderzoek voltooid. De bewerking vormt dus een afzonderlijke fase van het dataminingsproces.

### *6.2.2 Onderscheid tussen bepaald en onbepaald*

Om te kunnen spreken van een koppeling in juridische zin dient er sprake te zijn van een op voorhand onbepaalde groep van personen omtrent welke, als resultaat van een vergelijking, gegevens kunnen worden verkregen. De begrippen ‘bepaald’ en ‘onbepaald’ hebben vanuit juridisch perspectief een andere betekenis dan die in het maatschappelijk verkeer. Daardoor is niet in alle gevallen duidelijk, wanneer bij onderzoek sprake is van een onbepaalde groep van personen. Die duidelijkheid is echter wel een noodzakelijke voorwaarde voor het uitvoeren van een koppeling in juridische zin. In het hierna volgende wordt de juridische betekenis gespecificeerd van de begrippen ‘bepaald’ en ‘onbepaald’.

---

21. Commissie Mevis 2001, p. 29, 31 en 33.

### Het ‘onbepaalde’ bepaald

Ter verduidelijking wordt gebruik gemaakt van een voorbeeld. In het kader van een onderzoek naar de verspreiding van kinderporno bestaan aanwijzingen, dat een bepaalde chatbox op internet wordt gebruikt voor de uitwisseling van kinderporno. Bij aanvang van het onderzoek is het uitgangspunt dus de verspreiding van kinderporno. In het kader van dat onderzoek komen personen in beeld, die de betreffende chatbox bezoeken. Deze groep van personen is onbepaald. De omvang en samenstelling van die groep kan, met name wanneer het een vrij toegankelijke chatbox betreft, enorm variëren. Naarmate het onderzoek vordert zal de groep van personen waarop het onderzoek zich richt kleiner worden. Personen die de chatbox een enkele maal bezoeken en niet meer terugkomen kunnen afvallen. Frequente bezoekers, die bovendien op grote schaal bestanden uitwisselen of eigen servers draaien, kunnen in aanmerking worden gebracht voor nader onderzoek. Op dat moment behoeft echter geenszins sprake te zijn van een verdenking tegen één of meer personen, ook niet wanneer die personen identificeerbaar zijn. Identificeerbaarheid in juridische zin impliceert geenszins dat één of meer van de betreffende personen zich daadwerkelijk schuldig hebben gemaakt aan strafbare gedragingen en maakt de groep derhalve in juridische zin nog niet bepaald van aard. Dat wordt pas duidelijk nadat nader onderzoek heeft plaatsgevonden waaruit een verdenking voortvloeit. Juridisch gezien richt het onderzoek zich derhalve nog steeds op een onbepaalde groep van personen en de behoefte aan nadere informatie (door toepassing van dataminingonderzoek) is nog steeds aanwezig. Ook een groep personen die naar maatschappelijke maatstaven als ‘bepaald’ kan worden omschreven, kan vanuit juridisch oogpunt dus onbepaald zijn. Bij een onderzoek waaraan een strafbare gedraging ten grondslag ligt wordt gestreefd naar het verkrijgen van één of meerdere namen van personen die in verband kunnen worden gebracht met die gedraging. Pas op het moment waarop een onderzoek een verdenking oplevert jegens één of meer personen wordt gesproken van een ‘bepaald persoon’ of een ‘bepaalde groep van personen’. Er is geen behoefte meer aan aanvullende informatie en het zwaartepunt van het onderzoek verschuift naar een controle van het gevonden resultaat (te weten de bepaalde persoon of groep van personen). De focus van onderzoek is niet langer gelegen in de verspreiding van kinderporno maar op de verspreiding van kinderporno door persoon X. Bepaling van één persoon (en niet een groep van personen) is noodzakelijk gezien het individuele karakter van het Nederlandse strafrecht. In het kader van het dataminingonderzoek bestaat geen onduidelijkheid over de status van het onderzoek wanneer het gaat om het bevragen van bestanden op één enkel persoon. In die fase van het onderzoek is niet langer sprake van koppeling, maar van verificatie.

Samengevat is vanuit juridisch perspectief sprake van een onbepaalde groep van personen wanneer behoefte bestaat aan nadere informatie. Daarbij staat van tevoren niet vast, over welke personen<sup>22</sup> informatie wordt verkregen. Het omslagpunt tussen bepaald en

---

22. Het kan niet gaan om één enkel persoon.

onbepaald wordt gevormd door de mate van verdenking. Wanneer geen behoefte (meer) bestaat aan aanvullende informatie wordt gesproken van een bepaalde groep van personen. De bevraging die daarna plaatsvindt heeft als doel de controle van het eerder gevonden resultaat, waarbij geen sprake meer is van koppeling maar van verificatie.

### *6.2.3 Kenmerken van juridische koppeling*

Gelet op het voorgaande kunnen vier kenmerken worden genoemd, aan de hand waarvan kan worden vastgesteld of er sprake is van een koppeling als bedoeld in art. 6 WPolr.

1. Het resultaat van de koppeling kan niet aan één van de betrokken gegevensverzamelingen afzonderlijk worden ontleend.
2. Op voorhand staat niet vast omtrent wie, als gevolg van de verwerking in het kader waarvan de koppeling plaatsvindt, (de gezochte) informatie wordt verkregen.
3. De koppeling voorziet in een behoefte aan nadere informatie.
4. Koppeling in het kader van een onderzoek met betrekking tot één enkele persoon is uitgesloten.

## **6.3 Verhouding van juridische koppeling volgens Wpolr tot de koppelingsvormen**

Nu duidelijkheid bestaat over de reikwijdte van de juridische koppeling zoals door de wetgever bedoeld bij de totstandkoming van de WPolr, kan worden onderzocht hoe deze zich verhoudt tot de vier in de literatuur onderscheiden koppelingsvormen: verificatie, computer matching, computerprofiling en integratie.<sup>23</sup>

### **Verificatie**

Verificatie van bestanden ziet op het uitwisselen van gegevens over een bepaalde persoon of groep van personen die bekend zijn onder naam of nummer. Wanneer een zodanig verband bestaat tussen verschillende gegevensbestanden dat persoonsgegevens uit het ene bestand 'geverifieerd' kunnen worden aan de hand van gegevens uit het andere bestand, is er geen sprake van een koppeling in de zin van art. 6 WPolr. Er wordt niet voldaan aan de eis van de wetgever, dat er sprake dient te zijn van een op voorhand onbepaalde groep van personen.

### **Computer matching**

Bij computer matching vindt een vergelijking plaats van twee of meer gegevensverzamelingen, teneinde tot dan toe onbekende personen aan de hand van bepaalde kenmerken of vooronderstellingen op te kunnen sporen. Hierbij wordt voldaan aan de voorwaarde van koppeling in art. 6 WPolr, dat er sprake dient te zijn van een op voorhand onbe-

---

23. Zie sectie 6.1.

paalde groep van personen omtrent welke, als resultaat van de vergelijking, gegevens kunnen worden verkregen. Evenals bij de koppeling van art. 6 WPoI is hier sprake van het zogenaamde ‘matchen’ van registraties<sup>24</sup> of het koppelen in enge zin. Bij computer matching kan dus zowel in de algemene als in de juridische betekenis van het woord van koppeling worden gesproken.

### **Computerprofiling**

Computerprofiling vertoont sterke overeenkomsten met computer matching. In beide gevallen wordt gestreefd naar het verkrijgen van informatie over een in beginsel onbepaalde groep van personen. Het verschil is dat bij computerprofiling wordt gezocht naar aanleiding van een bepaalde veronderstelling (of bepaalde kenmerken), terwijl bij computerprofiling een bepaald profiel als uitgangspunt wordt genomen. Computerprofiling past in beginsel binnen de wettelijke definiëring van het begrip ‘koppeling’. Computerprofiling kan evenwel ook worden toegepast op één enkel register, in welk geval van een koppeling in de zin van art. 6 WPoI geen sprake is.<sup>25</sup>

### **Integratie**

Van integratie is sprake wanneer een koppeling van gegevensbestanden leidt tot het ontstaan van een nieuw bestand. Integratie kan ook in de juridische zin van het woord als koppeling worden aangeduid. De aanleg van een apart register kan namelijk worden aangemerkt als het treffen van een technische of organisatorische voorziening, waardoor verschillende verzamelingen van persoonsgegevens systematisch met elkaar kunnen worden vergeleken. Wil in het geval van integratie evenwel inderdaad sprake zijn van een koppeling in juridische zin dan is het noodzakelijk, dat de bevraging in het kader waarvan de integratie plaatsvindt betrekking heeft op een op voorhand onbepaalde groep van personen.

### **Resumerend**

Wanneer de in de literatuur beschreven koppelingsvormen van computer matching, computerprofiling en integratie worden afgezet tegen de juridische definitie van koppeling blijkt, dat deze drie vormen in principe voldoen aan de in die definitie genoemde voorwaarden. Uitzondering daarop wordt gevormd door computerprofiling met betrekking tot één gegevensverzameling. Bij verificatie is sprake van een op voorhand bekende persoon of groep van personen. Vanuit juridisch oogpunt gezien kan deze bewerking derhalve niet als een koppeling worden aangemerkt. De aard van de verificatie zoals beschreven in de literatuur komt in beginsel overeen met die, welke plaatsvindt in het kader van het dataminingsproces. In dat proces wordt bewust onderscheid gemaakt tussen koppe-

---

24. Zie Schreuders 2001, p. 27 en Tekst en commentaar WPoI, p. 29.

25. Bij een koppeling zijn twee of meer gegevensbestanden betrokken.

ling en verificatie. Een juridische koppeling vindt plaats in het kader van een data-miningonderzoek; in de fase van verificatie is het onderzoek beëindigd en daar is dus geen sprake meer van koppeling.

Het aanmerken van een aantal van de in de literatuur onderscheiden koppelvormen als koppelingen in juridische zin betekent niet, dat deze daarmee volledig kunnen worden gelijkgeschakeld. De wetgever ziet het koppelen van gegevens als een voorbereidende handeling, voorafgaande aan de bewerking (analyse) van de gekoppelde gegevens. De koppeling houdt enkel het samenvoegen van bestanden in. De bewerking die vervolgens plaatsvindt is niet geregeld door art. 6 WPolr, aangezien deze wordt beschouwd als een techniekafhankelijke benadering van de materie waarbij de wijze van bewerken niet van invloed is op de koppeling. Dit in tegenstelling tot de benadering van het begrip koppeling in de literatuur zijnde een combinatie van koppelen en bewerken. Ergo, drie van de vier koppelvormen zijn niet per definitie kenmerkend voor een bepaalde manier van koppelen, maar voor een koppeling in combinatie met een bepaalde bewerking. Bij de integratie ligt de nadruk wel op de koppelvorm, namelijk op het samenvoegen van twee of meer bestanden tot een nieuw bestand. Integratie is niet gerelateerd aan een bepaalde vorm van bevragen en het doel ervan vormt in beginsel geen issue. In die zin sluit integratie het nauwst aan bij de juridische koppeling.

Gelet op het voorgaande kunnen de koppelvormen van computer matching, computerprofilering en integratie met name worden aangemerkt als beschrijvingen van toepassingsmogelijkheden van de juridische koppeling. Het in de literatuur gemaakte onderscheid naar vier koppelvormen is enigszins misleidend, omdat ieder van deze afzonderlijk geen voor die vorm kenmerkende toepassingsmogelijkheden bevatten. Daaruit kunnen situaties ontstaan waarin verschillende koppelvormen, al naar gelang het gewenste resultaat, worden gecombineerd. Dankzij het techniekafhankelijke karakter van de juridische koppelingsregeling zal niet direct behoefte ontstaan aan verbetering van de reikwijdte van die regeling. De wijze evenwel waarop de juridische koppeling zich verhoudt tot de in de literatuur onderscheiden koppelvormen levert specifieke aanrijpingspunten op voor juridische regulering van het koppelen zelf. In die zin is de bestaande koppelingsregeling van art. 6 WPolr in de volgende sectie onderwerp van kritische beschouwing.

#### **6.4 Bewustwording en verduidelijking**

Tijdens de totstandkoming van de WPolr noodzaakte de stand van de techniek nog niet tot een uitgebreide en duidelijke regeling voor het koppelen van gegevens(bestanden). Uit de kamerstukken bij de totstandkoming van de WPolr blijkt dat op dat moment het koppelen zoals bedoeld in de WPolr weliswaar nog niet plaatsvond, maar dat in de toekomst behoefte zou kunnen ontstaan aan koppeling bij de opsporing van veel voorkomende of van ernstige delicten, bijvoorbeeld in verband met het opstellen van een mis-

daadanalyse. Sinds de totstandkoming van de WPolr hebben zich grote veranderingen voorgedaan op het gebied van de toepassing(smogelijkheden) van koppeling. Aangezien het thans technisch mogelijk is om gegevens (verzamelings) op vrijwel iedere denkbare wijze te koppelen, lijkt de hedendaagse opsporingspraktijk te worstelen met vooral ontoereikende en onduidelijke wet- en regelgeving op dit punt.

### **Belang van een duidelijke regeling**

Tot op heden (2005) ontbreekt het aan een duidelijke wettelijke regeling omtrent het koppelen van gegevens(bestanden) in het kader van de opsporing. De bestaande koppelingsregeling in de WPolr en het BPolr biedt onvoldoende houvast aan de praktische toepassing van koppeling. De algemene regels over het verenigbare gebruik bieden hier geen uitkomst. Zoals gebleken in de voorgaande paragrafen wordt op verschillende manieren uitleg gegeven aan het begrip koppeling. Doordat de juridische betekenis van de term 'koppeling' afwijkt van de betekenis die daaraan in de literatuur en het dagelijks taalgebruik wordt gehecht, kan onduidelijkheid ontstaan. Het brede toepassingsbereik van de bestaande koppelingsregeling van art. 6 WPolr blijkt onder meer uit de constatering dat, op één na, alle in de literatuur onderscheiden koppelingsvormen als een koppeling in juridische zin kunnen worden beschouwd, terwijl het begrip 'koppelen' in feite in ruimere zin wordt gehanteerd; de WPolr ziet immers enkel op het koppelen van gegevens en niet op het bewerken van de gekoppelde gegevens.

Het werken met een technisch achterhaalde koppelingsregeling die dateert uit een tijd waarin het daadwerkelijk en op grote schaal toepassen van koppeling nog toekomstmuziek was, heeft nadelige gevolgen voor de opsporingspraktijk. Het ontbreken van bijvoorbeeld een duidelijke regeling van de bevoegdheden in het kader van voor het koppelen van bestanden kan misbruik in de hand werken. Daarbij kan worden gedacht aan koppeling van gegevens(bestanden) zonder dat daarbij rekening wordt gehouden met de voorwaarden die de WPolr en het BPolr daaraan stellen. Dergelijke ingrijpende handelingen dienen te worden gereguleerd in duidelijk omschreven en begrensde bevoegdheden. Daarmee wordt niet alleen de bescherming van de rechten van de burger gewaarborgd, maar wordt tevens zekerheid verschaft over de positie van zowel de burger als de overheid. Voorts leiden de ontwikkelingen in de informatietechnologie tot verruimde mogelijkheden tot het koppelen van bestanden, hetgeen een reële bedreiging vormt voor de persoonlijke levenssfeer van de burger. In het rapport van de commissie 'Grondrechten in het digitale tijdperk' wordt vastgesteld, dat het koppelen van bestanden één van de belangrijkste knelpunten is met betrekking tot de grondrechten in het digitale tijdperk.<sup>26</sup> Het ligt dus voor de hand dat wordt voorzien in een regeling voor het koppelen van

26. *Rapport van de Commissie Grondrechten in het digitale tijdperk* 2000, p. 281.

bestanden, die duidelijkheid biedt aangaande bevoegdheden en handelingen op dat terrein en daarmee afdoende waarborgen levert voor de bescherming van de privacy.

Een duidelijke regeling kan voor (bijvoorbeeld) de opsporing leiden tot een efficiënt en veelvuldig gebruik van de mogelijkheden van koppeling. Door een onduidelijke regeling kunnen opsporingsinstanties zich terughoudend opstellen ten aanzien van het toepassen van koppeling. Men is zich onvoldoende bewust van de mogelijkheden van koppeling, of is bang in strijd te handelen met de bestaande wet- en regelgeving. Daardoor is het gevaar van in een vicieuze cirkel te geraken niet denkbeeldig: doordat om bovengenoemde redenen nauwelijks koppeling plaatsvindt lijkt in de dagelijkse opsporingspraktijk (nog) geen noodzaak te bestaan tot een herziening (verduidelijking) van de bestaande wettelijke regeling. De commissie Mevis constateert in dit verband, dat tot op de dag van vandaag nauwelijks gebruik lijkt te zijn gemaakt van de bevoegdheid van art. 6 WPolr.<sup>27</sup> De commissie zegt in de praktijk slechts enkele toepassingen van koppeling in het kader van strafvorderlijke gegevensvergaring te zijn tegengekomen.<sup>28</sup> Dit wordt onder meer toegeschreven aan de onduidelijkheid over de exacte definiëring van het begrip koppeling en het ontbreken van voldoende wettelijke uitvoeringsmogelijkheden, waardoor tegen problemen wordt aangelopen als definitiekwesties en verschillen in dataopslag die de feitelijke mogelijkheden van registervergelijking beperken.

### Wbp

De reden waarom in de Wbp niet is voorzien in een duidelijke regeling aangaande de koppeling is gelegen in de veronderstelling, dat het in de praktijk niet om een éénzijdig begrip zou gaan.<sup>29</sup> De ontwikkelingen in de informatietechnologie leiden tot verruiming van de mogelijkheden tot koppeling en van de maatschappelijke acceptatie daarvan. Om die redenen is niet gekozen voor voorstellen voor of handhaving van strikte bepalingen op dit punt. Daar waar koppeling tot vergaande consequenties dreigt te leiden bestaat volgens de wetgever de mogelijkheid om aan de norm van het verenigbare gebruik, op een op de desbetreffende sector toegespitste wijze, invulling te geven via een jurisprudentiële concretisering of een nadere uitwerking in bijvoorbeeld gedragscodes. Er wordt dus volstaan met het standpunt, dat de algemene regels over het verenigbare gebruik van toepassing zijn op gegevensverwerkingen die als koppeling worden aangemerkt. Daarmee lijkt te worden berust in de huidige regeling omtrent koppeling in de WPolr en het BPolr.

In de MvT bij de Wbp wordt het standpunt herhaald, dat bij een koppeling steeds dient te worden nagegaan of de daarmee gepaard gaande inbreuk op de persoonlijke levens-

---

27. Schreuders & Van Kralingen 1998, p. 5. 'In het kader van de Wet en het Besluit politieregisters is dit juridische begrip koppeling nooit uit de verf gekomen'.

28. Commissie Mevis 2001, p. 31.

29. *Kamerstukken II*, 1997/198, 25 892, nr. 3, p. 93-94.

sfeer wordt gerechtvaardigd door het doel waartoe er wordt gekoppeld. Wanneer wordt gekoppeld voor een doel dat relatief ver verwijderd ligt van het doel waarvoor de gegevens zijn vergaard, zal er sprake zijn van onverenigbaar gebruik<sup>30</sup>. Met het oog op de normerende werking van de Wbp in deze zal daarmee bij de toepassing van koppeling in de praktijk rekening dienen te worden gehouden.

### Afsluitend

Volgens de wetgever is uitbreiding van de koppelingsregeling niet mogelijk, omdat koppeling geen eenduidig begrip zou zijn. Dit standpunt laat echter de deur open voor verschillende interpretaties van het begrip koppeling. Het hanteren van verschillende definities voor het koppelen van bestanden is nu juist een van de belangrijkste oorzaken van de bestaande onduidelijkheid. Hoewel een koppeling onder verschillende omstandigheden kan plaatsvinden zij erop gewezen dat art. 6 WPolr slechts ziet, en behoeft te zien, op het koppelen zelf en niet op alle denkbare, specifieke bewerkingen waarop koppeling kan worden toegepast. Gestreefd dient te worden naar een techniekonafhankelijke en vooral duidelijke regeling die de knelpunten wegneemt waarmee opsporingsinstanties kunnen worden geconfronteerd en die daarnaast kan voorzien in de huidige en de toekomstige toepassingsvormen van koppeling. Een techniekonafhankelijke benadering, waarbij voor elke koppelingsvorm afzonderlijk een regeling wordt getroffen, is onwenselijk. Naast de beperkte houdbaarheid<sup>31</sup> van een dergelijke oplossing wordt daarmee vooral de onduidelijkheid van een regeling in de hand gewerkt. In de praktijk zal het namelijk lastig zijn om alle koppelingen in een bepaald hokje te plaatsen. Zeker wanneer zich combinaties van koppelingsvormen voordoen kan onduidelijkheid ontstaan over de vraag, om welke koppelingsvorm het gaat en of er sprake is van een koppeling in juridische zin. Nadeel van de techniekonafhankelijke benadering is de onduidelijkheid die daarmee, gezien de voortschrijdende ontwikkelingen op met name het gebied van de elektronica, gepaard kan gaan. Duidelijkheid over het gebruik van koppeling kan worden bereikt door toepassing van de voorgestelde gedragscodes. Ook kan een herformulering van art. 6 WPolr worden overwogen, waarbij dan tegelijkertijd kan worden voorzien in de doelbinding in het geval van een koppeling.

### 6.5 Koppeling en het dataminingsproces

In het hierna volgende komen twee zaken aan bod met betrekking tot het koppelen van bestanden in het kader van het dataminingsproces. Ten eerste wordt aan de orde gesteld het bevragen van bestanden op één bepaald persoon, in welk geval niet van koppelen maar van raadplegen wordt gesproken. Onderzocht is of bij het raadplegen van bestanden op één bepaald persoon nog sprake is van dataminingsonderzoek. Ten tweede wordt

---

30. *Kamerstukken II*, 1997/98, 25 892, nr. 3, p. 94.

31. In verband met de technologische turbulentie.

gekeken naar het onderscheid dat de WPolr en het BPolr maken tussen het verstrekken en het koppelen van gegevens. Onderzocht is hoe deze twee begrippen zich tot elkaar verhouden.

#### *6.5.1 Het bevragen van bestanden op een bepaalde persoon*

In deze sectie draait het om de vraag, of een dataminingonderzoek betrekking kan hebben op een enkel individu. Uit de Nota WES<sup>32</sup> blijkt, dat met betrekking tot wetgeving over het bevragen van bestanden een onderscheid dient te worden gemaakt tussen het bevragen op een bepaalde persoon en het bevragen op een op voorhand onbepaalde groep van personen (datamining)<sup>33</sup>. Het bevragen van bestanden op een enkele persoon wordt niet als datamining aangemerkt. Dit past binnen de beschrijving van wat volgens de regering onder datamining dient te worden verstaan, namelijk het geautomatiseerd doorzoeken van grote gegevensbestanden en het combineren van gegevens die verspreid in bestanden liggen opgeslagen, waarna met behulp van speciale programmatuur in deze gegevens vervolgens wordt gezocht naar anomalieën, trends of bepaalde kenmerken.<sup>34</sup> Bij het bevragen op een individueel persoon vindt geen grootschalige zoektocht plaats, maar wordt gericht naar informatie gezocht of gevraagd. Ook hoeft in beginsel geen verdere bewerking van de verkregen informatie plaats te vinden. Er is sprake van een incidentele bevraging of raadpleging. Wanneer in het kader van een dataminingonderzoek sprake is van een bevraging van bestanden op een bepaalde persoon, wordt gesproken van verificatie.

In sommige gevallen is niet geheel duidelijk of er sprake is van het bevragen van een bestand op een bepaalde persoon. Dit kan het geval zijn bij een verwerking die plaatsvindt in het kader van een register-MOT. Hierbij is in beginsel sprake van het bevragen van bestanden (bijvoorbeeld het register zware criminaliteit) op een bepaalde persoon. Omdat een register-MOT echter niet op één maar op alle verdachte transacties betrekking heeft, is het geen incidentele maar een stelselmatige bevraging. Er is sprake van een op voorhand onbepaalde groep van personen, waarbij niet bekend is ten aanzien van wie van hen de bewerking uiteindelijk een match oplevert. De stelselmatige bevraging in het kader van een register-MOT kan worden aangemerkt als een koppeling, hetgeen inhoudt dat er sprake kan zijn van dataminingonderzoek.

#### **Dataminingonderzoek en verificatie**

Ter verduidelijking volgen hieronder twee voorbeelden van een onderzoek. In het eerste geval is sprake van datamining en in het tweede van verificatie. Het betreft een fictief

---

32. *Kamerstukken II*, 1997/98, 25 880, nrs. 1-2, p. 86.

33. Zie ook sectie 3.3.

34. *Kamerstukken II*, 1997/98, 25 880, nrs. 1-2, p. 30 en 42.

onderzoek naar een inbraak die op 21 december te Enschede werd gepleegd en waarbij getuigen een blauwe auto hebben zien wegrijden. Opsporingsdiensten bevragen vervolgens drie registers die mogelijk informatie bevatten die tot de dader(s) kan leiden.

- Register A: bevat gegevens (antecedenten) over personen die met de politie in aanraking zijn geweest vanwege inbraak of diefstal.
- Register B: bevat gegevens over bekeuringen voor verkeersovertredingen.
- Register C: bevat gegevens over autobezit.

Wanneer er nog geen verdachte is, kan een gericht dataminingonderzoek worden verricht. Met de voorhanden zijnde gegevens kunnen, teneinde tot een verdachte te komen, de drie registers worden bevroegd. In het kader van het dataminingonderzoek kan op een aantal kenmerken worden bevroegd. Zo kan worden gezocht op (1) personen uit de omgeving Enschede die (2) in het bezit zijn van een blauwe auto, (3) eerder in aanraking zijn geweest met de politie in verband met een vergelijkbaar vergrijp en (4) op de dag van de inbraak toevalligerwijs zijn bekeurd/geregistreerd in de omgeving van de plaats delict. Indien een bepaalde persoon op basis van die kenmerken in meer dan één van de registers tegelijkertijd voorkomt, kan dat een aanwijzing zijn voor betrokkenheid bij de inbraak. Wanneer iemand in alle drie registers voorkomt kan zelfs worden gesproken van een sterke aanwijzing/verdenking.

Het is ook mogelijk dat men met betrekking tot de inbraak al een verdachte op het oog heeft. Om deze verdenking te verifiëren kan worden nagegaan of de naam van de verdachte in één of meer van de genoemde registers voorkomt. In dat geval is, ook vanuit juridisch oogpunt, geen sprake meer van dataminingonderzoek, maar van verificatie (de WPoR spreekt op dit punt over raadpleging); er wordt immers op één bepaalde persoon gezocht. De mate van verdenking is in sterke mate bepalend voor de vraag welke registers op welke wijze mogen worden bevroegd.

### Resumerend

Een onderzoek waarbij een bepaalde gedraging centraal staat of dat zich richt op meerdere personen (tegen wie nog geen concrete verdenking bestaat) kan worden aangemerkt als een dataminingonderzoek. Een verwerking van externe gegevens kan daarbij in beginsel worden aangemerkt als een koppeling. Een dataminingonderzoek kan geen betrekking hebben op één enkel persoon. Wanneer een onderzoek uiteindelijk tot een bepaalde naam heeft geleid, zal in beginsel ook een verdenking bestaan tegen deze persoon. Hiervan is enkel sprake wanneer voldoende informatie voorhanden is. Vanaf dat moment verlegt het zwaartepunt van het onderzoek zich van het verzamelen van nieuwe informatie naar het verifiëren van de tot dan toe gevonden informatie. Een zodanige bewerking is geen dataminingonderzoek maar verificatie. Het gebruik van aanvullende gegevens ter verificatie van het gevonden resultaat (de verdenking) wordt aangeduid als raadpleging.

### 6.5.2 Koppeling en verstrekking van gegevens

De koppeling van gegevens is onlosmakelijk verbonden met de verstrekking daarvan. Een verstrekking daarentegen hoeft niet noodzakelijkerwijs een gevolg te zijn van een koppeling. In deze sectie wordt kort ingegaan op een aantal zaken die met de verstrekking van gegevens samenhangen.

Een verstrekking van gegevens is mogelijk in het kader van een koppeling, maar ook in dat van een raadpleging. In het eerste geval zal de verstrekking in beginsel plaatsvinden in het kader van een dataminingonderzoek. Bij een verstrekking in het kader van een raadpleging is dat niet per definitie het geval. Bij een bevraging van een register in het kader van de politietaak kan het gaan om een incidentele bevraging, die vanuit juridisch oogpunt als raadpleging wordt aangeduid. In de regel gaat het daarbij om een bevraging naar aanleiding van een bepaald, bekend gegeven. Deze vindt niet plaats in het kader van het dataminingsproces. Het is ook denkbaar dat in het kader van het dataminingsproces sprake is van een incidentele bevraging op een bepaalde persoon. In dat geval wordt niet gesproken van raadplegen, maar van verificatie. Verificatie heeft geen betrekking op het dataminingonderzoek, maar kan wel worden beschouwd als onderdeel van het dataminingsproces. Schematisch samengevat toont het voorgaande het volgende beeld:

	Bevraging op	Bewerking	Ten behoeve van	
<b>Verstrekken</b>	Onbepaalde groep	Koppelen	Dataminingonderzoek	Dataminingsproces
	Bepaald persoon	Verificatie	Verificatie	
		Raadplegen	Algemene politietaak	

Schema 7 Uitwerking verstrekking

#### Koppelen en verstrekken

Een koppeling brengt per definitie een verstrekking met zich mee. In dat verband lijkt de wetgever uit te gaan van de veronderstelling dat een koppeling van een bepaald register per definitie gepaard gaat met een verstrekking van gegevens uit dat register.<sup>35</sup> Bij een koppeling in het kader van een dataminingonderzoek is dat echter niet altijd het geval. Met het oog op de verschillende verstrekkingenregimes die bij een koppeling betrokken kunnen zijn dient te worden vastgesteld van welk register een koppeling in een bepaald geval uitgaat (het basisregister). Zo vormt bij een ongericht dataminingonderzoek ter verbetering van politieregister X, politieregister X het basisregister. Wanneer een koppeling plaatsvindt met politieregister Y kan in het kader van die koppeling een verstrekking

35. Kamerstukken I, 1998/99, 25 398, nr. 63b, p. 8.

van gegevens plaatsvinden. Het gaat daarbij dus om een verstrekking van gegevens uit register Y aan register X. Uit het basisregister X vindt in het geheel geen gegevensverstrekking plaats. Vanuit het standpunt van register X bezien betekent een koppeling niet automatisch een verstrekking van gegevens (uit dat register).

### 6.6 Overzicht koppeling

Ter completering van de uitwerking van de juridische koppeling is met behulp van onderstaand schema aangegeven, hoe de koppeling zich verhoudt tot het dataminingsproces en het proces van informatiegaring.

	Ontdekken		Toetsing
<b>Het proces van informatiegaring</b>	Opbouwen en instandhouden van de informatiepositie	Verken-nend onderzoek	Opsporingsonderzoek
<b>Dataminingsproces</b>	Ongericht dataminingsonderzoek	Gericht dataminingsonderzoek	Verificatie
<b>Juridische koppeling</b>	Ja	Ja	Nee
<b>Koppeling art. 6 WPoI</b>	Onbepaald	Onbepaald	Bepaald
<b>Dagelijks taalgebruik</b>	Onbepaald	Bepaald	

*Schema 8 De relatie tussen de juridische koppeling en de processen van dataminering en informatiegaring*

Uit het model kan worden afgelezen dat ook bij een gericht dataminingsonderzoek, waarbij wordt gezocht naar een bepaalde, op voorhand bekende groep van personen, sprake is van een juridische koppeling. Op dit punt kan de formulering van de huidige koppelingsregeling tot misverstanden leiden. Bij een onderzoek in het kader van art. 126<sup>gg</sup> Sv bijvoorbeeld is bij uitstek sprake van een bekende, zo duidelijk mogelijk omschreven groep van personen. Vanuit de juridische koppeling bezien dient in dit kader echter nog steeds te worden gesproken van een onbepaalde groep van personen. Of een bevroegde groep van personen als bepaald kan worden aangemerkt is afhankelijk van de mate van verdenking, die onder meer kan worden afgelezen uit de positie van het onderzoek binnen het dataminingsproces.

Volledigheidshalve is in het model aangegeven op welk punt, uitgaande van het dagelijks taalgebruik, de vraag kan worden gesteld of er nu sprake is van een onbepaalde of een bepaalde groep van personen. De interpretatie van 'een bepaalde groep van personen' in het dagelijks taalgebruik is ruimer dan die vanuit juridisch oogpunt. In juridische zin is bij een ongericht dataminingsonderzoek in beginsel steeds sprake van een onbepaalde

groep van personen. Een gericht dataminingonderzoek kan zeer wel betrekking hebben op een nader gespecificeerde groep van personen. In het kader van bijvoorbeeld een verkennend onderzoek in de zin van art. 126<sup>gg</sup> Sv, dient de groep van personen op wie het onderzoek betrekking heeft zo nauwkeurig mogelijk te worden omschreven. Desondanks is deze groep van personen vanuit juridisch oogpunt gezien onbepaald. Op het moment van verificatie bevindt het onderzoek zich in de eindfase en zal in beginsel sprake zijn van één of meer bepaalde personen.

### **6.7 Afsluitend**

Vooraf dankzij het techniekonafhankelijke karakter van art. 6 WPolr lijkt de huidige koppelingsregeling te kunnen voorzien in de bestaande en toekomstige toepassingsvarianten van het dataminingsproces. De techniekonafhankelijke formulering van de koppelingsregeling vormt echter tegelijkertijd een obstakel bij de toepassing daarvan. Het ontbreken van een duidelijk afgebakende definitie leidt tot synonymie van termen als registervergelijking, verwerking en bewerking in het kader van de juridische koppeling van art. 6 WPolr. Het is vanuit juridisch oogpunt van belang dat duidelijkheid bestaat over de exacte reikwijdte van de koppelingsregeling. Daarmee kan bijvoorbeeld de vraag worden beantwoord of alleen sprake is van een koppeling indien twee afzonderlijke bestanden worden gekoppeld, of dat ook een gedeeltelijke koppeling van gegevens(bestanden) als een koppeling kan worden aangemerkt. Gestreefd dient te worden naar een techniekonafhankelijke en vooral duidelijke regeling die de knelpunten wegneemt waarmee opsporingsinstanties kunnen worden geconfronteerd. In hoofdstuk 11 van dit onderzoek wordt nader ingegaan op de wijze waarop aan een dergelijk streven uitvoering kan worden gegeven.

---

## 7 Ongericht dataminingonderzoek en de gewone politieregisters

In dit hoofdstuk wordt onderzocht in hoeverre met behulp van ongericht dataminingonderzoek een verbetering van de informatiepositie van de gewone politieregisters kan worden nagestreefd. Daarbij staat de vraag centraal in hoeverre gegevens uit de verschillende aan opsporingsdiensten ter beschikking staande bronnen mogen worden gebruikt in het kader van een ongericht dataminingonderzoek ter verbetering van de informatiepositie van een gewoon politieregister. Om het wettelijke kader waarbinnen aan het dataminingproces uitvoering dient te worden gegeven toegankelijker te maken, worden de verschillende varianten van het dataminingproces toegepast op de bestaande politieregisters; daarbij wordt onderzocht onder welke omstandigheden en voorwaarden die varianten mogen worden gebruikt. Vooraleerst is in de volgende sectie stilgestaan bij de verschillende functies die een politieregister kan vervullen en de invloed hiervan op het dataminingproces.

### 7.1 Functies politieregisters en dataminingonderzoek

Bij een verwerking van gegevens in het kader van een dataminingonderzoek kan het gaan om het verzamelen, verifiëren, vastleggen en het bewerken (analyseren) van gegevens. De WPolr en het BPolr spreken niet over het verwerken van gegevens maar over de registratie en de verstrekking van gegevens in het kader van de politietaak. Alvorens te onderzoeken in hoeverre de informatiepositie van de politieregisters met behulp van dataminingonderzoek kan worden verbeterd, wordt kort stilgestaan bij de wijze waarop de functies van een politieregister zich verhouden tot de mogelijkheid om dataminingonderzoek te doen. Politieregisters kunnen drie belangrijke functies vervullen waarmee wordt voorzien in de bestaande behoeften bij de uitvoering van de politietaak. Het betreft de volgende functies:

- Registratie.
- Analyse.
- Raadpleging.

### **Registratie**

In beginsel biedt elk politieregisters de mogelijkheid om in het kader van de politietaak gegevens op een verantwoorde wijze op te slaan. Naast de algemene bepalingen van art. 4 tot en met 9 WPolr omtrent de registratie van gegevens in een politieregister, bevatten de WPolr en het BPolr specifieke voorwaarden omtrent de vraag welke gegevens, wanneer en voor welke doeleinden mogen worden vastgelegd. De regels die de WPolr en het BPolr stellen omtrent de registratie van gegevens zijn ook van invloed op het dataminingsproces. Een registratie in een register is mogelijk voor het doel van dat register. Een registratie kan daarbij twee uitgangspunten hebben. Ten eerste kan het gaan om een registratie in een register van gegevens die als zelfstandig subject voor registratie in dat register in aanmerking komen. Ten tweede kan het gaan om een registratie van gegevens die weliswaar worden vastgelegd voor het doel van het register maar niet als zelfstandig subject voor een registratie in dat register in aanmerking komen. Hiervan kan sprake zijn wanneer er in het kader van een koppeling (in het kader van een dataminingonderzoek) gegevens worden vastgelegd in het basisregister dat kan worden aangemerkt als het datawarehouse. Deze registratie hangt samen met het doelbindingsbeginsel, het gebruik van de externe gegevens dient noodzakelijk te zijn voor het doel van het dataminingonderzoek.

### **Analyse**

De tweede functie die een politieregister kan vervullen, betreft het analyseren van de opgeslagen gegevens. In dit verband spreken de WPolr en het BPolr bijvoorbeeld over het koppelen van gegevensbestanden. Deze taak kan ook worden gerekend tot de algemene zorgplicht die een beheerder van een register heeft op grond van art. 7 WPolr. Voor bepaalde politieregisters is de functie van analyse slechts een bijzaak terwijl het bij andere, veelal de bijzondere politieregisters, een hoofdzaak betreft. Bij een analyse van een register kan de beheerder zich beperken tot de gegevens die al in dat register aanwezig zijn. Het is echter ook denkbaar dat de beheerder, in het kader van een dataminingonderzoek, gebruik maakt van externe gegevens. Deze externe gegevens worden dan weliswaar verwerkt voor het doel van het register maar komen in beginsel niet in aanmerking voor zelfstandige registratie in dat register.

### **Raadpleging**

Ten derde is het mogelijk dat een politieregister kan worden geraadpleegd ten behoeve van de politietaak. Hierbij kan het gaan om een verstrekking naar aanleiding van een incidentele bevraging maar ook om een verstrekking die plaatsvindt in het kader van een dataminingonderzoek. Met name de gewone politieregisters zijn bestemd voor operationeel gebruik en kunnen in het kader van de politietaak vrij worden geraadpleegd. Wanneer een politieregister de mogelijkheid biedt tot raadplegen, kan dat de mogelijkheid om de gegevens in dat register zelf te analyseren, beperken. De mogelijkheid om een bepaald register te kunnen raadplegen is namelijk inherent verbonden aan de aard van de

gegevens die in dat register mogen worden vastgelegd en het doel waarvoor dit gebeurt. Dit betekent dat alleen de gegevens die als zelfstandig subject in dit register kunnen worden vastgelegd zijn bestemd voor operationeel gebruik. Externe gegevens die in het kader van een analyse van het register in dat register worden vastgelegd dienen daarom niet vrij te kunnen worden geraadpleegd. In de praktijk staat noch de WPolr noch het BPolr hieraan echter in de weg. Omdat het verstrekkingenregime van de WPolr en het BPolr toch gewaarborgd dient te worden, zullen de mogelijkheden van een analyse door middel van bijvoorbeeld dataminingonderzoek beperkt zijn.

### Resumerend

Gewone politieregisters kunnen in beginsel alle drie de besproken functies vervullen. De manier waarop de verschillende functies van een register zich tot elkaar verhouden is uiteindelijk bepalend voor de vraag op welke wijze de gegevens verwerkt kunnen worden. Zonder al te zeer op de volgende hoofdstukken vooruit te lopen zij opgemerkt dat er in het kader van de toepassing van een ongericht dataminingonderzoek een tweedeling kan worden gemaakt tussen een verwerking (registratie) van een gegeven als zelfstandig subject in een register en de verwerking (registratie) die plaatsvindt in het kader van een analyse. In de laatste situatie zal sprake zijn van dataminingonderzoek. Onderstaand is dit onderscheid schematisch weergegeven.

<b>Registratie voor het doel van het register</b>	⇒	<b>Zelfstandige registratie</b>	<b>Operationeel gebruik</b>	<b>Politieregister</b>
---	---	---------------------------------	-----------------------------	------------------------

*Schema 9 Verwerking bestaande uit een zelfstandige registratie dan wel een registratie in het kader van een analyse*

In de volgende sectie wordt nagegaan of het mogelijk is om de informatiepositie van de gewone politieregisters met behulp van een ongericht dataminingonderzoek te verbeteren (analyse). Daarna kan worden onderzocht in hoeverre de verschillende functies elkaar beïnvloeden en welke betekenis de met de functies samenhangende regels hebben voor het dataminingonderzoek.

## 7.2 Toepassing ongericht dataminingonderzoek

Alvorens te kijken naar de mogelijkheden om met behulp van ongericht dataminingonderzoek de gebruikswaarde van de informatie in de gewone politieregisters te vergroten zal worden vastgesteld of de kenmerkende eigenschappen van een ongericht dataminingonderzoek verenigbaar zijn met de aard van de gewone politieregisters.

### Doel

De WPolr en het BPolr reguleren de opslag, de bewerking en het gebruik van gegevens door de politie. De gewone politieregisters worden in beginsel aangelegd in het kader

van de algemene politietaak en niet voor de politietaak in een bepaald geval. Dit blijkt onder meer uit het open verstrekkingenregime dat op de gegevens in deze politieregisters van toepassing is. Voor een verbetering van de informatiepositie van het gewone politieregister heeft het dataminingonderzoek hetzelfde doel als het politieregister waarop het betrekking heeft. Wanneer dat algemeen van aard is, zal dat ook gelden voor het dataminingonderzoek.

#### **Inbreuk privacy**

Een dataminingonderzoek ter verbetering van de informatiepositie van een gewoon politieregister gaat niet per definitie gepaard met een ontoelaatbare inbreuk op de privacy. Wanneer de gegevens die al in een politieregister aanwezig zijn rechtmatig zijn verkregen is een eventuele inbreuk op de persoonlijke levenssfeer bij de verwerking daarvan toelaatbaar, ongeacht de aard van die gegevens en het van toepassing zijnde verstrekkingenregime. Hoewel niet in alle gevallen noodzakelijk, kan ook gebruik worden gemaakt van externe gegevens; ook dat hoeft niet direct te resulteren in een (ontoelaatbare) inbreuk op de privacy.

#### **Tijdelijk of permanent karakter**

Voor het politieregister is niet alleen het verkrijgen, maar vooral ook het handhaven van een goede informatiepositie van belang. De gewone politieregisters worden in beginsel dan ook gekenmerkt door een permanent karakter.<sup>1</sup> Wanneer een dataminingonderzoek betrekking heeft op een gewoon politieregister zal dat onderzoek eveneens een permanent karakter hebben.

#### **Gebruik van externe gegevens**

Een dataminingonderzoek met betrekking tot een gewoon politieregister zal zich voornamelijk richten op de gegevens die al in het register aanwezig zijn. Wanneer gebruik wordt gemaakt van externe gegevens zullen die voornamelijk afkomstig zijn uit een ander politieregister. De behoefte (en de mogelijkheid) aan verwerking van andere gegevens dan die binnen de politieke sfeer zal zich vooral voordoen in het kader van een specifiek onderzoek. In dat geval zal echter sprake zijn van een gericht dataminingonderzoek, dat in beginsel geen betrekking heeft op een gewoon politieregister.

#### **Resumerend**

Een ongericht dataminingonderzoek blijkt goed verenigbaar te zijn met de verwerking van gegevens zoals die plaatsvindt in de gewone politieregisters. Daarom kan worden geconcludeerd dat het mogelijk is om met behulp van een ongericht dataminingonderzoek te streven naar een verbetering van de informatiepositie van een gewoon politie-

---

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

register. In de volgende sectie zal worden onderzocht wat de mogelijkheden zijn van een dergelijk onderzoek.

### 7.3 Vier verschillende onderzoeksmogelijkheden

Afhankelijk van de aard van de te verwerken gegevens kan ongericht dataminingonderzoek met betrekking tot een gewoon politieregister worden uitgevoerd, waarbij:

- geen gebruik wordt gemaakt van externe gegevens;
- gebruik wordt gemaakt van externe gegevens die niet afkomstig zijn uit een politieregister;
- gebruik wordt gemaakt van externe gegevens afkomstig uit een gewoon politieregister;
- gebruik wordt gemaakt van externe gegevens afkomstig uit een bijzonder politieregister.

#### 7.3.1 *Geen gebruik externe gegevens*

Voor een ongericht dataminingonderzoek met betrekking tot een gewoon politieregister waarbij er geen gebruik van externe gegevens wordt gemaakt, bestaan op grond van de huidige wet- en regelgeving in beginsel geen belemmeringen. Het onderzoek dat strekt om de aanwezige gegevens in een gewoon politieregister zo goed mogelijk te benutten, kan worden gerekend tot de algemene zorgplicht van de beheerder van het register.<sup>2</sup>

Voor een verwerking van gegevens in het kader van de politietaak, zoals een dataminingonderzoek, geldt wel een aantal algemene voorwaarden die voortvloeien uit de WPolr en de daarop gebaseerde wet- en regelgeving. Zo mag een politieregister slechts voor een bepaald doel worden aangelegd en alleen voor zover dit noodzakelijk is voor een goede uitvoering van de politietaak.<sup>3</sup> Daarnaast mag een register slechts gegevens bevatten die rechtmatig zijn verkregen en welke noodzakelijk zijn voor het doel van het register.<sup>4</sup> Deze voorwaarden hebben ook gevolgen voor een dataminingonderzoek in het kader waarvan een datawarehouse wordt aangelegd. Het uitvoeren van een ongericht dataminingonderzoek dient noodzakelijk te zijn voor de politietaak en rekening dient te worden gehouden met het doelbindingsbeginsel. Daarnaast is van belang door wie het dataminingonderzoek wordt uitgevoerd.<sup>5</sup> De betekenis van deze voorwaarden worden in het onderstaande belicht.

---

2. Deze vloeit voort uit art. 7 WPolr.

3. Deze uitgangspunten zijn gebaseerd op de wet- en regelgeving die in sectie 4.2 is besproken. Het verwerken van persoonsgegevens dan wel het verwerken van gegevens voor een ander doel dan waarvoor zij zijn vastgelegd dient noodzakelijk te zijn voor de politietaak en te berusten op een wettelijke regeling.

4. Art. 4 WPolr.

5. Zie ook hoofdstuk 5.

### De politietaak

Op grond van de WPolr en het BPolr dient een verwerking van gegevens (en daarmee het verrichten van een dataminingonderzoek), noodzakelijk te zijn voor een goede uitvoering van de politietaak.<sup>6</sup> De politietaak betreft de taak van de politie zoals die is omschreven in art. 2 Politiewet 1993<sup>7</sup>:

*‘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.’*

Tot de politietaak behoren de hulpverlening en de handhaving van de rechtsorde; de laatste valt uiteen in de strafrechtelijke handhaving van de rechtsorde en de handhaving van de openbare orde. De reikwijdte van de politietaak – de vraag of en in hoeverre bepaalde activiteiten en werkzaamheden behoren tot een goede uitvoering van de politietaak – staat in beginsel ter beoordeling van de politie en het bevoegd gezag. Dit onderzoek omvat een studie naar de mogelijkheden van de toepassing van het dataminingsproces ten behoeve van de opsporing.<sup>8</sup> Het dataminingsproces wordt toegepast in het kader van het proces van informatiegaring (opsporing). Een ongericht dataminingonderzoek vindt plaats in het derde stadium van het proces van informatiegaring, te weten het opbouwen en in stand houden van een zekere informatiepositie in het belang van de strafrechtelijke handhaving van de rechtsorde<sup>9</sup>. Dit gebeurt door het opslaan, bewerken, gebruiken en analyseren van gegevens dan wel het vergaren van gegevens door de toepassing van niet-ingrijpende middelen. De toepassing van dergelijke niet-ingrijpende middelen is niet in de wet geregeld omdat daarmee geen ongeoorloofde inbreuk op de privacy wordt gemaakt. Het gebruik ervan moet wel passen binnen en dienen ter uitvoering van de politietaak met betrekking tot de strafrechtelijke handhaving van de rechtsorde.<sup>10</sup> Dit betekent dat burgers gevrijwaard zijn van politieke activiteit indien hun persoon geen aanleiding geeft tot politieke bemoeienis.

Gelet op het voorgaande kan worden gesteld dat het hier bedoelde dataminingonderzoek wordt verricht in het kader van de strafrechtelijke handhaving van de rechtsorde. De strafrechtelijke handhaving van de rechtsorde betreft de daadwerkelijke voorkoming, de opsporing, de beëindiging, de vervolging en berechting van strafbare feiten, alsmede de tenuitvoerlegging van beslissingen van de rechter of het OM in strafzaken. Hieronder

---

6. Zie onder meer art. 4 lid 1 en art. 6 lid 1 WPolr.

7. Art. 1 sub *b* WPolr.

8. Met ‘opsporing’ wordt hier niet alleen bedoeld op het opsporingsonderzoek, maar op het proces van informatiegaring als geheel waarvan het opsporingsonderzoek deel uitmaakt.

9. *Kamerstukken II, 1996/97, 25 403, nr. 3, p. 8.* Zie ook sectie 3.5.

10. *Kamerstukken II, 1996/97, 25 403, nr. 3, p. 8.*

worden alle taken begrepen die de politie onder de verantwoordelijkheid van het OM en daarmee van de MvJ in verband met (mogelijke) strafbare feiten verricht.<sup>11</sup> Dataminingonderzoek kan op een unieke wijze bijdragen aan het verkrijgen en het in stand houden van een goede informatiepositie. Die informatiepositie vormt de basis voor een succesvolle invulling van de opsporingstaak. In dit licht kan worden gezegd dat de toepassing van dataminingonderzoek noodzakelijk is voor een goede uitvoering van de politietaak (voor zover het de strafrechtelijke handhaving van de rechtsorde betreft).

### Verdieping noodzakelijkheidbeginsel

De wetgever gaat in de MvT van de Wet<sup>12</sup> 'Vorderen gegevens telecommunicatie'<sup>13</sup> in op de vraag wanneer is voldaan aan het noodzakelijkheids criterium bij de verwerking van (persoons)gegevens ten behoeve van de opsporing. In het wetsvoorstel gaat het onder meer om de bevoegdheid tot het van de aanbieder van een openbaar telecommunicatienetwerk of een openbare telecommunicatiedienst vorderen van gebruikersgegevens die bijdragen aan het identificeren van een persoon, zoals naam, adres, woonplaats, nummer en soort dienst. De toepassing van de bevoegdheid tot het vorderen van gebruikersgegevens als zodanig zal niet resulteren in het verkrijgen van een min of meer volledig beeld van bepaalde aspecten van iemands leven. De inbreuk op de persoonlijke levenssfeer is daarmee beperkt. Wel zal deze bevoegdheid er veelal toe leiden, dat de gegevens voor een ander doel worden gebruikt dan waartoe zij zijn verwerkt. Om die reden dient een toetsing plaats te vinden met het oog op de afweging van enerzijds het belang van zorgvuldige hantering van persoonsgegevens en anderzijds dat van de opsporing. Op grond van het Databeschermingsverdrag<sup>14</sup> is doelafwijkend gebruik mogelijk indien dat bij wet is voorzien en noodzakelijk is in het belang van het bestrijden van strafbare feiten in een democratische samenleving. Er dient dus te worden voldaan aan het noodzakelijkheids criterium. Bovendien dient de vergaring van gegevens rechtmatig en niet bovenmatig te zijn.<sup>15</sup> Van belang is dat bovenstaande niet alleen geldt voor het vorderen van gebruikersgegevens, maar ook voor het verwerken van (persoons)gegevens voor een ander doel (opsporing) in het algemeen.

De voorwaarde voor verwerking van persoonsgegevens zoals gesteld in het Databeschermingsverdrag lijkt door de wetgever te worden aangescherpt. Hij geeft aan dat het individuele belang van de burger bij bescherming van zijn persoonsgegevens, voor zover het

---

11. Corstens 2002, p. 96-97.

12. Het wetsvoorstel 'Vorderen gegevens telecommunicatie' is inmiddels in werking getreden met de Wet van 18 maart 2004 tot wijziging van het Wetboek van Strafvordering en andere wetten in verband met de aanpassing van de bevoegdheden tot het vorderen van gegevens terzake van telecommunicatie (*Stb.* 2004, 105).

13. *Kamerstukken II*, 2001 /02, 28 059, nr. 5, p. 10.

14. Zie ook hoofdstuk 4.

15. *Kamerstukken II*, 2001 /02, 28 059, nr. 3, p. 5.

gaat om strafbare feiten die geen misdrijven zijn, zwaarder dient te wegen dan het algemene belang van de opsporing, ook al zijn de gegevens op zichzelf niet ingrijpend voor de persoonlijke levenssfeer. Een verwerking van persoonsgegevens, hoe gering ook, lijkt met het oog hierop alleen noodzakelijk bij misdrijven. Opvallend is dat dit uitgangspunt ook wordt gehanteerd met betrekking tot een verkennend onderzoek van art. 126gg Sv.<sup>16</sup> Hoewel een verkennend onderzoek ziet op de bestrijding of vervolging van misdrijven acht de wetgever de voorwaarden waaronder een verkennend onderzoek kan worden uitgevoerd (uit feiten of omstandigheden dienen aanwijzingen voort te vloeien) blijkbaar onvoldoende om een verwerking van persoonsgegevens te rechtvaardigen.<sup>17</sup> Ergo, een verwerking van (persoons)gegevens voor een ander doel is in beginsel alleen noodzakelijk, en daarmee wettelijk toegestaan, wanneer het gaat om misdrijven. Bij een verkennend onderzoek lijkt een verwerking van persoonsgegevens in het geheel niet mogelijk.

Het is de vraag of dit niet een te vergaande beperking is. Een strikte interpretatie betekent dat opsporingsinstanties in de praktijk geen persoonsgegevens mogen verwerken bij overtredingen. Zelfs wanneer een wettelijke grondslag aanwezig is zal een verwerking van persoonsgegevens niet meer mogelijk zijn; daarvoor moet immers, naast een wettelijke grondslag, ook een noodzaak tot die verwerking aanwezig zijn. Daarvan zou dan alleen nog sprake zijn bij misdrijven. Dit standpunt zou de dagelijkse opsporingspraktijk vrijwel onmogelijk maken. De verwerking van persoonsgegevens is noodzakelijk bij de bestrijding van *alle* strafbare feiten. De manier waarop die persoonsgegevens worden verwerkt kan, en dient, echter wel te worden gereguleerd. Daartoe is de wettelijke grondslag ook bedoeld. Als algemene regel kan daarom worden aangehouden dat een verwerking van persoonsgegevens minder bezwaarlijk is wanneer het gaat om misdrijven. Voorts zal een noodzaak tot een verwerking van persoonsgegevens minder snel aanwezig zijn wanneer het gaat om overtredingen.

### Het doelbindingsbeginsel

In sectie 4.2 is ingegaan op de betekenis van de Wbp voor de WPolr. In het verlengde hiervan dient bij een dataminingonderzoek onder meer rekening te worden gehouden met het doelbindingsbeginsel. Dit betekent voor een ongericht dataminingonderzoek dat het doel van dat onderzoek verenigbaar dient te zijn met het (specifieke) doel van het gewone politieregister waarop het onderzoek betrekking heeft.<sup>18</sup> Gezien het streven naar een verbetering van de informatiepositie van het register waarop het onderzoek betrekking heeft zal dat bij een ongericht dataminingonderzoek in beginsel steeds het geval zijn.

---

16. Sietsma 2004.

17. Met betrekking tot de bestrijding van terroristische misdrijven neemt de wetgever een afwijkend standpunt in (*Kamerstukken II*, 2004/05, 30 164, nr. 3, p. 28).

18. Zie ook *Kamerstukken II*, 1997/98, 25 880, nrs. 1-2, p. 83.

### **Uitvoering**

In het geval van een ongericht dataminingonderzoek is het wenselijk dat het onderzoek wordt uitgevoerd door, dan wel onder het gezag van, de beheerder van het politieregister waarop het onderzoek betrekking heeft. Er vindt dan namelijk geen verstrekking plaats van gegevens uit het basisregister, zoals bedoeld in art. 1 lid 1 onder *b* WPolr. Hierdoor kan het basisregister als datawarehouse worden aangemerkt en kan het bestaande verstrekkingenregime worden gehandhaafd. Het reglement van het basisregister blijft van toepassing omdat het dataminingonderzoek ‘binnenshuis’ plaatsvindt.

### **Resumerend**

De WPolr en het BPolr stellen algemene voorwaarden aan de verwerking van gegevens die plaatsvindt bij de uitvoering van de politietaak. Bij het verrichten van een ongericht dataminingonderzoek met betrekking tot een gewoon politieregister dient rekening te worden gehouden met deze voorwaarden en de consequenties daarvan. Een ongericht dataminingonderzoek dient noodzakelijk te zijn voor de vervulling van de politietaak<sup>19</sup>; er dient rekening te worden gehouden met het doelbindingsbeginsel. Het onderzoek dient te worden uitgevoerd door, dan wel onder het gezag van, de beheerder van het basisregister.

#### *7.3.2 Het gebruik van externe, niet uit een politieregister afkomstige gegevens*

In het kader van een ongericht dataminingonderzoek met betrekking tot een gewoon politieregister kan gebruik worden gemaakt van externe gegevens. Dit leidt onder meer tot een verrijking van het resultaat van het onderzoek, wat in positieve zin bijdraagt aan de informatiepositie van het politieregister. Er kunnen twee categorieën externe gegevens worden onderscheiden. De eerste categorie betreft gegevens die al aanwezig zijn in andere politieregisters. In de secties 7.3.3 en 7.3.4 wordt ingegaan op de verwerking daarvan in het kader van een ongericht dataminingonderzoek. De tweede categorie betreft gegevens die afkomstig zijn buiten de politieke sfeer, zoals gegevens in een telefoonboek of op het internet. In deze sectie staat het gebruik van deze categorie externe gegevens centraal.

Bij de verwerking van externe gegevens in het kader van een ongericht dataminingonderzoek dient steeds rekening te worden gehouden met het noodzakelijkheids criterium en de doelbinding. Deze beperkingen gelden vooral voor externe gegevens die tevens persoonsgegevens zijn. Voor een verwerking van die gegevens dient een specifieke wettelijke grondslag te zijn aangezien art. 2 Politiewet 1993 in dat geval niet volstaat. Bovendien lijkt het gebruik van deze gegevens alleen noodzakelijk te zijn bij de bestrijding van misdrijven. Ook bij een verkennend onderzoek is een verwerking van persoonsgegevens in

---

19. Voor zover het de strafrechtelijke handhaving van de rechtsorde betreft.

beginsel uitgesloten.<sup>20</sup> Wanneer de externe gegevens geen persoonsgegevens zijn, volstaat art. 2 Politiewet 1993 in beginsel als wettelijke grondslag voor een verwerking. Ook in dat geval dient het gebruik noodzakelijk te zijn voor de politietaak maar ontbreekt een beperking tot misdrijven. Tevens kunnen deze externe gegevens worden gebruikt in het kader van een verkennend onderzoek. Eén en ander is in onderstaand schema weergegeven.<sup>21</sup>

	Beperking o.g.v.	Noodzakelijkheids criterium	Wettelijke grondslag
<b>Externe persoonsgegevens</b>	Privacy/doelbinding	Art. 4 WPolr, (misdrijven/geen verkennend onderzoek)	Specifieke wettelijke grondslag
<b>Externe gegevens</b>	Doelbinding	Art. 4 WPolr	Art. 2 Politiewet 1993

*Schema 10 Beperkingen die voortvloeien uit het noodzakelijkheids- en het doelbindingsbeginsel*

#### 7.3.2.1 Aard ongericht dataminingonderzoek

Bij een ongericht dataminingonderzoek is in beginsel nog geen sprake van actieve opsporingsactiviteiten. Het onderzoek heeft tot doel een informatiepositie op te bouwen en niet het nemen van strafvorderlijke beslissingen. Een ongericht dataminingonderzoek wordt niet tot de opsporing gerekend. In het stadium van het proces van informatiegaring<sup>22</sup> waarin een ongericht dataminingonderzoek plaatsvindt, dient terughoudend met het gebruik van externe gegevens te worden omgegaan. De mogelijkheid om actief naar externe gegevens te zoeken, is beperkt. Het actief speuren naar en verzamelen van externe gegevens ten behoeve van de algemene informatiepositie van een register, gaat niet goed samen met het passieve karakter van de ongerichte dataminingsvariant. Naarmate het doel van het politieregister dat onderwerp vormt van het ongericht dataminingonderzoek algemener van aard is, is het moeilijker om te bepalen of het gebruik van bepaalde externe gegevens noodzakelijk is voor dat doel. Die noodzaak is echter een minimumvoorwaarde om de gegevens te mogen gebruiken.

Politiële activiteiten zijn alle activiteiten die door de politie worden verricht en gericht zijn op de strafrechtelijke handhaving van de rechtsorde. Onggericht dataminingonderzoek betreft een 'politiële activiteit' en maakt onderdeel uit van de strafrechtelijke handhaving van de rechtsorde.<sup>23</sup> Wanneer een betrokkene daartoe geen aanleiding geeft

20. Zie ook sectie 7.3.1 en *Kamerstukken II*, 2001 /02, 28 059, nr. 5, p. 10.

21. Behalve door onderstaande factoren kan het gebruik van externe gegevens ook worden beperkt door de aard van een ongericht dataminingonderzoek, de koppelingsregeling van art. 6 lid 2 WPolr en de Wbp.

22. Zie sectie 3.6 en Model IV.

23. *Kamerstukken II*, 1996 /97, 25 403, nr. 3, p. 9.

mogen noch zwaardere, noch lichtere opsporingsbevoegdheden waarvoor de grondslag in de politietaak besloten ligt, worden toegepast.<sup>24</sup> Dit beperkt de mogelijkheid van het zoeken naar en het gebruiken van externe gegevens van buiten de politieke sfeer. De beperkingen zijn in beginsel alleen van toepassing op externe gegevens die als persoonsgegevens kunnen worden aangemerkt. Het resultaat van bijvoorbeeld een fenomeenonderzoek, dat niet tot een natuurlijke persoon herleidbaar is, kan in beginsel wel worden gebruikt. Wanneer die gegevens voor een ander doel zijn vastgelegd kan een verwerking ervan worden gerechtvaardigd door art. 2 Politiewet 1993. Hoewel het gebruik van externe gegevens ook dan noodzakelijk dient te zijn ten behoeve van de politietaak<sup>25</sup> is deze noodzakelijkheidseis minder strikt dan wanneer het persoonsgegevens betreft.

### 7.3.2.2 Koppeling

Bij het gebruik van externe gegevens in het kader van een ongericht dataminingonderzoek kan sprake zijn van een koppeling in de zin van art. 6 WPolr. In art. 1 lid 1 sub *d* WPolr wordt gesproken over ‘een vergelijking van verzamelingen van persoonsgegevens’, en niet over ‘een vergelijking van registraties’. Zoals uiteengezet biedt dit ruimte om zowel de koppeling van gehele gegevensbestanden als die van gedeelten daarvan als koppeling in de zin van art. 6 WPolr aan te merken.<sup>26</sup> Dit is niet het geval wanneer gebruik wordt gemaakt van externe gegevens die geen onderdeel uitmaken van een zelfstandig register.

#### Voorwaarden

Wanneer een verwerking van externe gegevens als een koppeling kan worden aangemerkt, is het gebruik van (en daarmee een koppeling met) externe gegevens die afkomstig zijn van buiten het politieke apparaat, slechts beperkt mogelijk. Op grond van art. 6 lid 1 WPolr en meer specifiek art. 4 lid 1 BPolr mag een politieregister alleen worden gekoppeld met een ander politieregister of met een persoonsregistratie van het Rijk, provincies, gemeenten en andere openbare lichamen met inbegrip van de daaronder ressorterende diensten, instellingen en bedrijven.<sup>27</sup> Verder dient een koppeling op grond van art. 6 lid 1 WPolr noodzakelijk te zijn voor de politietaak<sup>28</sup>.

Een koppeling die plaatsvindt in het kader van een ongericht dataminingonderzoek leidt tot een registratie van externe gegevens in het datawarehouse, ofwel het basisregister. Op grond van art. 4 lid 2 WPolr mag een register slechts persoonsgegevens bevatten die noodzakelijk zijn voor het doel waarvoor dat register is aangelegd. Dit betekent dat de

---

24. *Kamerstukken II*, 1997/98, 25 403, nr. 7, p. 18.

25. Art. 4 WPolr.

26. Verbeek e.a. 1999, p. 170-171.

27. Als bedoeld in art. 17, aanhef en onder *a* Wpr.

28. Hier voor zover het de strafrechtelijke handhaving van de rechtsorde betreft.

registratie van gegevens uit een ander register in het basisregister (en daarmee ook de koppeling waaruit de registratie voortvloeit), noodzakelijk dient te zijn voor het doel van het basisregister. In dit verband kan worden gesproken van een indirecte doelbinding.

Art. 6 lid 2 WPoI bepaalt dat een koppeling in beginsel slechts mogelijk is indien en voor zover het reglement dat bepaalt<sup>29</sup>. Ingeval van een koppeling van een politieregister met gegevens afkomstig van bronnen buiten de politieke sfeer dient het reglement van het (politie)register (basisregister/datawarehouse) te voorzien in een mogelijkheid tot een dergelijke koppeling. Hoewel een koppeling in beginsel krachtens de regelgeving van alle in het geding zijnde registers toelaatbaar dient te zijn<sup>30</sup> kan uit de formulering van art. 6 lid 2 WPoI niet onmiddellijk worden opgemaakt of ook voor niet-politieregisters een voorziening in het reglement dient te worden getroffen. In een tijd waarin de roep om het gebruik van allerhande gegevensverzamelingen ten behoeve van de opsporing steeds luider wordt is duidelijkheid op dit punt van belang.

### 7.3.2.3 *Wpr en Wbp*

De Wbp ziet op elke geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens<sup>31</sup>, alsmede de niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of bestemd zijn om daarin te worden opgenomen.<sup>32</sup> In art. 2 lid 2 sub *c* Wbp is bepaald, dat de Wbp niet van toepassing is op de verwerking van persoonsgegevens ten behoeve van de politietoek.<sup>33</sup> Met dit artikel is uitvoering gegeven aan art. 3 lid 2 van de Privacyrichtlijn; volgens dat artikel zijn de bepalingen van de richtlijn niet van toepassing op verwerking van persoonsgegevens die geschiedt met het oog op de uitoefening van niet binnen de werkingssfeer van het gemeenschapsrecht vallende activiteiten. Voorbeelden daarvan zijn verwerkingen die betrekking hebben op de openbare veiligheid, defensie, de veiligheid van de Staat en de activiteiten van de Staat op strafrechtelijk gebied. Gebruik makend van de mogelijkheid die de Richtlijn daartoe biedt heeft de wetgever gekozen voor de regeling van de verwerking van gegevens door de opsporingsdiensten in het kader van de politietoek in een aparte wet: de WPoI. Aangezien in de Wpr al werd bepaald dat die wet niet van toepassing is op persoonsregistraties die worden aangelegd ten dienste van de uitvoering van de politietoek zoals omschreven in art. 2 van de Politiewet 1993<sup>34</sup>, wordt deze situatie in feite in de WPoI gehandhaafd.

---

29. *Kamerstukken II*, 1985/86, 19 589, nr. 3, p. 9 en art. 6 lid 2 WPoI.

30. *Kamerstukken II*, 1988/89, 19 589, nr. 11, p. 13.

31. Gegevens betreffende een geïdentificeerde of identificeerbare natuurlijke persoon (art. 1 sub *a* Wbp).

32. Art. 2 lid 1 Wbp.

33. Zie ook sectie 4.2.

34. Art. 2 lid 3 sub *b* Wpr.

De uitzonderingsbepaling in de Wpr wijkt echter op een belangrijk punt af van die in de Wbp, waarin het begrip ‘persoonsregistratie’ is vervangen door ‘de verwerking van persoonsgegevens’. Dit heeft tot gevolg dat op *alle* verwerkingen die plaatsvinden in het kader van de uitvoering van de politietaak de WPolr van toepassing is en niet de Wbp. Onder ‘verwerken’ verstaat de Wbp elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, evenals het afschermen, uitwissen of vernietigen van gegevens.<sup>35</sup> De formulering van de uitzonderingsbepaling in de Wbp geeft de nieuwe bepaling een veel grotere reikwijdte dan zijn voorganger. Ook het gebruik of het opvragen van gegevens uit een register, niet zijnde een politieregister, ten behoeve van een ongericht dataminingonderzoek kan als een verwerking in de zin van de Wbp worden aangemerkt. Er wordt niet meer gekeken naar de aard van de registratie waaruit de externe gegevens afkomstig zijn, maar naar het doel waarvoor de gegevens gebruikt worden. Wanneer het daarbij om een verwerking in het kader van de politietaak gaat, is de WPolr van toepassing. Een gevolg daarvan is dat het CBP minder toezichthoudende bevoegdheden heeft ten aanzien van de betreffende gegevensverwerking. Een ander gevolg is dat zowel de WPolr als het BPolr van toepassing is in het geval van een koppeling ten behoeve van een ongericht dataminingonderzoek in het kader van de strafrechtelijke handhaving van de rechtsorde. Het is dus wenselijk dat met de wet- en regelgeving wordt voorzien in een duidelijke regeling voor de verwerking van externe gegevensverzamelingen in het kader van de opsporingstaak en de rol die het reglement daarbij speelt. In het reglement dient te worden aangegeven op welke wijze de gegevens verwerkt mogen worden. Wanneer in art. 6 lid 2 WPolr wordt bepaald dat een koppeling met externe gegevens alleen mogelijk is in overeenstemming met het reglement van dat register, dan wordt daarmee voldaan aan de doelbinding van de Wbp.

In de praktijk zal de betekenis van de Wbp bij een verwerking van externe gegevens in het kader van een ongericht dataminingonderzoek gering zijn. Een mogelijkheid van een zodanige verwerking is, gezien de hiervoor besproken aard van het ongerichte dataminingonderzoek, namelijk beperkt. De Wbp ziet op de verwerking van persoonsgegevens, of gegevens betreffende een geïdentificeerde of identificeerbare, natuurlijke persoon. In het kader van een ongericht dataminingonderzoek is het in beginsel niet mogelijk om deze (externe) gegevens te verwerken. Bij het opbouwen en in stand houden van een zekere informatiepositie is het vergaren van externe gegevens enkel mogelijk door toepassing van niet-ingrijpende middelen. Het gebruik van deze middelen mag niet leiden tot een inbreuk op de persoonlijke levenssfeer. Omdat een verwerking van per-

---

35. Art. 1 sub b Wbp.

soonsgegevens in het kader van de strafrechtelijke handhaving van de rechtsorde in beginsel steeds een dergelijke inbreuk impliceert, is het gebruik ervan ten behoeve van een ongericht dataminingonderzoek niet zonder meer toegestaan. Dit kan anders zijn wanneer het gebruik van de betreffende gegevens is gebaseerd op een wettelijke grondslag.

#### 7.3.2.4 *Vrijwillige verstrekking en 'fishing expeditions'*

Om te voorzien in hun informatiebehoefte doen opsporingsdiensten in toenemende mate een beroep<sup>36</sup> op allerhande verwerkers van persoonsgegevens, zoals vliegmaatschappijen, banken en internetproviders.<sup>37</sup> Daarbij wordt een verzoek gedaan om bepaalde gegevens op vrijwillige basis te verstrekken. Het is echter de vraag in hoeverre opsporingsdiensten deze 'vrijwillig' verstrekte gegevens mogen verwerken. Voorheen was een vrijwillige verstrekking gebaseerd op art. 11 Wpr, tegenwoordig is dat art. 43 Wbp. Het bepaalde in art. 43 onder *b* Wbp vormt een grondslag voor een vrijwillige verstrekking door een houder van gegevens, indien die verstrekking (voor een afwijkend doel) noodzakelijk is in het belang van de voorkoming, opsporing en vervolging van strafbare feiten. De houder van de gegevens dient een afweging te maken of een verstrekking inderdaad noodzakelijk is

#### **Geen wettelijke basis verwerking**

Het is de vraag of een verwerking door politie van gegevens die zijn verkregen op basis van art. 43 Wbp rechtmatig is nu dit artikel slechts een bevoegdheid verleent om gegevens te verstrekken.<sup>38</sup> Bij een strafvorderlijke gegevensvergaring waarbij een inbreuk op de persoonlijke levenssfeer wordt gemaakt of waarbij gegevens voor een ander doel worden gebruikt dan waarvoor zij zijn vastgelegd, dient te worden voldaan aan een aantal voorwaarden. Een zodanige bevoegdheid dient bij wet te zijn voorzien, te voldoen aan eisen van toegankelijkheid en voorzienbaarheid en waarborgen te bevatten tegen willekeur. Van een wettelijke regeling die aan deze eisen voldoet is geen sprake indien, zoals bij art. 43 Wbp, vrijwilligheid voorop staat en de tot opsporing bevoegde instantie in overleg met de houder van de gegevens komt tot afspraken over welke gegevens in een bepaald geval verstrekt zullen worden.<sup>39</sup> Daarom lijkt het ongewenst art. 43 Wbp te beschouwen als basis voor reguliere verstrekking van persoonsgegevens ten behoeve van de opsporing<sup>40</sup>. Internetprovider XS4ALL maakt al jaren bezwaar tegen het gebruik, om vrijwillige medewerking te vragen op grond van passages uit de Wbp. Privacywetgeving is uitdrukkelijk bedoeld om de privacy te beschermen, niet als onderbouwing van opspo-

---

36. *Kamerstukken II*, 2001/02, 28 059, nr. 3, p. 2.

37. Commissie Mevis 2001, p. 20.

38. Sietsma 2004.

39. *Kamerstukken II*, 2001/02, 28 366, nr. 1, p. 5.

40. *Kamerstukken II*, 2001/02, 28 366, nr. 1, p. 7.

ringsbehoeften. Ook met het oog op art. 2 Wbp lijkt een beroep op art. 43 Wbp twijfelachtig. Art. 2 lid 2 onder *c* verklaart de Wbp niet van toepassing op de verwerking van persoonsgegevens ten behoeve van de uitvoering van de politietaak, zoals omschreven in art. 2 Politiewet 1993.

Op het moment van schrijven ligt bij de Eerste Kamer het wetsvoorstel Vorderen gegevens<sup>41</sup> waarin bevoegdheden worden gecreëerd voor de opsporingsambtenaar en de OvJ om in het belang van een opsporingsonderzoek de beschikking te krijgen over gegevens die bij derden aanwezig zijn. Hiermee wordt de noodzakelijke praktijk van het schijnbaar oneigenlijk gebruik van art. 43 Wbp door opsporingsdiensten grotendeels overbodig. Voor de verwerking van gegevens die op grond van het wetsvoorstel mogen worden gevorderd is dan een wettelijke grondslag aanwezig. Tegelijkertijd betekent dit dat, buiten de bevoegdheden van het voorstel om, aan derden niet mag worden gevraagd om op vrijwillige basis mee te werken aan het verstrekken van gegevens.<sup>42</sup> Het is niet uitgesloten dat ook na de inwerkingtreding van het wetsvoorstel in incidentele gevallen nog op vrijwillige basis gegevens verstrekt zullen worden aan politie en justitie. Het initiatief daartoe gaat dan niet uit van politie en justitie.<sup>43</sup> Of deze gegevens nu moeten worden aangemerkt als onrechtmatig verkregen en niet mogen bijdragen aan het bewijs, hangt af van de omstandigheden van het geval. Factoren die hierbij een rol spelen zijn de aard van het belang dat geschonden is door het niet toepassen van de wettelijke bevoegdheid, de ernst van het verzuim en het nadeel dat daardoor wordt veroorzaakt. Bovendien zal, indien het niet de verdachte is die getroffen is in het belang dat door de niet nageleefde regel wordt beschermd, in de regel daaraan in de strafzaak geen rechtsgevolg worden verbonden.<sup>44</sup>

#### Wettelijke basis en ‘fishing expeditions’

De informatie- en communicatietechnologie zorgt ervoor dat er steeds meer gegevens beschikbaar zijn bij instellingen en bedrijven. In de MvT bij het wetsvoorstel Vorderen gegevens<sup>45</sup> is aangegeven dat, wanneer deze gegevens kunnen bijdragen aan de opsporing van strafbare feiten, het voor de instanties die belast zijn met de opsporing van belang is om over deze gegevens de beschikking te kunnen krijgen. In de praktijk zou de eenvoudige toegang tot zoveel gegevens zogenaamde fishing expeditions door opsporingsdiensten in de hand kunnen werken. Een instantie als Interpay heeft bijvoorbeeld een schat aan informatie in huis en legt deze ook doelbewust vast.<sup>46</sup> Het structureel verwerken van deze gegevens ten behoeve van de opsporing tot er ‘iets interessants’ uitkomt, zou op

41. *Kamerstukken II*, 2003 /04, 29 441, nr. 3.

42. Tenzij de Wbp hierop niet van toepassing is.

43. *Kamerstukken I*, 2004 /05, 29 441, C, p. 2-3.

44. HR 30 maart 2004, LJN AM2533.

45. *Kamerstukken II*, 2003 /04, 29 441, nr. 3.

46. Zie CBP: Wbp Meldingenregister, Interpay Nederland B.V., meldingsnr. 1080620

gespannen voet staan met de rechtsstaat. Het kan er volgens de wetgever toe leiden dat de burger te eenvoudig als verdachte kan worden aangemerkt omdat bevoegdheden te gemakkelijk misbruikt kunnen worden. Ook wordt de opsporing minder effectief wegens gebrek aan selectiviteit. Om één en ander te ondervangen is de inzet van de bevoegdheden in het wetsvoorstel gebonden aan voorwaarden. Gegevens kunnen uitsluitend gevorderd worden in het belang van een concreet opsporingsonderzoek ter opheldering van een gepleegd misdrijf dan wel het in georganiseerd verband beramen of plegen van misdrijven die een ernstige inbreuk op de rechtsorde maken. De grond voor het vorderen van gegevens is altijd gelegen in de concrete strafbare feiten of omstandigheden die onderzocht worden.<sup>47</sup> Het is dus niet mogelijk dat van bepaalde personen gegevens kunnen worden gevorderd, welke personen vervolgens vanwege hun belangstellingssfeer als verdacht kunnen worden aangemerkt. Uitsluitend indien dit van belang is voor een concreet opsporingsonderzoek kunnen van bepaalde personen gegevens gevorderd worden.

#### 7.3.2.5 *Gebruik van gegevens uit openbare registers*

Het belang van de doelbinding bij de verwerking van externe gegevens ten behoeve van de opsporingstaak wordt afzonderlijk onderstreept voor de openbare registers. In de MvT<sup>48</sup> is aangegeven dat er buiten een verkennend onderzoek, verdenking of een andere ‘uitvoering van de politietaak in een bepaald geval’ (bij het hanteren van een tijdelijk register), niet zomaar gebruik kan worden gemaakt van gegevens uit een openbaar register ten behoeve van de opsporing. Persoonsgegevens mogen alleen worden verwerkt indien dat noodzakelijk is voor de uitvoering van de politietaak. Het noodzakelijkheidsvereiste brengt met zich dat de politietaak niet kan rechtvaardigen dat over een onbepaalde groep van burgers gegevens worden vergaard voor algemene politieke doeleinden, ook niet uit openbare bronnen.<sup>49</sup> Dit betekent dat het gebruik van gegevens uit openbare registers ten behoeve van ongericht dataminingonderzoek in beginsel niet is toegestaan.<sup>50</sup>

Het gebruik van (gegevens uit) openbare registers die bij wet zijn ingesteld, is wel mogelijk ten behoeve van een gericht dataminingonderzoek of verificatie waarbij het de politietaak in een bepaald geval betreft. Deze lijn is voortgezet met de aanpassing van art. 126gg Sv. Daardoor is het mogelijk dat de OvJ, indien dit noodzakelijk is voor de uitvoering van het (verkenning) onderzoek, kan bepalen dat art. 9 lid 1 Wbp<sup>51</sup> met

47. *Kamerstukken I*, 2004/05, 29 441, C, p. 10.

48. *Kamerstukken II*, 1998/99, 26 410, nr. 3.

49. *Kamerstukken II*, 1998/99, 26 410, nr. 3, p. 10-11.

50. In art. 125i Sv wordt de politie de mogelijkheid geboden om buiten de situatie van het verkennend onderzoek, toegang te hebben tot openbare registers. De gegevens waartoe toegang kan worden verkregen zijn in art. 125i Sv nader geclausuleerd. Belangrijke voorwaarde daarbij is dat de op grond van art. 125i Sv verkregen gegevens in een tijdelijk register komen. Zij mogen niet voor de opsporing in algemene zin worden gebruikt (*Kamerstukken II*, 1998/99, 26 410, nr. 3, p. 11). Met het oog hierop is het niet mogelijk om de op grond van deze bevoegdheid verkregen gegevens te gebruiken voor een ongericht dataminingonderzoek.

betrekking tot het onderzoek niet van toepassing is op daarbij nader aan te geven openbare registers die bij wet zijn ingesteld. In dat geval kan er in het kader van een gericht dataminingonderzoek gebruik worden gemaakt van gegevens uit de betreffende openbare registers, zelfs wanneer dit in strijd zou zijn met het doelbindingsbeginsel. Met betrekking tot een verstrekking op grond van bijvoorbeeld art. 15 lid 3 sub *b* van de Handelsregisterwet 1996, een spiegelbepaling van art. 126gg Sv lid 2, wordt aangegeven dat deze kan plaatsvinden naar aanleiding van een concrete aanwijzing in een individueel geval maar ook een bulkverstrekking kan betreffen die het mogelijk maakt te zoeken naar een op voorhand onbepaalde groep van personen. Het gebruik van de gegevens is beperkt tot een ‘bepaald geval’ in de zin van art. 13 WPolr, dus bij een verdenking of een CIE-subject. Het meest vergaande gebruik wordt aangetroffen bij een verkennend onderzoek. Voor het dataminingonderzoek kan dit betekenen dat er in het kader van een verkennend onderzoek niet alleen gegevens uit een ander register mogen worden gebruikt maar dat het, gezien de term ‘bulkverstrekking’, zelfs mogelijk is om een volledige koppeling van registers te bewerkstelligen.<sup>52</sup>

### Resumerend

Wanneer in het kader van een dataminingonderzoek met betrekking tot een gewoon politieregister gebruik wordt gemaakt van externe gegevens van buiten de politieke sfeer, geldt een aantal bijkomende voorwaarden:

- een koppeling dient noodzakelijk te zijn voor de politietaak voor zover deze de strafrechtelijke handhaving van de rechtsorde betreft;
- een koppeling dient noodzakelijk te zijn voor het doel van het basisregister<sup>53</sup>;
- het reglement van het basis(politie)register dient in de mogelijkheid van een koppeling te voorzien<sup>54</sup>;
- met het gebruik van externe gegevens wordt geen ontoelaatbare inbreuk op de privacy gemaakt<sup>55</sup>;
- het gebruik van (persoons)gegevens uit een openbaar register is in beginsel niet toegestaan.

51. Dit artikel ziet op de doelbinding. Art. 9 lid 1 Wbp: ‘Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen.’

52. *Kamerstukken II*, 1998/99, 26 410, nr. 3, p. 10.

53. Het register waarop het dataminingonderzoek betrekking heeft.

54. Wanneer de externe gegevens geen deel uitmaken van enig (politie)register, is er geen sprake van een koppeling in de zin van art. 6 WPolr.

55. In dat geval zou het in beginsel een ingrijpend middel betreffen, hetgeen in dit stadium van het proces van informatiegaring niet is toegestaan.

De mogelijkheden om in het kader van een ongericht dataminingonderzoek gebruik te maken van gegevens van buiten de politieke sfeer lijken hiermee beperkt. De verwerking van persoonsgegevens zal vaak afketsen op privacyrechtelijke gronden. Bij een verwerking van externe gegevens zal het vooral gaan om tips die bij opsporingsinstanties binnenkomen.

### 7.3.3 *Het gebruik van gegevens uit een gewoon politieregister*

De tweede categorie van externe gegevens betreft de gegevens die al in de overige politieregisters aanwezig zijn. Voor de gegevens in de gewone politieregisters wordt het uitgangspunt van een vrij verkeer ('free flow') binnen het politieapparaat gehanteerd.<sup>56</sup> Dit betekent dat deze in beginsel zonder nadere voorwaarden mogen worden gebruikt in het kader van de vervulling van de politietaken.<sup>57</sup> Indien de bevraging past binnen dat kader geldt voor de houder van een politieregister een verplichting tot verstrekking.<sup>58</sup> Binnen het politieapparaat kunnen de verstrekte gegevens in beginsel voor alle politietaken worden gebruikt.<sup>59</sup> Over de ruime toegang tot de gegevens in de gewone politieregisters die een verplichting tot verstrekken met zich meebrengt, zegt de wetgever het volgende<sup>60</sup>:

*'Wij achten het ongewenst dat op het terrein van de gegevensverstrekking binnen de Nederlandse politie een compartimentering zou ontstaan waardoor politiekorpsen met behulp van de hen ter beschikking staande gegevens elkaar zouden hebben kunnen beconcurreren in de misdaadbestrijding. Een Nederlandse politieambtenaar moet, mits het doel dit rechtvaardigt, kunnen beschikken over alle gegevens die binnen de Nederlandse politie zijn opgeslagen.'*

Deze passage dient in de juiste context te worden gezien. Schreuders<sup>61</sup> geeft aan dat er vooral mee wordt bedoeld op de goede samenwerking van politie-instanties en de bestrijding van ongewenste bureaupolitiek. De passage mag niet als een vrijbrief voor ongelimiteerde informatie-uitwisseling worden uitgelegd. In tegenstelling tot de veronderstelling van de PEC<sup>62</sup> bestaan er voor de politie wel degelijk beperkingen om tot koppeling met

56. *Kamerstukken II*, 1996/197, 25 398, nr. 3, p. 4.

57. *Kamerstukken II*, 1995/196, 24 072, nrs. 10-11, p. 283.

58. *Kamerstukken II*, 1995/196, 24 072, nr. 14, p. 376. Van deze verplichting zijn onder omstandigheden uitgezonderd de registers zware criminaliteit, de tijdelijke registers, de voorlopige registers en de registers aangelegd ten behoeve van de hulpverlenende taak van de politie. Voor de registers die bij de politie worden gehouden, maar die niet zijn terug te voeren op de politietaken ex art. 2 Politiewet 1993 geldt het regime van de Wbp. Dit betekent bij bevraging voor de houder van het register dat hij een afweging van belangen moet maken.

59. *Kamerstukken II*, 1997/198, 25 398, nr. 6, p. 2. Zie ook de art. 14 tot en met 16, alsmede 18 WPolr.

60. *Kamerstukken II*, 1988/89, 19 589, nr. 6, p. 11.

61. Schreuders 1995.

bij zichzelf berustende registers over te gaan. Deze beperkingen hangen samen met de doelbinding, de aard van de politietaak, de koppeling, het gebruik van externe gegevens in het kader van een ongericht dataminingonderzoek en de bevoegdheden van de beheerder van een politieregister.

### 7.3.3.1 De doelbinding

Het doelbindingsbeginsel gaat ervan uit dat het doel waarvoor bepaalde gegevens in eerste instantie zijn vastgelegd, zich kan verzetten tegen verstrekking en gebruik van die gegevens voor andere doeleinden. Dit beginsel komt overeen met het principe van verenigbaar gebruik zoals beschreven in het Databeschermingsverdrag. In de WPolr en het BPolr ontbreekt vooralsnog de doelbinding als specifieke voorwaarde voor de verwerking van gegevens die zijn vastgelegd in de gewone politieregisters.<sup>63</sup> Dit betekent echter niet dat het doelbindingsbeginsel geen betekenis heeft voor het gebruik van gegevens uit de gewone politieregisters. De Wbp vormt een afspiegeling van de bestaande internationale opvattingen op het gebied van gegevensverwerking en zoals uiteengezet<sup>64</sup>, dient bij de uitleg van de WPolr aansluiting te worden gezocht bij de Wbp. Hoewel de gewone politieregisters in beginsel worden aangelegd ten behoeve van de algemene politietaak, kan het doelbindingsbeginsel een beperking vormen voor het vrije verkeer van de gegevens uit deze registers binnen het politieapparaat. In beginsel is het doel van een ongericht dataminingonderzoek de verbetering van de informatiepositie van politie en justitie. Dat doel kan nader worden gespecificeerd wanneer de nagestreefde verbetering van de informatiepositie betrekking heeft op één bepaald gewoon politieregister. Om te beginnen dient te worden bepaald voor welk specifiek doel het basisregister tot stand is gebracht. Vervolgens kan worden getoetst of het doel van het register waaruit de aangeboden of verzochte gegevens afkomstig zijn daarmee (grotendeels) verenigbaar is. Wanneer gegevens in gewone politieregisters in eerste instantie voor een totaal ander doel zijn verkregen dan waarvoor ze worden opgevraagd dan is de verwerking ervan in het kader van een ongericht dataminingonderzoek omstreden. Dit geldt des te meer wanneer het dataminingonderzoek een ingrijpend doel als de strafrechtelijke handhaving van de rechtsorde dient. Hoewel een verplichte verstrekking van gegevens het uitgangspunt is, dient de mogelijkheid om een verstrekking te weigeren op grond van het doelbindingsbeginsel niet te worden uitgesloten.

---

62. *Kamerstukken II*, 1995/96, 24 072, nr. 14, p. 238 “Inhoudelijke beperkingen aan de politie om al dan niet tot koppeling met bij zichzelf berustende registers over te gaan zijn niet aangetroffen: ook ‘grijze-veld’ registers (de huidige registers zware criminaliteit) en registers van contacten kunnen onbeperkt worden gekoppeld.”

63. Alleen het hulpverleningsregister en het register-MOT vormen hierop een uitzondering, zie art. 12 BPolr.

64. Zie sectie 4.2.

Het standpunt dat bij een verwerking van gegevens rekening dient te worden gehouden met het doelbindingsbeginsel lijkt te worden bevestigd door art. 4 lid 2 WPolr. Op grond daarvan dient de aanwezigheid van persoonsgegevens in een politieregister noodzakelijk te zijn voor het doel waarvoor het register is aangelegd. Voor een dataminingonderzoek betekent dit dat een registratie van externe (persoons)gegevens in het basisregister<sup>65</sup> noodzakelijk dient te zijn voor het doel van het basisregister en daarmee voor het dataminingonderzoek. Wanneer de externe gegevens met een andere doelstelling zijn vastgelegd dan waarvoor zij thans worden verwerkt is mogelijk niet voldaan aan de voorwaarde, dat de aanwezigheid van de gegevens noodzakelijk dient te zijn voor het doel van het basisregister. In dit licht vervult art. 4 lid 2 WPolr een vangnetfunctie waarmee indirect wordt voorzien in het doelbindingsbeginsel. Hier blijkt dat de regels, die de WPolr stelt aan een registratie van gegevens in een bepaald gewoon politieregister, ook van toepassing zijn wanneer in het kader van een dataminingonderzoek gegevens uit een ander gewoon politieregister in dat register worden vastgelegd<sup>66</sup>. Aangezien de gewone politieregisters in beginsel zijn aangelegd ter ondersteuning van de algemene politietaak, zijn zij qua doelstelling sterk aan elkaar verwant.<sup>67</sup> Hierna wordt ingegaan op twee gewone politieregisters die daarop een uitzondering vormen, te weten het hulpverleningsregister en het register van het Meldpunt Ongebruikelijke Transacties.

#### **Het Hulpverleningsregister en het register Meldpunt Ongebruikelijke Transacties**

In tegenstelling tot de overige gewone politieregisters kennen het hulpverleningsregister en het register van het Meldpunt Ongebruikelijke Transacties wel een doelbindingsbepaling. Op grond van art. 12 lid 1 sub *a* en *b* BPolr mogen deze registers in beginsel alleen worden gebruikt voor het doel waarvoor zij in eerste instantie zijn aangelegd. Hoewel het gaat om gewone politieregisters zijn zij niet bestemd voor raadpleging.<sup>68</sup> Met betrekking tot de gegevens in een hulpverleningsregister bepaalt art. 12 lid 1 sub *a* BPolr dat deze niet voor andere doeleinden mogen worden gebruikt, tenzij met uitdrukkelijke instemming van de geregistreerde. Overigens betekent de aanwezigheid van een zodanige instemming niet dat de gegevens zonder meer in het kader van een dataminingonderzoek mogen worden gebruikt. Bij een ongericht dataminingonderzoek dienen burgers in beginsel namelijk gevrijwaard te blijven van politieke bemoeienis indien hun persoon daartoe geen aanleiding geeft.<sup>69</sup> Het enkele feit dat iemand is opgenomen in een hulpver-

65. Het basisregister vormt in het geval van een ongericht dataminingonderzoek het datawarehouse.

66. Zie sectie 7.1.

67. Dit in tegenstelling tot de nog te bespreken bijzondere politieregisters, die juist met het oog op een specifiek doel worden aangelegd. Doelstellingen van een tijdelijk register zijn veel strikter omlijnd en minder algemeen. Het bereik van het doel moet te voorzien zijn; bijvoorbeeld door het vinden van de dader komt er een einde aan een reeks overvallen.

68. Zie sectie 7.1.

69. *Kamerstukken II*, 1996/97, 25 403, nr. 3, p. 8.

leningsregister kan moeilijk als een zodanige aanleiding worden aangemerkt. Met het beperkte verstrekkingenregime dat op een hulpverleningsregister van toepassing is wordt beoogd te voorkomen dat hulpbehoevenden zich belemmerd voelen door de mogelijkheid, dat de aangaande hun persoon vastgelegde gegevens voor andere doeleinden worden gebruikt<sup>70</sup>. Met het oog op de specifieke aard en het doel van de gegevens die in een hulpverleningsregister liggen opgeslagen kan het niet zo zijn dat die gegevens ook voor politiedoeleinden worden gebruikt, laat staan ten behoeve van de opsporing. De doelbindingsbepaling vormt hier in eerste instantie een waarborg voor de burger. De aanwezigheid van een uitdrukkelijke instemming van de geregistreerde om zijn of haar gegevens te verwerken impliceert om die reden niet zonder meer een dergelijke bevoegdheid voor de opsporingsautoriteiten. Voor een register van het Meldpunt Ongebruikelijke Transacties (register-MOT) wordt in art. 12 lid 1 sub *b* BPoI bepaald dat een verstrekking uit dit register slechts is toegestaan voor het doel waarvoor het register in eerste instantie is aangelegd. Bovendien is een verstrekking alleen mogelijk met het oog op de voorkoming en opsporing van misdrijven.<sup>71</sup> Hoewel op art. 12 lid 1 sub *b* BPoI enkele uitzonderingen bestaan, zijn deze in beginsel niet van toepassing op een verstrekking die plaatsvindt ten behoeve van een verbetering van de informatiepositie van een gewoon politieregister.

#### *7.3.3.2 De aard van de politietaak*

De vraag of aan het doelbindingsbeginsel is voldaan wordt in sterke mate beïnvloed door de aard van de politietaak in het kader waarvan de (externe) gegevens in een gewoon politieregister zijn verzameld en vastgelegd. In sectie 7.3.1 bleek dat de politietaak bestaat uit de hulpverlening en de handhaving van de rechtsorde, welke laatste uiteenvalt in de strafrechtelijke handhaving van de rechtsorde en de handhaving van de openbare orde. Een ongericht dataminingonderzoek zoals hier beschreven vindt plaats in het kader van de politietaak ten behoeve van de strafrechtelijke handhaving van de rechtsorde. Niet alle politieregisters worden echter in dat kader aangelegd en bijgehouden. Het is de vraag in hoeverre, gelet op de doelbinding, gebruik kan worden gemaakt van gegevens uit gewone politieregisters die niet zijn aangelegd ten behoeve van de politietaak voor zover het de strafrechtelijke handhaving van de rechtsorde betreft.

#### **Niet aangelegd ten behoeve van de politietaak**

Om te beginnen bestaan er politieregisters die in het geheel niet zijn aangelegd in het kader van de politietaak zoals omschreven in art. 2 Politiewet 1993. Naast de taken uit de Politiewet 1993 heeft de politie bij bijzondere wetten namelijk ook taken toebedeeld gekregen die niet direct tot de politietaak zijn te herleiden. Hierbij gaat het bijvoorbeeld

---

70. Art. 12 BPoI.

71. Art. 4 lid 2 Wet MOT.

om de Wet wapens en munitie (WMM) en de Wegenverkeerswet (WVW). Ook op de gebieden van de horeca en het milieu heeft de politie meer taken dan de strafrechtelijke handhaving van omvangrijke regelgeving. Voor de uitvoering van deze taken worden registers aangelegd waarvan sommige een rol kunnen spelen bij de bestrijding van de georganiseerde criminaliteit. In beginsel vallen deze registers niet onder het regime van de WPolr, maar onder dat van de Wbp.<sup>72</sup> In bepaalde gevallen worden de registers beheerst door een eigen, bij of krachtens de wet vastgestelde, regeling.<sup>73</sup> Van belang is dat er met betrekking tot deze categorie politieregisters geen sprake is van een vrij verkeer van informatie. Voor het gebruik van deze gegevens ten behoeve van dataminingsonderzoek gelden in beginsel dezelfde voorwaarden als die welke van toepassing zijn op het gebruik van externe gegevens afkomstig van buiten de politieke sfeer. Op het moment dat gegevens uit deze registers worden verwerkt in het kader van de politietaken, is zoals uiteengezet in sectie 7.3.2.2, niet de Wbp van toepassing maar de WPolr. Hoewel de politieregisters waar het hier om gaat in eerste instantie niet in het kader van de politietaken zoals omschreven in art. 2 Politiewet 1993 zijn aangelegd, vindt de verstrekking uit die registers wel in het kader daarvan plaats. Naast registers die in het geheel niet zijn aangelegd ten behoeve van de politietaken zijn er ook politieregisters die wel in het kader van de politietaken worden aangelegd maar niet voor zover het de strafrechtelijke handhaving van de rechtsorde betreft. Het gaat dan om de politieregisters die worden aangelegd in het kader van de handhaving van de openbare orde en de hulpverleningstaak.

#### **De handhaving van de openbare orde**

Informatie die is verzameld in het kader van de handhaving van de openbare orde wordt opgeslagen in een register openbare-ordehandhaving (OOH-register). Het OOH-register is een politieregister zoals bedoeld in art. 1 lid 1 sub *c* WPolr. In het register worden geen strafrechtelijke gegevens opgenomen en een permanente registratie kan zowel regionaal als landelijk worden samengesteld en bijgehouden. Het doel van de OOH-registers verschilt van dat van de registers die zijn aangelegd voor de uitvoering van de justitiële politietaken. Het aanknopingspunt voor de op te nemen categorieën van persoonsgegevens in een OOH-register is de mate waarin en de redenen waarom betrokkenen in verband kunnen worden gebracht met (toekomstige) verstoringen van de openbare orde. Kenmerkend voor de te nemen beslissingen in het kader van de handhaving van de openbare orde is dat informatie nodig is over de bewegingen en activiteiten van groepen van personen en over de gevolgen die daaraan verbonden kunnen zijn voor de openbare orde. Wanneer de politie streeft naar het verkrijgen van een beeld van de bewegingen en activiteiten van groepen van personen, is in beginsel behoefte aan groepsgerichte en niet aan persoonsgerichte informatie. Anders dan ten behoeve van de opsporing van strafbare fei-

---

72. Art. 2 Wbp.

73. *Kamerstukken II*, 1995/196, 24 072, nr. 14, p. 347.

ten is de informatie-inwinning niet gericht op het verkrijgen van sluitende bewijzen tegen bepaalde personen. Ook anderszins wordt geen informatie ingewonnen die gericht is op het kunnen treffen van maatregelen tegen individuele personen.<sup>74</sup>

Het inwinnen van informatie door de politie ter handhaving van de openbare orde vindt plaats op grond van art. 2 Politiewet 1993. De reikwijdte van dit artikel is in zoverre beperkt dat het geen basis biedt voor methodieken van informatie-inwinning waarvan de toepassing als zodanig kan resulteren in een min of meer volledig beeld van bepaalde aspecten van het leven van een bepaalde persoon. Daarvoor is een afzonderlijke wettelijke basis vereist.<sup>75</sup> Voor een antwoord op de vraag wanneer sprake is van de toepassing van dergelijke methodieken kan aansluiting worden gezocht bij de Wet BOB, die als criterium daarvoor het begrip ‘stelselmatig’ hanteert. Alleen toepassingsvormen van observatie, inzet van een informant en inzet van een politiële undercover die gericht zijn op het stelselmatig inwinnen van informatie over een persoon, kunnen een inbreuk op de privacy maken. Het begrip ‘stelselmatig’ houdt in dat de toepassingsvorm van dien aard is dat daarmee een min of meer volledig beeld wordt verkregen van bepaalde aspecten van iemands leven.<sup>76</sup>

*Handhaving openbare orde en handhaving strafrecht* – De handhaving van de openbare orde en de handhaving van het strafrecht hebben ieder een eigen traject met eigen verantwoordelijkheden. De burgemeester is verantwoordelijk voor de handhaving van de openbare orde en de OvJ voor de handhaving van het strafrecht.<sup>77</sup> Bij grootschalige ongeregeldeheden kan soms moeilijk een helder onderscheid worden gemaakt tussen de handhaving van de openbare orde en de strafrechtelijke handhaving van de rechtsorde. Voor de handhaving van de openbare orde kan het voor de autoriteiten van belang zijn om over bepaalde informatie te beschikken die gerelateerd is aan de strafrechtelijke handhaving van de rechtsorde. Andersom is dat ook het geval. Zo kunnen gegevens in een OOH-registratie over een reeks diefstallen in een bepaalde buurt ook van belang zijn in het kader van de strafrechtelijke handhaving van de rechtsorde. In die gevallen bestaat behoefte aan de inzet van een beperkt aantal inlichtingenmiddelen (of bijzondere methoden).<sup>78</sup> Voor een optimale uitvoering van de verantwoordelijkheden is het gewenst dat op operationeel niveau, tijdens de daadwerkelijke handhaving, het bestuur, het OM en de politie voortdurend met elkaar in contact staan en afstemmen. Volgens de handleiding ‘Informatie Inwinning Openbare Orde’<sup>79</sup> kunnen de verantwoordelijkheden voor de

---

74. *Kamerstukken II*, 1999 /00, 25 232, nr. 18, p. 3.

75. *Kamerstukken II*, 1999 /00, 25 232, nr. 18, p. 6.

76. *Kamerstukken II*, 1996 /97, 25 403, nr. 3, p. 26.

77. Art. 1 sub *b* BPolr.

78. *Kamerstukken II*, 1998 /99, 26 269, nrs. 4-5.

79. Handleiding 2000.

handhaving van de openbare orde en de strafrechtelijke handhaving van de rechtsorde worden onderscheiden, maar zijn deze niet zodanig te scheiden dat zij volledig onafhankelijk van elkaar kunnen worden ingevuld. Over de exploitatie van informatie uit OOH-registraties (bijvoorbeeld ten behoeve van ongericht dataminingonderzoek) wordt in de handleiding het volgende gesteld<sup>80</sup>:

*‘De gegevens die in het kader van de openbare-ordehandhaving worden verzameld, kunnen tevens van belang zijn voor de handhaving van het strafrecht. Niet zelden zal immers openbare-orde informatie gegevens opleveren over – gepleegde of dreigende – strafbare feiten. Informatie die is vergaard door middel van een inwinningsmethode die past binnen artikel 2 van de Politiewet 1993, en schriftelijk is vastgelegd door de desbetreffende politieambtenaar, is informatie die ten dienste van politie en justitie staat. Deze informatie kan derhalve worden geëxploiteerd tussen politie en justitie (OM).’*

*Gebruik OOH-register ten behoeve van een ongericht dataminingonderzoek* – Het vergaren van informatie in het kader van de handhaving van de openbare orde met behulp van inwinningsmethoden die passen binnen art. 2 Politiewet 1993, vereist in beginsel geen aanvullende wettelijke basis. Omdat de informatie die wordt vergaard geen volledig beeld geeft van bepaalde aspecten van iemands leven, blijft de inbreuk op de privacy namelijk beperkt. Met het oog hierop lijkt het in beginsel ook mogelijk om de gegevens in de OOH-registers te gebruiken ten behoeve van een ongericht dataminingonderzoek. Een zodanige verwerking zal, gezien de aard van de gegevens in de OOH-registers en de omstandigheden waaronder deze zijn verkregen, geen ontoelaatbare inbreuk op de persoonlijke levenssfeer met zich meebrengen. De handleiding ‘Informatie Inwinning Openbare Orde’ stelt geen nadere beperkingen aan de exploitatie van de gegevens die zijn vergaard door middel van een inwinningsmethode die past binnen art. 2 Politiewet 1993. De gegevens zijn vergaard in het kader van de politietaak en het betreft politie-registers in de zin van art. 1 lid 1 sub c WPolr. In beginsel is daarom sprake van een vrij verkeer van deze gegevens binnen het politieapparaat. De mogelijkheid om ten behoeve van de strafrechtelijke handhaving van de rechtsorde gegevens te exploiteren die in eerste instantie in het kader van een andere politietaak zijn vergaard, kan echter worden beperkt door de doelbinding. Ook voor het gebruik van die gegevens in het kader van een bepaald ongericht dataminingonderzoek dient de noodzakelijkheid daarvan te worden aangetoond.

### **De hulpverleningstaak**

Een politieregister kan ten slotte zijn aangelegd in het kader van de politietaak voor zover het de hulpverlening betreft. Gegevens in dit register komen met het oog op de

---

80. Handleiding 2000 en *Kamerstukken II*, 1999 /00, 25 232, nr. 18.

doelbinding in beginsel niet in aanmerking voor gebruik ten behoeve van een ongericht dataminingonderzoek. Op grond van art. 12 lid 1 sub *a* BPolr worden uit een register dat uitsluitend is aangelegd met het oog op de uitvoering van de hulpverleningstaak geen gegevens verstrekt voor een ander doel dan waarvoor het register is aangelegd. De aard van de politietaak waarvoor gegevens in een hulpverleningsregister worden vastgelegd staat in beginsel los van de aard van de politietaak in het kader waarvan het ongerichte dataminingonderzoek hier plaatsvindt. Een verwerking van gegevens uit dit register ligt daarom niet in de rede. Slechts ingeval een geregistreerde uitdrukkelijk instemt met het gebruik van zijn gegevens is een uitzondering mogelijk op de strikte doelbinding van het hulpverleningsregister. Een zodanig verzoek aan een specifieke geregistreerde is echter moeilijk rijmbaar met het karakter van een ongericht dataminingonderzoek. In tegenstelling tot de hierboven besproken OOH-registers impliceert het gebruik van gegevens uit een hulpverleningsregister namelijk een inbreuk op de persoonlijke levenssfeer.

#### *7.3.3.3 Koppeling*

Wanneer in het kader van een ongericht dataminingonderzoek gebruik wordt gemaakt van gegevens uit een ander gewoon politieregister is in de regel sprake van een koppeling. Op grond van art. 6 lid 1 WPolr kan een gewoon politieregister worden gekoppeld met een ander gewoon politieregister wanneer dat noodzakelijk is voor de politietaak. Omdat de koppeling in dit geval plaatsvindt in het kader van de opsporingstaak kan worden gesteld, dat deze noodzakelijk dient te zijn voor de politietaak voor zover het de strafrechtelijke handhaving van de rechtsorde betreft. De mogelijkheid tot koppeling kan worden beperkt indien daarbij registers zijn betrokken die niet in het kader van de(z) politietaak zijn aangelegd. Op grond van lid 2 van art. 6 WPolr dienen de reglementen van beide bij de koppeling betrokken registers te voorzien in een mogelijkheid tot koppeling.<sup>81</sup> Omdat een gewoon politieregister op grond van art. 9 WPolr steeds een reglement dient te hebben, behoeft deze voorwaarde geen probleem te vormen.

#### **Functionaliteit gewone politieregisters**

Zoals uiteengezet in sectie 7.1 worden bij een koppeling met een ander gewoon politieregister gegevens uit dat register geregistreerd in het gewone politieregister waarop het dataminingonderzoek betrekking heeft. Een zodanige registratie is in beginsel steeds mogelijk wanneer dit gebeurt voor het doel van het basisregister. Omdat de gegevens in een gewoon politieregister, en dus ook in het basisregister, zijn bestemd voor operationeel gebruik is het echter de vraag of een registratie van deze gegevens in het basisregister niet in strijd komt met het verstrekkingenregime dat op de verstrekte gegevens van toe-

---

81. Art. 6 lid 2 WPolr en *Kamerstukken II*, 1995/196, 24 072, nr. 14, p. 238 'Wil koppeling met bestanden van derden toegepast kunnen worden dan dient het toepasselijke reglement een regeling hieromtrent te bevatten.'

passing is. De gegevens in de gewone politieregisters zijn in beginsel rechtmatig verkregen en kennen één en hetzelfde verstrekkingenregime. Dit verklaart een vrij verkeer van gegevens, waarbij het gebruik van gegevens uit een ander politieregister niet per definitie resulteert in een ontoelaatbare inbreuk op de privacy. Een verwerking in het kader van een ongericht dataminingonderzoek is mogelijk wanneer daarmee het van toepassing zijnde verstrekkingenregime niet wordt veranderd. Dat is anders wanneer het gaat om een koppeling met een gewoon politieregister met een afwijkend verstrekkingenregime, zoals het hulpverleningsregister of het register-MOT. In dat geval beperkt de functie van raadpleging van het basisregister de registratiefunctie, en daarmee de analysefunctie, daarvan.

#### *7.3.3.4 De aard van het ongerichte dataminingonderzoek*

De ongerichte dataminingvariant kenmerkt zich door een terughoudende opstelling wanneer het gaat om het gebruik van externe gegevens. Bij de verwerking van externe gegevens van buiten de politieke sfeer ligt daaraan vooral de bescherming van de persoonlijke levenssfeer ten grondslag. Bij de verwerking van externe gegevens die afkomstig zijn uit andere gewone politieregisters is in beginsel geen sprake van een ontoelaatbare inbreuk op de persoonlijke levenssfeer. Desondanks dient ook bij het gebruik van deze externe gegevens terughoudendheid te worden betracht. Daarbij heeft de aard van een ongericht dataminingonderzoek een beperkende invloed op de wijze, waarop gebruik kan worden gemaakt van gegevens in andere gewone politieregisters. Een volledige onderlinge koppeling van gewone politieregisters lijkt – noch vanuit praktisch, noch vanuit juridisch oogpunt – wenselijk. Aangezien een ongericht dataminingonderzoek in beginsel een permanent karakter heeft zou dat ook gelden voor een zodanige koppeling. Een volledige koppeling lijkt ook niet te passen binnen het streven om eventuele inbreuken op de persoonlijke levenssfeer tot een minimum te beperken. Met het oog op de mogelijkheden en de aard van een ongericht dataminingonderzoek is het verder de vraag in hoeverre het wenselijk is, dat de uitvoerder van het dataminingonderzoek het initiatief dient te nemen tot het vergaren van gegevens uit andere politieregisters. Het zelfstandig en actief verzamelen van gegevens uit andere politieregisters is niet altijd verenigbaar met het ongerichte karakter van het dataminingonderzoek, en evenmin met de voorwaarde dat het gebruik van de desbetreffende gegevens noodzakelijk dient te zijn voor het onderzoek.

Het gebruik van gegevens uit andere gewone politieregisters is ook mogelijk zonder dat de uitvoerder van het ongerichte dataminingonderzoek daartoe het initiatief neemt. Een verstrekking uit een ander politieregister kan tevens plaatsvinden op initiatief van de verstrekker. De uitvoerder van een ongericht dataminingonderzoek kan in beginsel niet op de hoogte zijn van alle eventueel bruikbare gegevens die in de politieregisters aanwezig zijn. Wanneer hij geen kennis heeft van het bestaan van bepaalde gegevens zal hij daar ook niet om verzoeken. Een verstrekking van gegevens op initiatief van de verstrekker kan daarom een belangrijke bijdrage leveren aan een ongericht dataminingonderzoek en aan de informatiepositie als geheel. De passieve rol die de uitvoerder van het onder-

zoek in dat geval vervult sluit goed aan op het karakter van een ongericht dataminingonderzoek. Het belang van een gegevensverstrekking zonder een daaraan ten grondslag liggend verzoek onderstreept de noodzaak van een goede samenwerking en informatie-uitwisseling, zowel binnen een politiekorps als tussen de verschillende korpsen onderling. Wanneer opsporingsdiensten (ten minste in grote lijnen) van elkaar weten waar men op een bepaald moment mee bezig is kan dat veel onnodig werk besparen en bijdragen aan een succesvolle uitvoering van opsporingstaak. Tot op zekere hoogte is men afhankelijk van de bereidheid van de beheerders van andere, gewone politieregisters om gegevens te verstrekken. Wanneer sprake is van een grootschalige informatiebehoefte, zoals bij het dataminingsproces het geval is, ligt het echter voor de hand gebruik te maken van een geautomatiseerde gegevensuitwisseling, bijvoorbeeld door middel van algemene informatiesystemen en zogenaamde ‘verwijsindexen’.

#### **Informatiesystemen en verwijsindexen**

Er bestaan verschillende gewone politieregisters die specifiek bedoeld zijn om bij te dragen aan een goede samenwerking op het gebied van informatiebeheer en -spreiding. Enkele voorbeelden daarvan zijn de registers van het Bedrijfsprocessensysteem, het Herkenningsdienstsysteem en het bestand Meldingen Districtelijke Recherche Onderzoeken. De twee eerstgenoemde registers zijn informatiesystemen en het laatste register is een verwijsindex. Deze politieregisters geven een centraal overzicht van de informatie die binnen het politieapparaat aanwezig is.

*Informatiesystemen* – Eén van de bij de politie in gebruik zijnde informatiesystemen is het Bedrijfsprocessensysteem (BPS). Het BPS is een (gewoon) politieregister dat een belangrijke functie vervult bij de uitvoering van de dagelijkse politietaak. Voorbeelden daarvan zijn de werkzaamheden van de surveillancedienst en het opmaken van een proces-verbaal (aangifte) bij melding van een mogelijk strafbaar feit. Met behulp van de informatie in een BPS kan na verloop van tijd onder meer een beeld worden verkregen waar, wanneer en mogelijk door wie, afwijkend gedrag wordt gepleegd. Zo kan efficiënter op bepaalde omstandigheden worden gereageerd en geanticipeerd.

Het Herkenningsdienstsysteem (HKS) is een landelijk dekkend systeem dat sinds 1986 door de politie wordt gebruikt voor het registreren van gegevens. Omdat de verschillende politieregio’s het systeem beheren is feitelijk sprake van meerdere systemen: voor elke politieregio en de Koninklijke Marechaussee (KMar) één. Het HKS bevat zowel de aangiftegegevens van misdrijven als de persoonsgegevens van de verdachten daarvan. Er kunnen personen vanaf 12 jaar in worden opgenomen, tegen wie als verdachte van een misdrijf proces-verbaal is opgemaakt. In beginsel wordt ieder proces-verbaal in het register opgenomen, hetgeen een continue registratie van feiten oplevert. Het HKS is een op zichzelf staand registratiesysteem. Informatie die in HKS wordt opgenomen registreert de politie ook in andere bedrijfsprocessensystemen. Het HKS bevat informatie over bijvoorbeeld het delict, het tijdstip waarop het gepleegd werd, de modus

operandi, maar ook persoonskenmerken van de verdachten zoals geboortedatum, geslacht, nationaliteit en eventuele aanwezigheid van verslavingsproblematiek. Het HKS wordt vooral gebruikt om na te gaan of personen eerder met de politie in aanraking zijn geweest. De algemene doelstelling van dit register is dan ook gerelateerd aan de herkenning van deze groep personen met het oog op de uitvoering van de politietaak, nu en in de toekomst.<sup>82</sup> Het HKS is het enige bestand dat positionele gegevens bevat van alle geregistreerde antecedenten van verdachten in Nederland. Dit biedt de mogelijkheid tot een waardevolle verdieping in informatie over verdachten, hetgeen dit register interessant maakt voor toepassing van het dataminingsproces.

*Verwijsindexen* – Naast de bedrijfsprocessensystemen wordt ook gebruik gemaakt van verwijsindexen. Met behulp daarvan kan het gezamenlijke gebruik van gegevens en de uitwisseling van gegevens binnen bijvoorbeeld de opsporingsinstanties worden vereenvoudigd<sup>83</sup>. Een verwijsindex geeft een overzicht van andere bestanden waarin – vooral gegevens over – een bepaalde persoon (of zaak) zijn opgenomen. Die gegevens zelf worden niet of zeer beperkt in de verwijsindex opgenomen. Op die manier kan een goed overzicht worden verkregen van de aanwezige informatie, zonder dat daarbij meteen de (gevoelige) informatie zelf hoeft te worden verwerkt.

Een voorbeeld van een verwijsindex is het bestand Meldingen Districtelijke Recherche-Onderzoeken (M(D)RO), dat een landelijk overzicht verschaft van de onderzoeken die de politie uitvoert. In een MRO-bestand worden alle onderzoeken geregistreerd die langer dan een week duren en gericht zijn op misdrijven waarvoor voorlopige hechtenis is toegelaten.<sup>84</sup> Het bestand heeft tot doel de informatievoorziening in het kader van de uitvoering van art. 2 Politiewet 1993 binnen het korps mogelijk te maken voor zover het gaat om het verkrijgen van inzicht in een rechercheonderzoek, dat in behandeling is bij een dienstonderdeel van het korps; het gaat daarbij om verdachten die betrokken zijn bij een rechercheonderzoek als bedoeld in de art. 126gg en 132a Sv. Op deze wijze kunnen verbanden worden onderkend met andere rechercheonderzoeken binnen het korps. Uit een MRO-bestand worden tevens de gegevens die daarvoor in aanmerking komen aan de Verwijzingsindex Recherche-Onderzoeken Subjecten (VROS) verstrekt.<sup>85</sup> De VROS is een programma dat de CIDSi vergelijkt met de MRO-bestanden, en de laatste onderling vergelijkt. De op deze wijze verkregen vergelijkingen worden zonder tussenkomst van personen naar de betrokken regio's gestuurd. Dit systeem functioneert alleen wanneer de regiokorpsen daaraan optimale medewerking verlenen.

---

82. *Kamerstukken II*, 1997/198, 25 398, nr. 6, p. 6.

83. *Kamerstukken II*, 2001/02, 26 269, nr. 46 (Uitvoering aanbevelingen enquêtecommissie opsporingsmethoden; Brief minister over de vulling van de Verwijsindex Recherche Onderzoeken en Subjecten (VROS)).

84. *Kamerstukken II*, 1998/199, 26 269, nrs. 4-5, p. 124. (Commissie-Kalsbeek)

85. Art. 2 Privacyreglement Meldingen Districtelijke Recherche-Onderzoeken (MRO).

Het gebruik van een overkoepelend informatiebeheer sluit in beginsel goed aan op het passieve karakter van een ongericht dataminingonderzoek. Door te koppelen met een centraal politieregister wordt de inbreuk op de persoonlijke levenssfeer beperkt. Bovendien is een koppeling met één centraal register veel efficiënter dan wanneer met alle mogelijk interessante informatie bevattende registers afzonderlijk dient te worden gekoppeld.<sup>86</sup> Aan de verwerking van de gegevens die via deze weg beschikbaar zijn dienen evenwel voorwaarden te worden verbonden.

#### **Beperkingen van overkoepelend informatiebeheer**

De besproken informatiesystemen en verwijzindexen worden aangemerkt als gewone politieregisters. Dit betekent dat eenieder binnen het politieapparaat in beginsel vrij over de gegevens in deze registers kan beschikken. Dit maakt het mogelijk om op een goede en vooral efficiënte manier uitvoering te geven aan de politietaak. In de overkoepelende informatiesystemen kunnen ook (kortstondig) gegevens worden opgeslagen die betrekking hebben op onverdachte personen, dan wel gegevens die eigenlijk thuishoren in een bijzonder politieregister. De registratie van dergelijke gegevens is normaliter voorbehouden aan de bijzondere politieregisters en slechts mogelijk voor een beperkt aantal doeleinden. In de praktijk blijkt het evenwel ook mogelijk om, onder bepaalde omstandigheden, dergelijke gegevens in een gewoon politieregister vast te leggen. Het is de vraag of het vastleggen van (verwijzingen naar) gevoelige en zelfs zachte gegevens in een gewoon politieregister wel in overeenstemming is met de systematiek van de WPolr. In het verlengde hiervan lijkt het gebruik van informatiesystemen en verwijzindexen in het kader van een ongericht dataminingonderzoek niet steeds vanzelfsprekend.

*Informatiesystemen en art. 5a WPolr* – Voor (de tijdelijke) opslag in een gewoon politieregister van gegevens die in een bijzonder politieregister thuishoren bestaan geen directe juridische belemmeringen. De MvT<sup>87</sup> stelt dat het mogelijk is om persoonsgegevens die voldoen aan de opslagcriteria voor een register zware criminaliteit of een voorlopig politieregister kortstondig te registreren in een gewoon politieregister. De juridische grondslag daarvoor is art. 5a WPolr. Daar wordt bepaald dat de registratie van onverdachte personen in een gewoon politieregister mogelijk is voor de duur van vier maanden. Art. 5a WPolr is erop gericht een doelmatige taakuitvoering van de politie mogelijk te maken.<sup>88</sup> Alle mutaties met mogelijke opsporingsrelevante informatie kunnen nu eenmaal niet meteen worden getoetst aan de criteria voor de bijzondere politieregisters. Bovendien wordt dergelijke informatie kort na de registratie vaak operationeel gecheckt, waarbij wordt nagegaan of er echt iets aan de hand is.

---

86. En waarnaar de desbetreffende verwijzindex verwijst.

87. *Kamerstukken II*, 1996/97, 25 398, nr. 3, p. 8 en *Kamerstukken II*, 1997/98, 25 398, nr. 6, p. 7.

88. *Kamerstukken I*, 1998/99, 25 398, nr. 63b, p. 4.

In beginsel kan in het kader van een ongericht dataminingonderzoek zonder problemen worden gekoppeld met een overkoepelend informatiesysteem dat is gebaseerd op art. 5a WPolr. Het doel noch de aard van het betreffende informatiesysteem zal een dergelijke handeling in de weg staan. Hoewel sprake kan zijn van een verwerking van gegevens die betrekking hebben op onverdachte personen leidt dit niet tot een ontoelaatbare inbreuk op de persoonlijke levenssfeer, gezien de wettelijke grondslag daarvoor in de vorm van art. 5a WPolr die deze inbreuk rechtvaardigt. Met behulp van een reglement kan tot op bepaalde hoogte worden voorzien in een afwijkend verstrekkingenregime. Op grond van art. 6 WPolr dient een koppeling namelijk in overeenstemming te zijn met het reglement van het register. Het privacyreglement van het BPS bestaat bijvoorbeeld uit verschillende modules. Ook met betrekking tot het raadplegen van informatiesystemen lijken geen aanvullende beperkingen te worden gesteld die samenhangen met de aard van de gegevens in deze registers. Op een verwerking van deze gegevens zijn dezelfde voorwaarden van toepassing als die welke voor de overige gewone politieregisters gelden.

*Verwijsindexen en dubbele registratie* – Een registratie van gegevens in een informatiesysteem op grond van art. 5a WPolr leidt niet per definitie tot een doorbreking van het beperkte verstrekkingenregime dat op de gegevens in de bijzondere politieregisters van toepassing is. Hier zij vooral gewezen op het feit dat de MvT spreekt over gegevens die kunnen worden opgeslagen in de bijzondere politieregisters, en niet over gegevens waar bij dat al daadwerkelijk het geval is. Echter, tips waarvan blijkt dat die direct voor registratie in een bijzonder politieregister in aanmerking komen, bijvoorbeeld ten behoeve van het afschermen van de identiteit van de tipgever, worden bij binnenkomst meteen geregistreerd in een gewoon politieregister. Wanneer een tipgever te kennen geeft dat zijn identiteit moet worden afgeschermd, zal hij in de regel worden doorverwezen naar de registerbeheerder van de bijzondere politieregisters<sup>89</sup>. Afscherming kan namelijk niet door de beheerder van het BPS worden geboden, tenzij gebruik gemaakt wordt van een voorziening op grond van het BPolr. Bij (tijdelijke) registratie van gegevens die ook in bijzondere politieregisters zijn opgeslagen is sprake is van een dubbele registratie, hetgeen wel een doorbreking van het beperkte verstrekkingenregime betekent. Met betrekking tot een verwijsindex kan dan ook de vraag worden gesteld of, en in hoeverre dat gewone politieregister gegevens mag bevatten die verwijzen naar gegevens in een register waarop een beperkt (en dus afwijkend) verstrekkingenregime van toepassing is. Het gaat er daarbij vooral om of met de aanleg van een verwijsindex een dubbele registratie zal ontstaan. Een registratie van zachte gegevens of gegevens die betrekking hebben op onverdachte personen is in beginsel voorbehouden aan de bijzondere politieregisters en voor een beperkt aantal doelstellingen. Om te voorkomen dat deze gegevens ook voor andere doeleinden worden verwerkt, is daarop een beperkt verstrekkingenregime van

---

89. *Handelingen II*, 1998/99, nr. 17, p. 1017-1019 (25 398).

toepassing. Een (dubbele) registratie van dergelijke gegevens in een gewoon politieregister, zoals een verwijsindex, is om die reden dan ook ongewenst. Daarnaast worden de gegevens voor een ander doel gebruikt dan waarvoor zij in eerste instantie zijn vastgelegd. Een verwijsindex dient in beginsel immers de algemene uitvoering van de politietoets, terwijl zachte gegevens slechts voor een beperkt aantal doeleinden (die een zodanige verwerking rechtvaardigen) mogen worden verwerkt.

Een registratie van zachte gegevens in een verwijsindex maakt het in theorie ook mogelijk om gegevens te vergelijken van, en kennis te vergaren over (grote groepen) personen ten aanzien waarvan geen feiten of omstandigheden bekend zijn dat zij zich bezighouden met strafbare feiten. Dit betekent dat er sprake is van een ingrijpende bevoegdheid, hetgeen noch in het kader van de uitvoering van de algemene politietoets, noch ten behoeve van een ongericht dataminingonderzoek is gerechtvaardigd.

Ten slotte is in verband met de bescherming van de persoonlijke levenssfeer het langdurig vastleggen van persoonsgegevens op grond van art. 4 WPolr slechts in beperkte gevallen toegestaan.<sup>90</sup> De duurzame opslag van gegevens ten behoeve van operationeel gebruik over personen ten aanzien van wie (slechts) een redelijk vermoeden bestaat dat zij betrokken zijn bij het beramen of plegen van strafbare feiten is alleen mogelijk, wanneer het gaat om misdrijven als bedoeld in de doelomschrijving van het register zware criminaliteit. Daarmee wordt een ondergrens gesteld aan de registratiebevoegdheid van de beheerder waar het gaat om de opslag van gegevens met het oog op de strafrechtelijke handhaving van de rechtsorde. Deze ondergrens wordt enerzijds bepaald door de kring van personen over wie gegevens mogen worden opgeslagen en anderzijds door het soort misdrijven (het moet gaan om zware criminaliteit). Deze nadere concretisering van het noodzakelijkheidsbegrip van art. 4 WPolr heeft een reflexwerking op de overige politieregisters die zijn aangelegd met het oog op de strafrechtelijke handhaving van de rechtsorde. De beheerder is niet meer vrij om gewone politieregisters aan te leggen met betrekking tot bovengenoemde categorie van 'aspirant'-verdachten, en evenmin ten aanzien van personen waarover nog minder aanwijzingen van betrokkenheid bij strafbare feiten bestaan.<sup>91</sup>

Aangezien een verwijsindex niet de gegevens zelf bevat maar enkel een verwijzing daarnaar kan de vraag worden gesteld, in hoeverre in dat kader kan worden gesproken van een dubbele registratie. Zo kan bepaalde informatie binnen de politie worden gecodeerd door gebruik te maken van (zaak)nummers in plaats van namen. Het gebruik van een verwijsindex is dus afhankelijk van de manier waarop aan de verwijzing wordt vormgegeven. Dat kan tot ongewenste situaties leiden, bijvoorbeeld in gevallen waarin het verstrekkingenregime van de WPolr een koppeling van een gewoon politieregister met een bijzonder politieregister in het kader van een ongericht dataminingonderzoek in de

---

90. *Kamerstukken II*, 1996/97, 25 398, nr. 3, p. 8.

91. *Kamerstukken II*, 1997/98, 25 398, nr. 6, p. 9.

weg staat. (De beperkende factor zal daarbij vaak het doel zijn waarvoor de gegevens mogen worden verwerkt.) Bij koppeling met een verwijsindex waarin gegevens zijn vastgelegd die betrekking hebben op de gegevens in het bijzondere politieregister waarmee niet rechtstreeks mocht worden gekoppeld, lijkt het verstrekkingenregime van de WPolr te worden omzeild. De gegevens in het bijzondere politieregister worden op deze wijze niet alleen beschikbaar, maar worden bovendien voor een ander doel verwerkt dan waarvoor zij in eerste instantie waren vastgelegd. Daarnaast kunnen bepaalde gegevens, of verwijzingen naar gegevens, betrekking hebben op onverdachte personen. Een verwerking van zodanige gegevens in het kader van een ongericht dataminingonderzoek dient in beginsel te worden aangemerkt als een ontoelaatbare inbreuk op de persoonlijke levenssfeer. Op grond van het feit dat een verwijsindex een overschrijding van de grenzen die de WPolr en het BPolr stelt mogelijk maakt, kan opslag van bepaalde gegevens daarin worden aangemerkt als een dubbele registratie.

Desondanks lijkt de toepassing van overkoepelend informatiebeheer in combinatie met dataminingstechnieken een krachtig instrument ter verkrijging en behoud van een goede informatiepositie. Ter verbetering van de informatiepositie van de politie als geheel is het wenselijk dat verwijsindexen ook gegevens bevatten die betrekking hebben op gegevens waarop normaliter een beperkt verstrekkingenregime van toepassing is. Juist voor het bereiken van de doelstellingen waartoe dergelijke zachte informatie wordt verwerkt, is een goede informatievoorziening onontbeerlijk. Tegelijkertijd dient zeer omzichtig met deze informatie te worden omgegaan, hetgeen op gespannen voet staat met het open karakter van een verwijsindex. Ter ondervanging van dat probleem kan worden gedacht aan verwijsindexen, die tevens verwijzen naar zachte opsporingsinformatie die binnen het politieapparaat aanwezig is. Ingeval van een match wordt, afhankelijk van de aard daarvan, informatie verstrekt aan de bevrager of aan de beheerder van de informatie waarmee de bevraging die match heeft opgeleverd. Een zodanig systeem voorziet in een optimaal gebruik van de aanwezige en verkregen informatie en waarborgt tegelijkertijd het verstrekkingenregime zoals dat is geregeld door de WPolr en het BPolr. Aan de gevolgen met betrekking tot de bescherming van de persoonlijke levenssfeer kan worden tegemoetgekomen in de reglementen van de registers die in het kader van het overkoepelende informatiebeheer worden gebruikt. Teneinde te voorzien in een beperkt verstrekkingenregime kan daarnaast worden gekozen voor kwalificatie van dergelijke registers als bijzonder politieregister.

#### *7.3.3.5 Weigering door de beheerder*

Bij een verstrekking van gegevens blijkt het begrip 'politietoek' een cruciale rol te spelen. In art. 14 sub *a* en *b* WPolr wordt bepaald, dat verstrekking plaatsvindt voor zover de ontvangers deze behoeven voor de vervulling van de politietoek. Deze ontvangers zijn de ambtenaren van de politie en de ambtenaren van de Koninklijke Marechaussee. Voor andere opsporingsambtenaren dan genoemd in art. 14 onder *a* en *b* WPolr geldt een regeling die een beperking van het verstrekkingenregime inhoudt<sup>92</sup>. De achtergrond voor

deze beperking zijn de verschillen tussen de opsporingsambtenaren met een algemene opsporingstaak, belast met de uitvoering van de politietaak van art. 2 Politiewet 1993, en opsporingsambtenaren<sup>93</sup> met beperktere taken en bevoegdheden. De betekenis van een 'vrij verkeer van gegevens' is mede afhankelijk van de status van degene die de gegevens ontvangt of daarom verzoekt.

Een beheerder van een politieregister is in beginsel niet bevoegd tot toetsing en eventuele weigering van een verzoek tot verstrekking, aangezien dat in strijd is met het beginsel van een vrij verkeer van gegevens binnen het politieapparaat. Een beheerder kan een verstrekking weigeren indien dat noodzakelijk is voor de goede uitvoering van de politietaak.<sup>94</sup> Op grond van art. 11 BPolr is een weigering mogelijk met het oog op de bescherming van politie-informanten en getuigen, of indien een verstrekking een direct gevaar oplevert voor de geregistreerde of voor derden. Daarnaast kan een verstrekking achterwege blijven indien aangenomen moet worden dat de gevraagde gegevens in alle redelijkheid en billijkheid niet benodigd, noodzakelijk of onvermijdelijk zijn in verband met de uitoefening van de taak waarvoor deze zijn gevraagd.<sup>95</sup> Een marginale toetsing door de verstrekker van gegevens past niet alleen in het grondrechtenbeschermende karakter van de WPolr, maar ligt tevens besloten in de algemene zorgplicht van de beheerder van een registratie zoals die is neergelegd in art. 7 WPolr.<sup>96</sup> Een noodzaak tot weigering op grond van de politietaak dient wel in concreto te worden aangetoond. Hierin spelen de bij de verstrekking met elkaar samenhangende eisen van proportionaliteit en subsidiariteit ook een rol. Eén en ander leidt ertoe dat een daadwerkelijke weigering tot verstrekking van gegevens zich nauwelijks voordoet.

### Resumerend

Ondanks een vrij verkeer van gegevens binnen het politieapparaat met betrekking tot de gegevens in de gewone politieregisters, dient bij het gebruik van deze gegevens ten behoeve van een ongericht dataminingonderzoek rekening te worden gehouden met enige beperkende factoren. Deze komen vooral voort uit de doelbinding, die in sterke mate wordt beïnvloed door de aard van de politietaak in het kader waarvan gegevens in eerste instantie zijn vastgelegd. Hoewel ook de beheerder van een politieregister in bepaalde gevallen een verstrekking in weg kan staan, is de impact van deze bevoegdheid in de praktijk erg klein. Van grotere betekenis is de terughoudendheid die bij de verwerking van externe gegevens dient te worden betracht. Met het oog op de persoonlijke levenssfeer en een zo efficiënt mogelijke invulling van de opsporingstaak gaat de voor-

---

92. *Kamerstukken II*, 1985/86, 19 589, nr. 3, p. 20.

93. Art. 142 Sv.

94. Art 11 lid 3 BPolr.

95. Art. 14 WPolr.

96. Aldus ook Van Ruth & Schreuders 2000.

keur uit naar een overkoepelend informatiebeheer. Daarbij dient het verstrekkingenregime van de WPolr en het BPolr gehandhaafd te blijven

#### *7.3.4 Het gebruik van gegevens uit een bijzonder politieregister*

In par. 3a WPolr is een regeling getroffen voor de bijzondere politieregisters<sup>97</sup> (het tijdelijke register, het voorlopige register en het register zware criminaliteit). Kenmerkend voor die registers is dat daarin voor een langere periode gevoelige en mogelijk onbetrouwbare opsporingsinformatie kan worden opgeslagen. Bij een verwerking van gegevens in het kader van de opsporingstaak dient sprake te zijn van een evenwicht tussen enerzijds een doelmatige uitvoering van de politietaak en anderzijds de bescherming van de persoonlijke levenssfeer. De noodzaak tot registratie van personen, los van de verdenking van een concreet strafbaar feit, moet de mogelijke inbreuk op de persoonlijke levenssfeer kunnen rechtvaardigen. Met het oog hierop beperkt par. 3a WPolr de mogelijkheden tot registratie en gebruik van zachte persoonsgegevens in verband met de strafrechtelijke handhaving van de rechtsorde. De bijzondere politieregisters kennen een beperkt verstrekkingenregime. Daarmee wordt de mogelijkheid voor het raadplegen van deze registers beperkt. Dit van de gewone politieregisters afwijkende verstrekkingenregime kan de mogelijkheid van registratie en verwerking van gegevens uit een bijzonder politieregister in een gewoon politieregister voor het analyseren van die gegevens in de weg staan. Dit is wellicht anders voor het register zware criminaliteit nu de gegevens in dat register deels zijn bestemd voor operationeel gebruik.

#### **Zachte gegevens**

Wanneer wordt overwogen om een register aan te leggen waarin met het oog op strafvorderlijke doeleinden persoonsgegevens worden opgenomen terwijl ten aanzien van de betrokken personen nog geen sprake is van een verdenking in de zin van art. 27 Sv, komen de bijzondere politieregisters in beeld. Die gegevens worden ook wel aangeduid als 'zachte gegevens'. In sectie 5.2.2.2 is stilgestaan bij de verwerking van zachte gegevens, ofwel gegevens over personen ten aanzien van wie (slechts) een redelijk vermoeden bestaat dat zij betrokken zijn bij het beramen of plegen van strafbare feiten, of personen ten aanzien van wie nog minder aanwijzingen van betrokkenheid bij strafbare feiten bestaan. De juistheid van deze informatie staat nog niet vast. De bepalingen met betrekking tot de bijzondere registers vormen een uitputtende regeling voor de opslag van dergelijke gegevens in die zin, dat zij niet structureel mogen worden opgeslagen in de overige (gewone) politieregisters. Langdurige registratie van zachte gegevens voor operationeel gebruik is alleen mogelijk in een register zware criminaliteit en slechts voor het specifieke doel van dat register.<sup>98</sup> Registratie van zachte gegevens (voor een ander

---

97. Zie ook *Rapport Evaluatie wet bijzondere politieregisters* 2004, p. 21-43.

98. Daarbij gaat het om de gegevens in art. 13a lid 1 onder b en c WPolr.

doel) is mogelijk in een voorlopig politieregister of een tijdelijk politieregister ten behoeve van een onderzoek naar een concreet voorgenomen of gepleegd strafbaar feit. Ten slotte kunnen zachte gegevens kortstondig worden geregistreerd in een gewoon politieregister als het BPS.

Met het oog op het zachte karakter van de gegevens in de bijzondere politieregisters en het type onderzoek waarvoor zij worden gebruikt, is daarop een afwijkend verstrekkingenregime van toepassing. De beperkte registratiemogelijkheid van zachte gegevens speelt een belangrijke rol bij de verdere verwerking van die gegevens in het kader van een dataminingonderzoek. Om te voorkomen dat de waarborgen van de regeling van de bijzondere politieregisters kunnen worden omzeild, bepaalt art. 13*d* lid 3 WPolr dat het vastleggen en gebruiken van persoonsgegevens voor de doeleinden van par. 3*a* WPolr alleen mogelijk is in overeenstemming met hetgeen par. 3*a* hieromtrent bepaalt. Uit par. 3*a* WPolr vloeit een aantal voorwaarden voort waarmee rekening dient te worden gehouden bij de verwerking van gegevens in de bijzondere politieregisters.

- De langdurige registratie van zachte persoonsgegevens is slechts mogelijk voor een beperkt aantal, nader in de wet omschreven doeleinden<sup>99</sup>.
- De aanleg van bijzondere politieregisters is slechts beperkt mogelijk<sup>100</sup>.
- De bijzondere registers kennen een beperkt verstrekkingenregime, dat afwijkt van het regime van de gewone politieregisters<sup>101</sup>.

Het valt op dat in par. 3*a* WPolr de nadruk ligt op de normering van de registratie van zachte gegevens en niet op de verwerking van de gegevens waarvan de registratie deel uitmaakt. Dit is waarschijnlijk een gevolg van het feit dat de WPolr en het BPolr zijn gebaseerd op de Wpr. In de Wpr lag de nadruk op het registreren van persoonsgegevens, terwijl de opvolger van de Wpr, de Wbp, op iedere vorm van gegevensverwerking ziet. De bescherming van de privacy blijft ook van belang wanneer eenmaal geregistreerde gegevens verder worden verwerkt. Aangezien de bestaande wet- en regelgeving voornamelijk voorwaarden stelt aan de registratie van zachte gegevens is het van belang, ook te voorzien in een regeling met betrekking tot de behandeling (verdere verwerking) van gegevens na registratie daarvan.

### **Koppeling registers van onverdachte personen**

In de registratie van zachte gegevens kan een nuancering worden aangebracht. Gegevens omtrent personen ten aanzien van wie (zelfs) nog geen redelijk vermoeden bestaat van

---

99. Art. 13*a* lid 1 en art. 13*b* lid 1 WPolr.

100. Art. 13*d* lid 1 WPolr.

101. Art. 13 lid 2, art. 13*a* lid 5 en art. 13*b* lid 2 WPolr.

betrokkenheid bij het beramen of plegen van strafbare feiten worden aangemerkt als gegevens omtrent onverdachte personen als bedoeld in art. 5a WPolr. Registratie is alleen mogelijk in een register zware criminaliteit (art. 13a sub c WPolr)<sup>102</sup>, een voorlopig politieregister, een tijdelijk politieregister, kortstondig in een gewoon politieregister als het BPS en, op grond van art. 5a lid 1 onder b WPolr, in het register-MOT.

In de Nota WES<sup>103</sup> wordt aangegeven dat er registers zijn, waarin gegevens als tips worden bijgehouden over burgers die niet als verdachte of als CIE-subject kunnen worden aangemerkt. Deze gegevens dienen te worden afgeschermd van andere registers. Het adagium 'if there is no crime, there is no investigation' impliceert, dat koppelingen van registers waarin onverdachte burgers zijn geregistreerd voor de politie niet zijn toegelaten. Dit leidt tot een compartimentering van registers voor zover het gaat om registraties van onverdachte burgers. De wetgeving voorziet niet in bevoegdheden die erop zijn gericht, deze compartimentering door een algemene registervergelijking te doorbreken. Met betrekking tot de verwerking van gegevens omtrent onverdachte personen geeft het CBP aan dat het mogelijk dient te zijn, deze registers op bepaalde individuele personen te bevragen. Dit is geen dataminingonderzoek, maar verificatie. Verder mag deze bevoegdheid niet worden gebruikt om bestanden te koppelen teneinde strafbare feiten boven water te halen waarvan op voorhand geen enkel vermoeden bestaat. Daarmee lijkt de mogelijkheid van dataminingonderzoek te worden uitgesloten.

Volgens de Nota moet evenwel worden onderzocht of de rechter-commissaris moet worden bevoegd om in zwaarwegende gevallen over te gaan tot een algemene vergelijking van registers van verdachte en niet verdachte burgers. Daarnaast geeft de wetgever aan dat in zeer ernstige zaken als de georganiseerde criminaliteit, volgens passende procedures, omvangrijke bestanden kunnen worden bevroegd en gekoppeld, ook wanneer deze zijn aangelegd voor geheel andere doeleinden. Daarmee wordt de mogelijkheid opengelaten om gegevens omtrent onverdachte personen te koppelen in het kader van een dataminingonderzoek. Bij 'passende procedures' gaat het in ieder geval om afscherming en specialiteit in die zin, dat de gegevens niet daarna voor andere onderzoeken kunnen worden gebruikt en, zodra mogelijk, moeten worden vernietigd. In dat kader kan gebruik worden gemaakt van een datawarehouse. Hoewel hiermee de mogelijkheid van een koppeling in beginsel wordt aanvaard, zijn er verschillende – met de huidige wet- en regelgeving samenhangende – factoren die van invloed zijn op de vraag, of een koppeling in een bepaald geval ook daadwerkelijk mogelijk is. Hierna wordt voor elk van de bijzondere

---

102. Anders in het *Rapport Gegevensuitwisseling en Terrorismebestrijding* 2003. Daarin worden de gegevens onder 13a lid 1 sub b WPolr eveneens aangemerkt als gegevens omtrent onverdachte personen. Deze subjecten vallen echter niet binnen de definitie van het begrip 'onverdachte personen' (*Kamerstukken I*, 1998/199, 25 398, nr. 63b, p. 6-7).

103. *Kamerstukken II*, 1997/198, 25 880, nrs. 1-2, p. 83.

politieregisters afzonderlijk onderzocht of deze gebruikt kunnen worden ten behoeve van een ongericht dataminingonderzoek ter verbetering van de informatiepositie van een gewoon politieregister.

#### *7.3.4.1 Het gebruik van een tijdelijk politieregister*

Een tijdelijk politieregister wordt aangelegd met het oog op de uitvoering van de politietoets in een bepaald geval of in het kader van een verkennend onderzoek. Een onderzoek dat ten grondslag ligt aan de aanleg van een tijdelijk register is in beginsel steeds gericht van aard. Er is een aantal factoren waarmee rekening dient te worden gehouden bij de vraag, of de gegevens in een tijdelijk politieregister in aanmerking komen voor het gebruik in het kader van een ongericht dataminingonderzoek met betrekking tot een gewoon politieregister. Daarbij gaat het om de doelbinding, de koppeling en de aard van het ongerichte dataminingonderzoek.

#### **De doelbinding**

Een tijdelijk politieregister wordt in beginsel steeds aangelegd in het kader van de politietoets voor zover het de strafrechtelijke handhaving van de rechtsorde betreft. Hoewel in zoverre geen beletsel bestaat voor het gebruik van dit register in het kader van een dataminingonderzoek, is een verstrekking uit een tijdelijk politieregister alleen mogelijk met het oog op het specifieke doel waarvoor dat register is aangelegd.<sup>104</sup> Bij een verstrekking aan een gewoon politieregister is hiervan geen sprake. Een gewoon politieregister dient een eigen doel, dat in beginsel afwijkt van dat van de tijdelijke politierregistere. Terwijl een gewoon politieregister de algemene politietoets dient, wordt een tijdelijk politieregister aangelegd voor de politietoets in een concreet geval. Op grond van art. 13 lid 2 WPolr lijkt een verstrekking aan een gewoon politieregister uitgesloten. Uitzondering op het beperkte verstrekkingenregime is alleen mogelijk bij een verstrekking ten behoeve van opname in een voorlopig politieregister en een register zware criminaliteit<sup>105</sup>, of indien uit de gegevens zelf een redelijk vermoeden voortvloeit dat een persoon een strafbaar feit heeft begaan.

*Art. 13d lid 3 WPolr* – Op grond van art. 13 lid 2 WPolr zou een verstrekking van gegevens uit een tijdelijk politieregister aan een gewoon politieregister in beginsel mogelijk zijn voor het doel, waarvoor ook het tijdelijke politieregister is aangelegd. Deze mogelijkheid wordt echter teniet gedaan door art. 13d lid 3 WPolr dat bepaalt, dat het vastleggen en gebruiken van gegevens voor de doeleinden van par. 3a WPolr slechts mogelijk is in overeenstemming met de in die sectie gestelde voorwaarden. Daarin wordt onder

---

104. Art. 13 lid 1 WPolr.

105. Op grond van art. 13 d lid 2 WPolr is een verstrekking eveneens mogelijk of wanneer uit de gegevens zelf een redelijk vermoeden voortvloeit dat een bepaalde persoon een strafbaar feit heeft begaan.

meer bepaald dat een verstrekking aan (en registratie in) een gewoon politieregister niet mogelijk is voor het doel waarvoor het tijdelijke politieregister is aangelegd. Op grond van art. 13*d* lid 3 dient in dat geval gebruik te worden gemaakt van een tijdelijk politieregister.

De gegevens die uit een tijdelijk politieregister worden verstrekt kunnen vervolgens elders worden geregistreerd; in de WPolr is geen afzonderlijke bepaling opgenomen die een dergelijke handeling in de weg staat. Dit is wel het geval voor een verstrekking van gegevens uit een voorlopig politieregister. In art. 13*b* lid 3 WPolr is bepaald, dat een zodanige verstrekking in beginsel niet in enig ander register wordt vastgelegd. Dit sluit naadloos aan op art. 13*d* lid 3 WPolr, waardoor een dergelijke regeling ook wenselijk lijkt voor het tijdelijke politieregister. Een aanvulling op dit punt komt de continuïteit en de duidelijkheid van de regeling van de WPolr en het BPolr ten goede.

*Initiatief verstrekking* – Het standpunt dat een registratie van gegevens (uit een tijdelijk politieregister) voor het doel waarvoor een tijdelijk politieregister is aangelegd in enig ander politieregister niet geoorloofd is, lijkt overeen te stemmen met art. 4 lid 2 BPolr. Daar is bepaald dat een tijdelijk politieregister slechts kan worden gekoppeld indien dat noodzakelijk is voor het doel van het tijdelijke politieregister. Hieruit kan worden afgeleid dat het initiatief tot een koppeling in beginsel steeds bij (de beheerder van) het tijdelijke politieregister berust. Daarvan is sprake wanneer een dataminingonderzoek betrekking heeft op een tijdelijk politieregister en niet bij een verstrekking van gegevens uit een tijdelijk politieregister ten behoeve van een ander dataminingonderzoek. Dit kan ook worden afgeleid uit de formulering van art. 13 WPolr. Uit een tijdelijk politieregister wordt in beginsel alleen verstrekt ter verrijking van al opgeslagen gegevens, of voor het specifieke doel waarvoor het tijdelijke politieregister in het leven is geroepen. Het initiatief voor een verstrekking ligt dan bij het tijdelijke politieregister, terwijl het initiatief bij het ongerichte dataminingonderzoek uitgaat van een gewoon politieregister. Wanneer een verstrekking alleen kan plaatsvinden op initiatief van de beheerder van het tijdelijke politieregister is ‘het gebruik’ van gegevens uit dat register ten behoeve van een ongericht dataminingonderzoek alleen al om die reden niet mogelijk.

*Art. 4 lid 2 WPolr* – Het gebruik van gegevens uit een tijdelijk politieregister in het kader van een ongericht dataminingonderzoek met betrekking tot een gewoon politieregister resulteert in een registratie van persoonsgegevens uit het tijdelijke politieregister in het gewone politieregister (basisregister). In art. 4 lid 2 WPolr is bepaald dat die registratie noodzakelijk dient te zijn voor het doel het gewone politieregister (of voor het ongerichte dataminingonderzoek). Vanwege de verschillende doelstellingen waarvoor de betrokken politieregisters (kunnen) worden aangelegd, zal van een zodanige noodzaak in beginsel geen sprake zijn.

### Koppeling

In het geval van een koppeling dient rekening te worden gehouden met de verstrekkingenregimes van de betrokken registers en het bepaalde in art. 5*a* en 13*d* lid 3 WPolr.<sup>106</sup> Het verstrekkingenregime van een tijdelijk politieregister beperkt de mogelijkheid om met dit register te koppelen. Op grond van art. 4 lid 2 BPolr dient een koppeling van een tijdelijk register met een ander register noodzakelijk te zijn voor het doel waarvoor het tijdelijke register is aangelegd. Het ongerichte dataminingonderzoek, en daarmee de koppeling, vindt plaats ten behoeve van een verbetering van de informatiepositie van een gewoon politieregister. Dit is in beginsel niet noodzakelijk voor (de informatiepositie van) een tijdelijk politieregister. Een koppeling lijkt dan ook niet mogelijk.

Een verwerking van gegevens omtrent onverdachte personen in een tijdelijk politieregister is in beginsel slechts mogelijk in het kader van een onderzoek dat is gelieerd aan de bestrijding van de zware criminaliteit. Aangezien een koppeling met een tijdelijk politieregister op grond van art. 4 lid 2 BPolr noodzakelijk dient te zijn voor het doel van het tijdelijke register, zal een koppeling van onverdachte gegevens in een tijdelijk politieregister slechts plaatsvinden ter bestrijding van de zware criminaliteit.<sup>107</sup> In dat geval is het weliswaar denkbaar dat met andere bijzondere politieregisters wordt gekoppeld, maar een koppeling met een gewoon politieregister is onwaarschijnlijk. Ook het bepaalde in art. 5*a* WPolr staat de registratie van gegevens over onverdachte personen in een gewoon politieregister in de weg. Het artikel beoogt een grens te stellen aan het gebruik van zachte informatie in verband met de uitvoering van de politietaak in het kader van de strafrechtelijke handhaving van de rechtsorde. Het bepaalde in art. 5*a* WPolr biedt in beginsel ook geen ruimte om in het kader van een ongericht dataminingonderzoek gegevens uit een tijdelijk politieregister tijdelijk te registreren in een gewoon politieregister (voor de duur van vier maanden)<sup>108</sup>. Het gaat hier immers niet om nieuw binnengekomen gegevens, maar om gegevens die reeds in een tijdelijk politieregister zijn geregistreerd.

Art. 6 lid 2 WPolr stelt dat een koppeling in beginsel slechts mogelijk is indien en voor zover het reglement dat bepaalt. Ingeval van een koppeling van een politieregister met een tijdelijk politieregister behoeft enkel het reglement van het gewone politieregister te voorzien in een mogelijkheid tot de koppeling.

---

106. *Kamerstukken I*, 1998/99, 25 398, nr. 63*b*, p. 8.

107. *Kamerstukken II*, 1996/97, 25 398, nr. 3, p. 8.

108. Zie ook sectie 5.2.2.2.

### **De aard van het ongerichte dataminingonderzoek**

Een tijdelijk politieregister biedt de mogelijkheid tot de registratie van zachte gegevens, hetgeen één van de redenen is voor het afwijkende verstrekkingenregime van dit register. Indien in het kader van een verbetering van de informatiepositie van een gewoon politieregister gebruik wordt gemaakt van gegevens uit een tijdelijk politieregister kan dit een ontoelaatbare inbreuk op de persoonlijke levenssfeer impliceren, hetgeen niet is toegestaan. Op de gegevens in een tijdelijk politieregister is immers een afwijkend verstrekkingenregime van toepassing, hetgeen het ter raadpleging vastleggen van gegevens uit dit register in een gewoon politieregister in de weg staat. Noch het doel van het ongerichte dataminingonderzoek, noch het verstrekkingenregime dat op het gewone politieregister van toepassing is, kunnen de verwerking van zachte gegevens rechtvaardigen.

### **Resumerend**

Ten behoeve van een ongericht dataminingonderzoek met betrekking tot een gewoon politieregister kan geen gebruik worden gemaakt van gegevens uit een tijdelijk politieregister. Het afwijkende verstrekkingenregime van de bijzondere politieregisters speelt hierbij een doorslaggevende rol. Het gebruik van de gegevens in deze registers wordt met name beperkt door het doelbindingsbeginsel. Op grond daarvan is een verstrekking van gegevens uit een tijdelijk politieregister aan een gewoon politieregister niet mogelijk. Ook de voorwaarden die op een koppeling van toepassing zijn staan het gebruik van gegevens uit een tijdelijk politieregister in de weg.

#### *7.3.4.2 Het gebruik van een voorlopig politieregister*

Het tweede bijzondere politieregister dat is onderzocht op het gebruik ten behoeve van een ongericht dataminingonderzoek is het voorlopige politieregister. Dit politieregister wordt aangelegd voor de opslag van gegevens ten aanzien waarvan moet worden vastgesteld of een geregistreerde, in samenhang met andere gegevens, kan worden opgenomen in het register zware criminaliteit.<sup>109</sup> Het register heeft daarmee een duidelijk afgebakende doelstelling. Evenals het tijdelijke politieregister kent een voorlopig register een beperkt verstrekkingenregime. De mogelijkheid om de gegevens in dit bijzondere politieregister verder te verwerken wordt beperkt door factoren als de doelbinding, de koppeling en de aard van een ongericht dataminingonderzoek.

### **Doelbinding**

Uit een voorlopig politieregister vindt in beginsel alleen verstrekking plaats ten behoeve van het doel waarvoor het is aangelegd en voor zover de gegevens benodigd zijn ter identificatie. Hierbij kan het gaan om een verstrekking ten behoeve van de verrijking van gegevens die al in het voorlopige register aanwezig zijn. Ook een voorlopig register kent

---

109. Art. 1 lid onder l WPolr.

enkele uitzonderingen op het verstrekkingenregime. Zo is verstrekking mogelijk ten behoeve van de opname in een ander bijzonder politieregister of ten behoeve van het Meldpunt, bedoeld in art. 2 Wet MOT.<sup>110</sup> Gegevens uit een voorlopig register kunnen ook worden verstrekt indien uit de gegevens zelf een redelijk vermoeden voortvloeit dat een persoon een strafbaar feit heeft begaan. In het kader van dit onderzoek gaat het om de vraag, of gegevens uit een voorlopig register mogen worden gebruikt ten behoeve van een ongericht dataminingonderzoek waarmee de verbetering van de informatiepositie van een gewoon politieregister wordt nagestreefd. Met het oog op art. 13*b* lid 2 WPolr lijkt dit niet mogelijk aangezien in beginsel niet wordt voldaan aan het doelbindingsbeginsel van een voorlopig politieregister. Uit de formulering van art. 13*b* lid 2 WPolr kan ook worden afgeleid, dat het initiatief voor een verstrekking bij de beheerder van het voorlopige politieregister ligt en niet bij de beheerder van het verzoekende, gewone politieregister. Dat impliceert dat een verzoek tot het gebruik van gegevens uit een voorlopig politieregister niet door een derde kan worden gedaan. Uitzondering daarop is een verstrekking aan het Meldpunt.

*Art. 4 lid 2, 13*b* lid 3 en 13*d* lid 3 WPolr* – In het kader van de doelbinding zij ook gewezen op de art. 4 lid 2, 13*b* lid 3 en 13*d* lid 3 WPolr. Het gebruik van gegevens uit een voorlopig politieregister in het kader van een ongericht dataminingonderzoek met betrekking tot een gewoon politieregister resulteert in een registratie van persoonsgegevens uit het voorlopige politieregister in een gewoon politieregister (basisregister). De genoemde artikelen staan dat in de weg. In art. 4 lid 2 WPolr is bepaald dat een zodanige registratie noodzakelijk dient te zijn voor het doel het gewone politieregister (of voor het ongerichte dataminingonderzoek). Vanwege de verschillende doelstellingen waarvoor de betrokken politieregisters (kunnen) worden aangelegd is daarvan in beginsel geen sprake. Een dergelijke registratie gaat ook niet samen met art. 13*b* lid 3 WPolr, waar wordt bepaald dat een verstrekking uit een voorlopig politieregister, anders dan aan een bijzonder politieregister of aan het Meldpunt, niet in enig ander register wordt vastgelegd. Tot slot is het denkbaar dat een verstrekking van gegevens uit een voorlopig politieregister plaatsvindt voor het doel waarvoor het voorlopig politieregister is aangelegd. In dat geval staat niet art. 13*b* lid 2 WPolr in de weg aan een verstrekking maar het bepaalde in 13*d* lid 3 WPolr. Op grond daarvan vindt de registratie van persoonsgegevens voor de doeleinden van de bijzondere politieregisters slechts plaats in overeenstemming met par. 3*a* WPolr. Dit betekent dat gegevens in een voorlopig politieregister niet voor dat doel mogen worden vastgelegd in een gewoon politieregister.

---

110. Art. 13*b* lid 2 WPolr.

### Koppeling

Bij het gebruik van gegevens uit een voorlopig register ten behoeve van een ongericht dataminingonderzoek zal sprake zijn van een koppeling. Een dergelijke koppeling is om twee redenen niet mogelijk. In de eerste plaats laat het verstrekkingenregime van het voorlopige register een koppeling met andere dan de bijzondere politieregisters niet toe; verstrekking ingevolge de koppeling zou betekenen dat gegevens worden verstrekt zonder dat tevoren duidelijk is dat meer informatie over de geregistreerde personen kan worden verkregen om te bepalen, of dezen kunnen worden opgenomen in het register zware criminaliteit.<sup>111</sup> In de tweede plaats wordt niet voldaan aan de voorwaarde van art. 6 lid 2 WPolr, op grond waarvan de reglementen van de betrokken registers in de mogelijkheid van een koppeling dienen te voorzien.

*Modelreglement voorlopig politieregister* – Bij een koppeling van twee politieregisters geldt de voorwaarde van reglementering voor beide te koppelen registers. In art. 14 van het modelreglement<sup>112</sup> van een voorlopig politieregister wordt met betrekking tot koppeling en verbanden met andere gegevensverzamelingen bepaald, dat een koppeling van het (voorlopig) register met een ander politieregister of een register als bedoeld in art. 17 aanhef en onder a Wpr, kan plaatsvinden voor zover dat noodzakelijk is voor het doel van het register, en het andere bijzondere politieregisters betreft. Hiermee wordt nogmaals het belang van de doelbinding bevestigd. Het is niet direct duidelijk of deze regeling cumulatief of alternatief is. In de toelichting op het modelreglement wordt namelijk opgemerkt:

*‘Deze regeling hangt samen met het feit dat koppeling juridisch gezien verstrekkingen met zich mee brengt. Een koppeling voor een ander doel zou dus in strijd zijn met de algemene regel dat uit het register slechts gegevens mogen worden verstrekt ten behoeve van het doel van het register. Daarnaast kan slechts koppeling plaats vinden voorzover dit in overeenstemming is met het stringente verstrekkingenregime dat wettelijk van toepassing is op het voorlopig register. In de praktijk zal dat betekenen dat slechts koppeling kan plaatsvinden met andere voorlopige registers en registers zware criminaliteit.’*

De beperkte mogelijkheid tot koppeling is gebaseerd op twee uitgangspunten. Ten eerste wordt ervan uitgegaan dat een verstrekking in het kader van een koppeling alleen is toegestaan ten behoeve van het doel van het voorlopige politieregister. Verstrekking uit een voorlopig politieregister is echter ook mogelijk ten behoeve van opname in een ander bijzonder register of ten behoeve van het Meldpunt. De tweede reden om een koppeling te beperken tot andere voorlopige registers en registers zware criminaliteit heeft volgens de

---

111. *Kamerstukken I*, 1998/99, 25 398, nr. 63b, p. 8.

112. Model privacyreglement voorlopig register, *Stert.* 12 oktober 2000, nr. 198, p. 17.

toelichting betrekking op het verstrekkingenregime van een voorlopig politieregister. Een koppeling mag slechts plaatsvinden in overeenstemming met het stringente verstrekkingenregime van het voorlopige politieregister. Aangezien het register-MOT een beperkt verstrekkingenregime heeft, zal een verstrekking aan dit register bijvoorbeeld gewoon mogelijk zijn. Een uitleg waarbij ervan wordt uitgegaan dat een voorlopig politieregister alleen kan worden gekoppeld met andere voorlopige registers en registers zware criminaliteit lijkt met het oog op het voorgaande onjuist. Dat zou namelijk betekenen dat het modelreglement van een voorlopig politieregister op het punt van koppeling strenger is dan op grond van het verstrekkingenregime van het register noodzakelijk. Een alternatieve uitleg van art. 14 van het modelreglement ligt daarom voor de hand, maar het reglement van een voorlopig politieregister maakt in dat geval een ruimere koppeling mogelijk dan op grond van het verstrekkingenregime<sup>113</sup> van art. 13*b* WPolr is toegestaan. Dat reglement bepaalt namelijk dat een koppeling ook mogelijk is met een ander politieregister of een register als bedoeld in art. 17, aanhef en onder *a* Wpr voor zover noodzakelijk voor het doel van het voorlopige register. Op grond van art. 13*b* lid 2 WPolr mogen echter uitsluitend voor identificatie benodigde gegevens worden verstrekt. Bovendien bepaalt art. 13*b* lid 3 WPolr dat de verstrekte gegevens niet in enig ander register mogen worden vastgelegd. Op grond daarvan is de koppelingsregeling van het reglement slechts in overeenstemming met de WPolr, indien de koppeling uitgaat van het voorlopige politieregister. Wanneer in het kader van een koppeling wordt verstrekt uit een voorlopig politieregister aan een ander register, niet zijnde een bijzonder register of register-MOT, is het reglement te ruim geformuleerd en is een verstrekking in het kader van een koppeling niet mogelijk. Het reglement staat hier dus een koppeling met een gewoon politieregister in de weg. Een zodanige koppeling zal niet noodzakelijk zijn voor het voorlopige politieregister, aangezien deze plaatsvindt ter verbetering van de informatiepositie van een gewoon politieregister. Voorts leidt een verstrekking aan een gewoon politieregister in het kader van een ongericht dataminingonderzoek tot het vastleggen van gegevens uit een voorlopig register in een gewoon politieregister. Daarmee wordt het verstrekkingenregime van de verstrekte gegevens uit het voorlopige register niet langer gehandhaafd. Bovendien bepaalt art. 13*b* lid 3 WPolr dat de verstrekte gegevens niet in enig ander register mogen worden vastgelegd.

*Register-MOT als bijzonder politieregister?* – Uit de MvT<sup>114</sup> bij de bijzondere politieregisters blijkt, dat de gegevens die nog niet voor opslag in het register zware criminaliteit in aanmerking komen vanwege de onzekere aard van de informatie niet mogen worden verstrekt met het oog op de uitvoering van enige politietaak. Alleen met het oog op de verkrijging van aanvullende informatie is een verstrekking mogelijk. Met betrekking tot het

---

113. Een koppeling is een vorm van verstrekken.

114. *Kamerstukken II*, 1996/97, 25 398, nr. 3, p. 19-20.

verstrekkingenregime van het voorlopige register geeft de wetgever aan dat de gegevens niet operationeel kunnen worden gebruikt in die zin, dat opsporingsbevoegdheden worden aangewend tot nadere informatie-inwinning of dat betrokkene in zijn contacten met de politie anders wordt bejegend. Wel kunnen de gegevens worden vergeleken met gegevens uit andere bijzondere politieregisters. De reden hiervoor is waarschijnlijk dat een koppeling van gegevens omtrent onverdachte personen in beginsel slechts mogelijk is voor de bestrijding van de zware criminaliteit, in het kader waarvan in beginsel alleen gebruik mag worden gemaakt van bijzondere politieregisters. Hoewel het register-MOT een gewoon politieregister is, ziet het ook op de bestrijding van zware criminaliteit. Een koppeling met dat register is daarom weinig bezwaarlijk, maar kan wel reden zijn om het te kwalificeren als een bijzonder politieregister.

#### **De aard van het ongerichte dataminingonderzoek**

Gegevens in een voorlopig politieregister kunnen betrekking hebben op onschuldige personen. Dit betekent dat zeer zorgvuldig met deze gegevens dient te worden omgegaan. Louter en alleen door het opslaan van zachte gegevens over bepaalde personen in politieregisters worden de personen op wie de gegevens betrekking hebben onderwerp gemaakt van politieke activiteiten. Een onderzoek met betrekking tot onschuldige personen impliceert, evenals de opslag van gegevens omtrent die personen, een vergaande inbreuk op de persoonlijke levenssfeer. Dit is alleen gerechtvaardigd indien het doel van het inbreukmakende onderzoek opweegt tegen de ernst van de inbreuk. Uit een voorlopig register worden geen gegevens verstrekt voor operationeel gebruik. De gegevens in een voorlopig politieregister voldoen namelijk nog niet aan het criterium voor het register zware criminaliteit. De waarborgen ter bescherming van de persoonlijke levenssfeer worden in dit geval niet zozeer gevonden in de criteria die de opslag van gegevens betreffen (het doel van het register biedt daarvoor onvoldoende houvast), maar vinden uitwerking in het zeer beperkte verstrekkingenregime dat voor het voorlopige register geldt.<sup>115</sup> Een dergelijk beperkt verstrekkingenregime ontbreekt bij de gewone politieregisters. Een verstrekking uit een voorlopig politieregister aan een gewoon politieregister in het kader van een ongericht dataminingonderzoek zal resulteren in een (duurzame) opslag van de verstrekte gegevens in het laatstgenoemde register. Het verstrekkingenregime van een gewoon politieregister zorgt ervoor dat de verstrekte gegevens ook voor operationeel gebruik in aanmerking komen. Of sprake is van een opslag van gegevens voor operationeel gebruik is afhankelijk van de vraag in hoeverre deze vrij binnen het politieapparaat beschikbaar zijn, hetzij direct, hetzij indirect. In dit geval gaat het om een verstrekking aan een gewoon politieregister in het kader van een ongericht dataminingonderzoek en zullen de gegevens dus geschikt zijn voor operationeel gebruik. Zelfs wanneer de ver-

---

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

streckte gegevens in eerste instantie niet direct beschikbaar zijn, zal het resultaat van het ongerichte dataminingonderzoek uiteindelijk ten goede komen aan het basisregister.

Het gebruik van gegevens ter verbetering van de informatiepositie van een gewoon politieregister vormt geen rechtvaardiging voor de inbreuk op de persoonlijke levenssfeer die daarvan het gevolg is. Daarbij wordt het verstrekkingenregime met een verstrekking uit een voorlopig politieregister aan een gewoon politieregister doorbroken. Wanneer de privacy van de in een voorlopig politieregister geregistreerde personen niet meer voldoende kan worden gewaarborgd is sprake van een ontoelaatbare inbreuk op de persoonlijke levenssfeer, hetgeen in het kader van een ongericht dataminingonderzoek niet is toegestaan.

### Resumerend

Een verstrekking van gegevens uit een voorlopig register aan een gewoon politieregister zal alleen mogelijk zijn, wanneer het gewone politieregister een register-MOT betreft. In andere gevallen is een verstrekking uit een voorlopig politieregister uitgesloten, hetgeen met name kan worden toegeschreven aan de functie die een voorlopig politieregister vervult als voorportaalregister van het register zware criminaliteit. De mogelijkheid tot de registratie van zachte gegevens is in beginsel voorbehouden aan de bijzondere politieregisters. Ook is het doel van een voorlopig politieregister moeilijk verenigbaar met het doel van een ongericht dataminingonderzoek waarbij wordt gestreefd naar een verbetering van de informatiepositie van een (gewoon) politieregister. Opvallend is dat ook het modelreglement van een voorlopig politieregister de mogelijkheid van een koppeling met een gewoon politieregister uitsluit.

#### *7.3.4.3 Het gebruik van het register zware criminaliteit*

Het derde en laatste bijzondere politieregister dat is onderzocht op de mogelijkheid van het gebruik van de daarin opgeslagen gegevens in het kader van een ongericht dataminingonderzoek, is het register zware criminaliteit. In beginsel worden alle gegevens met betrekking tot de misdrijven die zijn genoemd in art. 1 onder *k* WPolr opgenomen in dat register.<sup>116</sup> Met betrekking tot de content van een register zware criminaliteit maakt de WPolr een onderscheid naar gegevens met betrekking tot:

- 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 beramen of plegen van misdrijven als bedoeld onder *a*;
- c. personen die in een bepaalde relatie staan tot degenen, bedoeld onder *a* en *b*.<sup>117</sup>

---

116. *Kamerstukken II*, 1997/98, 25 398, nr. 6, p. 10.

*Gegevens categorieën A en B* – De gegevens die tot categorie *a* worden gerekend hebben betrekking op personen die verdacht worden van misdrijven, waarvoor een register zware criminaliteit is aangelegd. De informatie daaromtrent kan in beginsel als betrouwbaar worden aangemerkt. Dat geldt in mindere mate voor de gegevens die behoren tot categorie *b*, waarbij het gaat om personen ten aanzien van wie een redelijk vermoeden bestaat dat zij betrokken zijn bij het beramen of plegen van misdrijven als bedoeld onder *a*. De gegevens in categorie *b* zijn zachte gegevens. Dit brengt nadere beperkingen met zich mee aan de opslag en het gebruik van die persoonsgegevens in het kader van de politietoek, voor zover het gaat om de strafrechtelijke handhaving van de rechtsorde. In tegenstelling tot de overige bijzondere politieregisters<sup>118</sup> kent het register zware criminaliteit een open verstrekkingenregime voor zover het gegevens betreft die vallen onder de categorieën *a* en *b*. Terwijl uit de overige bijzondere politieregisters in beginsel alleen mag worden verstrekt voor het doel waarvoor die registers zijn aangelegd, ontbeert het verstrekkingenregime van een register zware criminaliteit een zodanige beperking. De criteria voor het opnemen van gegevens in een register zware criminaliteit zijn duidelijk vastgelegd en hebben betrekking op een bepaalde mate van betrokkenheid bij het beramen of plegen van strafbare feiten. Gegevens over de in dit register opgenomen subjecten kunnen meer algemeen binnen de politie worden gebruikt.<sup>119</sup> Het verstrekkingenregime van het register zware criminaliteit wijkt in zoverre af van het regime voor de gewone politieregisters, dat binnen het politieveld de mogelijkheid bestaat om verstrekking te weigeren wegens de politieke taakuitvoering. Er is geen grond om binnen de politie een verstrekking te weigeren wegens mogelijke aantasting van de persoonlijke levenssfeer.<sup>120</sup> Bij de verstrekking aan derden geldt verder dat de kring van personen aan wie gegevens verstrekt kunnen worden beperkter is dan die voor verstrekkingen uit de gewone politieregisters. In dit verband zij opgemerkt, dat in de praktijk sowieso terughoudend wordt omgegaan met de verstrekking van gegevens uit een register zware criminaliteit.<sup>121</sup>

*Gegevens categorie C* – De gegevens in categorie *c* van een register zware criminaliteit hebben in beginsel betrekking op onverdachte personen. De reden voor registratie in dat register is, dat zij in een bepaalde relatie staan tot personen die voldoen aan het opslagcriterium voor het register zware criminaliteit. Het gaat daarbij om contacten, getuigen,

---

117. De WPoR onderscheidt ook nog een vierde categorie, inhoudende ambtenaren van politie, van de Koninklijke marechaussee of van een publiekrechtelijk lichaam als bedoeld in art. 13c WPoR, voor zover dit van belang is voor het gebruik van de gegevens, bedoeld onder *a* tot en met *c*, alsmede voor de verantwoording van de verrichtingen naar aanleiding van de opgenomen gegevens. Omdat deze categorie voor dit onderzoek niet direct van belang is, blijft zij hier buiten beschouwing.

118. Art. 13 lid 1 en 13b lid 1 WPoR.

119. *Kamerstukken II*, 1997/98, 25 398, nr. 6, p. 5.

120. *Kamerstukken II*, 1997/98, 25 398, nr. 3, p. 54.

121. *Rapport Gegevensuitwisseling en Terrorismebestrijding* 2003, actiepunten 43 van het Actieplan Terrorismebestrijding en Veiligheid, p. 12.

informanten, aangevers en slachtoffers. Het is technisch mogelijk om uit een register zware criminaliteit afzonderlijk gegevens te verstrekken over deze categorie van personen. Een verstrekking voor operationeel gebruik is onwenselijk, omdat het aanknopingspunt voor een verstrekking uit dit register dient te zijn dat een persoon voldoet aan een criterium op grond waarvan een gericht politieoptreden gerechtvaardigd is. Dit is (nog) niet geval bij personen die in een bepaalde relatie staan tot degenen die als zelfstandig subject zijn opgenomen in het register zware criminaliteit.<sup>122</sup> Daarom is deze categorie gegevens niet geschikt voor operationeel gebruik. In art. 13*a* lid WPolr is bepaald dat het verstrekkingenregime van het voorlopige politieregister, dat is neergelegd in art. 13*b* lid 2 WPolr, van toepassing is op deze gegevens. Deze worden in beginsel alleen verstrekt ter bestrijding van de zware criminaliteit (overeenkomstig het doel waarvoor het register is aangelegd) en dan slechts voor zover zij nodig zijn ter identificatie. Voorts is verstrekking mogelijk ten behoeve van opname in een ander bijzonder politieregister of van een register-MOT. In die gevallen dient de verstrekking wel in overeenstemming te zijn met het doel van die registers.<sup>123</sup> In alle andere gevallen is een verstrekking van gegevens die behoren tot categorie *c* niet toegestaan.<sup>124</sup> Hoewel de gegevens in een register zware criminaliteit in principe zijn bestemd voor operationeel gebruik bestaan ook in dat verband beperkende factoren ten aanzien van het gebruik daarvan. Gedacht kan worden aan de doelbinding, de koppelingsregeling, de aard van het ongerichte dataminingonderzoek en de bevoegdheid van een beheerder om een verstrekking te weigeren. In het hierna volgende wordt ingegaan op de vraag, in hoeverre deze factoren van invloed zijn op het gebruik van gegevens uit een register zware criminaliteit ten behoeve van een ongericht dataminingonderzoek met betrekking tot een gewoon politieregister.

### De doelbinding

Een verstrekking van gegevens uit een register zware criminaliteit lijkt in beginsel geen relaties te hebben met het doel van het register. In art. 13*a* WPolr worden geen beperkingen gesteld aan de doeleinden waarvoor de gegevens in een register zware criminaliteit mogen worden verstrekt. De gegevens zijn geschikt voor operationeel gebruik.

*Art. 13*d* lid 3 en 13*a* lid 7 WPolr* – Een verstrekking van gegevens uit een register zware criminaliteit in het kader van een ongericht dataminingonderzoek ten behoeve van een gewoon politieregister resulteert in een registratie van de verstrekte gegevens in het gewone politieregister. Daarom dient rekening te worden gehouden met het bepaalde in art. 13*d* lid 3 WPolr. Persoonsgegevens die worden vastgelegd voor de doeleinden bedoeld in par. 3*a* WPolr mogen alleen worden vastgelegd en gebruikt overeenkomstig

---

122. *Kamerstukken II*, 1996/97, 25 398, nr. 3, p. 19.

123. *Kamerstukken II*, 1996/97, 25 398, nr. 3, p. 15.

124. Art. 13*b* lid 2 WPolr.

het in par. 3a WPolr bepaalde. Dit betekent dat een verstrekking uit een register zware criminaliteit aan een gewoon politieregister voor een van de doelstellingen van par. 3a WPolr niet mogelijk is. Bij een verstrekking van gegevens uit een register zware criminaliteit voor een ander doel is art. 13d lid 3 WPolr niet van toepassing. Het bepaalde in art. 13d lid 3 WPolr staat een verstrekking van gegevens in een register zware criminaliteit voor andere doeleinden dan genoemd in par. 3a WPolr niet in de weg. Een verstrekking aan en registratie in een gewoon politieregister zal dus mogelijk zijn.

De constatering dat de registratie van gegevens voor het doel van een register zware criminaliteit in een gewoon politieregister op grond van art. 13d lid 3 WPolr niet mogelijk is, lijkt te worden bevestigd door de uitzonderingsregeling van art. 13a lid 7 WPolr. Het zevende lid maakt het mogelijk om gegevens uit een register zware criminaliteit te registreren in bijvoorbeeld het opsporingsregister (OPS) of het HKS. Het HKS wordt veel gebruikt bij de dagelijkse uitvoering van de politietaak en kan behulpzaam zijn bij het volgen of het bejegenen van personen die ook in het register zware criminaliteit zijn opgenomen<sup>125</sup>. Het enkele feit dat een persoon op een bepaalde plaats door de politie wordt aangetroffen kan een belangwekkende aanvulling zijn op de reeds voorhanden zijnde informatie over die persoon. Voor dergelijke doeleinden biedt art. 13a lid 7 WPolr de mogelijkheid tot registratie van gegevens uit het register zware criminaliteit in een ander register. Een zodanige registratie dient gepaard te gaan met een instructie over de wijze waarop met de betreffende persoon moet worden omgegaan. De registratie van het enkele feit dat een persoon tevens in het register zware criminaliteit geregistreerd staat, is niet toegestaan. Het bepaalde in art. 13a lid 7 WPolr heeft geen directe gevolgen voor een verstrekking uit een register zware criminaliteit in het kader van een ongericht dataminingonderzoek dat betrekking heeft op een gewoon politieregister. In het geval van een verstrekking op grond van art. 13a lid 7 WPolr ligt het initiatief tot de verstrekking namelijk bij het register zware criminaliteit. Bij het hier aan de orde zijnde ongerichte dataminingonderzoek ligt het initiatief echter bij de uitvoerder van dat dataminingonderzoek. Bovendien kan uit de formulering van art. 13a lid 7 WPolr worden afgeleid dat het artikel ziet op een verstrekking in een bepaald geval, en niet op omvangrijke verstrekkingen zoals die waarvan sprake zal zijn in het kader van een ongericht dataminingonderzoek. Ondanks het feit dat het verstrekkingenregime van een register zware criminaliteit in art. 13a WPolr niet in een specifiek doelbindingsbeginsel voorziet, speelt dit beginsel een essentiële rol bij de verwerking van de gegevens in dit bijzondere politieregister.

*Art. 4 WPolr* – Met de bijzondere politieregisters is tegemoetgekomen aan de bevinding in het rapport van de parlementaire enquêtecommissie opsporingsmethoden, dat te veel

---

125. *Kamerstukken II*, 1996/197, 25 398, nr. 3, p. 17-18 en *Kamerstukken II*, 1997/198, 25 398, nr. 6, p. 34.

informatie werd opgeslagen in de registers van de criminele inlichtingendiensten. Om die reden heeft de wetgever ter nadere concretisering van het noodzakelijkheidsvereiste van art. 4 WPolr uitvoerig vastgelegd wanneer en over wie gegevens mogen worden geregistreerd in een register zware criminaliteit. Registratie is alleen mogelijk wanneer personen op een bepaalde wijze in verband kunnen worden gebracht met strafbare feiten die worden genoemd in de doelomschrijving van het register zware criminaliteit. Indien gegevens aan deze voorwaarden voldoen kunnen zij langdurig voor operationeel gebruik in dat register worden opgeslagen. Met de introductie van de bijzondere politieregisters is voor de opslag van zachte opsporingsinformatie een uitputtende wettelijke regeling getroffen in die zin dat dergelijke informatie in de overige politieregisters niet structureel mag worden vastgelegd.<sup>126</sup> In beginsel worden alle gegevens met betrekking tot de misdrijven die zijn genoemd in art. 1 onder k WPolr opgenomen in het register zware criminaliteit.<sup>127</sup> Dit is alleen anders wanneer een meer ingekaderde en op het specifieke geval gerichte registratie te prefereren is in welk geval kan worden overgegaan tot de aanleg van een tijdelijk register. Registratie van zachte gegevens voor een ander doel dan dat, waarvoor een register zware criminaliteit kan worden aangelegd is slechts mogelijk in een tijdelijk of een voorlopig politieregister. In combinatie met het bepaalde in art. 13d lid 3 WPolr betekent dit dat de mogelijkheid tot het registreren van zachte gegevens in beginsel is beperkt tot de bijzondere politieregisters. Slechts voor kortstondige registratie van zachte gegevens naar aanleiding van tips of meldingen mag gebruik worden gemaakt van een gewoon politieregister.

*Registratie* – Op grond van art. 4 WPolr is de duurzame opslag van gegevens over personen ten aanzien van wie het vermoeden bestaat dat zij betrokken zijn bij het beramen of plegen van strafbare feiten voor de (operationele) uitvoering van de justitiële politietaak (zachte gegevens) alleen noodzakelijk voor die misdrijven, waarvoor een register zware criminaliteit kan worden aangelegd of welke nader bij AMvB kunnen worden aangewezen.<sup>128</sup> Het criterium voor het registreren van gegevens in een register zware criminaliteit wordt gevormd door een met het oog op de bescherming van de persoonlijke levenssfeer aan te brengen begrenzing aan de opslag van de voor operationeel gebruik bestemde gegevens. De noodzaak tot een zodanige registratie van personen moet, los van de verdenking van een concreet strafbaar feit, de mogelijke inbreuk op de persoonlijke levenssfeer kunnen rechtvaardigen. Dat zal alleen het geval zijn wanneer de gegevens worden geregistreerd voor het doel waarvoor een register zware criminaliteit wordt aangelegd. Een verstrekking van gegevens uit een register zware criminaliteit die in een duurzame opslag van die gegevens voor operationeel gebruik resulteert, is alleen toegestaan voor het

---

126. *Kamerstukken II*, 1997/98, 25 398, nr. 6, p. 1.

127. *Kamerstukken II*, 1997/98, 25 398, nr. 6, p. 10.

128. *Kamerstukken II*, 1996/97, 25 398, nr. 3, p. 8.

doel van (en in) een register zware criminaliteit. Om die reden dient te worden onderzocht of een verstrekking uit een register zware criminaliteit in het kader van een ongericht dataminingonderzoek resulteert in een duurzame opslag van die gegevens voor operationeel gebruik. Indien daarvan sprake is, is een verstrekking niet mogelijk; een zodanige opslag is immers voorbehouden aan de registers zware criminaliteit.

In het kader van het ongerichte dataminingonderzoek zullen gegevens uit het register zware criminaliteit worden vastgelegd in een gewoon politieregister. Het is de vraag of deze registratie als duurzaam kan worden aangemerkt. De keuze om de registratie van gegevens uit een register zware criminaliteit slechts te beperken voor zover het een duurzame opslag betreft, heeft mogelijk te maken met het feit dat de gegevens in dit register zijn bestemd voor operationeel gebruik. Wanneer het register operationeel wordt geraadpleegd dient het mogelijk te zijn dat de verkregen informatie (weliswaar kortstondig) kan worden geregistreerd. In beginsel zal het dan gaan om een incidentele bevraging waarbij er geen sprake is van een langdurige registratie van de verkregen gegevens. Een registratie in het kader van een ongericht dataminingonderzoek kan echter moeilijk als kortstondig worden aangemerkt. Of er sprake is van een duurzame opslag hangt voornamelijk af van het doel waarvoor is verstrekt. In dit geval vindt de verstrekking plaats in het kader van een ongericht dataminingonderzoek dat betrekking heeft op een gewoon politieregister. Deze variant van het dataminingsproces heeft in beginsel steeds een permanent karakter, wat ook geldt voor het datawarehouse dat wordt aangelegd. Gelet hierop kan worden gesteld dat de verstrekking resulteert in een duurzame opslag. Wanneer gegevens uit een register zware criminaliteit worden verstrekt aan een gewoon politieregister in het kader van een ongericht dataminingonderzoek zijn die gegevens, evenals het uiteindelijke resultaat van het dataminingonderzoek, bestemd voor operationeel gebruik. Hoewel het onwenselijk mag worden geacht dat de gegevens in een datawarehouse kunnen worden verwerkt voor andere doeleinden dan het dataminingonderzoek waarvoor zij zijn vastgelegd, worden op dat punt door de huidige wet- en regelgeving geen beperkingen gesteld.

*Verwerking* – De doelstelling van een register zware criminaliteit rechtvaardigt de inbreuk op de persoonlijke levenssfeer die met de registratie van gegevens in dit bijzondere politieregister gepaard kan gaan. Deze inbreuk is tweeledig. Er kan op zeer grote schaal informatie over personen worden verzameld, hetgeen een vergaande inmenging van de overheid in het privé-leven van deze personen impliceert. Voorts vindt deze inmenging plaats op grond van informatie die veelal nog niet verifieerbaar is. Met het oog hierop dient niet alleen bij de registratie, maar ook bij een verdere verwerking van deze gegevens rekening te worden gehouden met het doelbindingsbeginsel in die zin dat deze dient plaats te vinden in het kader van de bestrijding van de zware criminaliteit. Wanneer dat niet het geval is zal geen sprake zijn van een balans tussen het doel van de verwerking (in plaats van registratie) en de bescherming van de persoonlijke levenssfeer. Gesteld mag worden dat het verstrekkingenregime van het register zware criminaliteit in

de WPolr en het BPolr tekortschiet waar het gaat om de vele manieren waarop gegevens vandaag de dag worden verwerkt.

De registratie van zachte gegevens is in de WPolr en het BPolr uitvoerig geregeld. Door de duurzame registratie van zachte gegevens voor operationeel gebruik voor te behouden aan het register zware criminaliteit, wordt indirect ook voorzien in een doelbindingsbeginsel wanneer het gaat om een verstrekking van gegevens uit dit bijzondere register. De doelbinding dient in beginsel een tweevoudige bescherming te bieden. Ten eerste wordt de burger beschermd tegen een al te lichtvaardige registratie van zijn gegevens in een register zware criminaliteit. Ten tweede kan worden voorkomen dat eenmaal in een register zware criminaliteit geregistreerde zachte gegevens worden verwerkt op een wijze die niet strookt met het doel waarvoor zij in eerste instantie zijn vergaard.<sup>129</sup> Het verstrekkingenregime van een register zware criminaliteit voorziet echter onvoldoende in deze tweede functie. De verwerking van eenmaal geregistreerde gegevens blijkt nauwelijks te zijn geregeld. Terwijl onder de bestaande wet- en regelgeving strenge voorwaarden gelden voor een registratie in een register zware criminaliteit, lijkt het van ondergeschikt belang hoe die gegevens vervolgens worden aangewend. Het verstrekkingenregime, bijvoorbeeld, staat een verstrekking van gegevens in een register zware criminaliteit voor doeleinden die niet zijn gerelateerd aan de bestrijding van de zware criminaliteit niet in de weg. Ook dit probleem is een gevolg van het feit dat de WPolr en het BPolr zijn gebaseerd op de oude Wpr – waarin de nadruk lag op de registratie van persoonsgegevens – in plaats van op de Wbp, die niet alleen op de registratie van gegevens maar op iedere vorm van gegevensverwerking ziet. In het kader van deze verschuiving op het gebied van de privacybescherming is een regeling noodzakelijk die niet is beperkt tot de registratie van gegevens, maar die voorziet in de gehele verwerking daarvan.

Momenteel kan voor een verdere verwerking van gegevens in een register zware criminaliteit alleen een relatie worden gelegd met de doelbinding die voortkomt uit art. 4 WPolr. Een duurzame opslag van zachte gegevens voor operationeel gebruik<sup>130</sup> is alleen toegestaan voor het doel waarvoor een register zware criminaliteit kan worden aangelegd. De doelbinding, en daarmee de bescherming van de persoonlijke levenssfeer, is afhankelijk van de vraag of sprake is van een duurzame registratie en het operationele gebruik van de gegevens. Hiermee blijft het mogelijk om zachte gegevens kortstondig te registreren of (langdurig) vast te leggen voor niet-operationeel gebruik ten behoeve van allerhande doeleinden, ook wanneer deze de inbreuk op de privacy die daarmee gepaard gaat niet rechtvaardigen. Het uitgangspunt dat, ook wanneer het gaat om kortstondige registratie, zorgvuldig met gegevens dient te worden omgegaan sluit aan bij de gedachte achter de beperking van het noodzakelijkheidsvereiste van art. 4 WPolr. Voor de invulling van het noodzakelijkheidsbegrip van dat artikel dient de noodzaak tot registratie de

---

129. *Kamerstukken II*, 1997/98, 25 398, nr. 6, p. 9.

130. Art. 4 WPolr.

mogelijke inbreuk op de persoonlijke levenssfeer te rechtvaardigen. Doorslaggevend daarbij is dat het gaat om misdrijven die ofwel naar hun aard een ernstige inbreuk op de rechtsorde opleveren ofwel het rechtsgevoel ernstig doen schokken.<sup>131</sup>

Ook de voorwaarde dat sprake dient te zijn van operationeel gebruik van gegevens doet onvoldoende recht aan de bescherming van de persoonlijke levenssfeer. Hoewel een beperking van het verstrekkingenregime waarborgen biedt ter bescherming van de persoonlijke levenssfeer, vormt het geenszins een garantie dat de gegevens niet op oneigenlijke wijze worden gebruikt. Daarvan kan sprake zijn wanneer de gegevens uit een register zware criminaliteit voor een geheel ander doel worden verwerkt dan waarvoor zij zijn geregistreerd.

*Aanpassing verstrekkingenregime* – Gelet op het voorgaande lijken de voorwaarden van duurzame opslag en het operationele gebruik van gegevens tekort te schieten als maatstaf voor de vraag, of een verstrekking met het oog op de bescherming van de persoonlijke levenssfeer toelaatbaar is. In het kader van de Wbp dient te worden gekeken naar de legitimiteit van de verwerking van gegevens (uit een register zware criminaliteit) als geheel. De vraag of een verstrekking (verwerking) in een bepaald geval mogelijk is dient te worden getoetst aan het doelbindingsbeginsel. In art. 13a WPolr is met betrekking tot de verwerking van de gegevens in een register zware criminaliteit de registratie en de verstrekking van die gegevens geregeld. Daarbij is weliswaar sprake van beperkte registratiemogelijkheden, maar worden aan de verstrekking van al geregistreerde gegevens nauwelijks voorwaarden gesteld. Een verstrekking kan plaatsvinden voor uiteenlopende doeleinden: een (incidentele) verstrekking in een bepaald geval of een verstrekking in het kader van een koppeling.

Voor de verstrekkingen die plaatsvinden in het kader van een koppeling lijkt een bepaling dat een verstrekking uit een register zware criminaliteit slechts mogelijk is voor de doeleinden waarvoor dat register kan worden aangelegd een logische aanpassing van het verstrekkingenregime. Een soortgelijke bepaling vloeit al voort uit het modelreglement van het register zware criminaliteit, maar dat reglement staat een incidentele verstrekking uit een register zware criminaliteit voor een ander doel dan waarvoor het is aangelegd niet in de weg. In combinatie met het feit dat de gegevens in een register zware criminaliteit geschikt zijn voor operationeel gebruik betekent dit dat de bescherming van de persoonlijke levenssfeer in het geding kan zijn bij een incidentele bevraging. Terwijl het incidenteel raadplegen van gegevens in een register zware criminaliteit niet per definitie een ontoelaatbare inbreuk op de persoonlijke levenssfeer impliceert, kan dat wel het geval zijn wanneer de verstrekte gegevens vervolgens elders worden vastgelegd en verwerkt. Het achterliggende doel van de verstrekking is in sterke mate bepalend voor de

---

131. *Kamerstukken II*, 1996/197, 25 398, nr. 3, p. 2 en 9 en *Kamerstukken II*, 1997/198, 25 398, nr. 6, p. 10.

vraag of een verstrekking in een bepaald geval wenselijk is. Het verdient aanbeveling om ook met betrekking tot een incidentele bevraging de voorwaarde van de doelbinding op te nemen in art. 13a WPolr., zodat de bescherming van de persoonlijke levenssfeer van de personen die in een register zware criminaliteit zijn geregistreerd niet langer is beperkt tot de registratie in dat register maar zich uitstrekt tot iedere verwerking van de gegevens.

Voor een adequate aanpak van de zware criminaliteit is het noodzakelijk dat opsporingsambtenaren dat register operationeel kunnen raadplegen. De aanbevolen aanpassing van art. 13a WPolr doet in beginsel geen afbreuk aan deze mogelijkheid. Naast het feit dat een incidentele bevraging minder bezwaarlijk is dan een koppeling, gaat het operationeel gebruik van het register zware criminaliteit goed samen met het doelbindingsbeginsel. Aan de noodzaak om opsporingsambtenaren toegang te geven tot de gegevens in een register zware criminaliteit ligt immers de bestrijding van diezelfde zware criminaliteit ten grondslag. Bij een verstrekking die plaatsvindt in overeenstemming met het doel van een register zware criminaliteit is de mogelijke inbreuk op de persoonlijke levenssfeer die met het gebruik van de verstrekte gegevens gepaard gaat gerechtvaardigd.

*Art. 4 lid 2 WPolr* – Volgens art. 4 lid 2 WPolr dient de registratie van de gegevens uit het register zware criminaliteit noodzakelijk te zijn voor het doel van het register waaraan wordt verstrekt. In beginsel lijkt het voor de verbetering van de informatiepositie van een gewoon politieregister niet noodzakelijk dat gebruik wordt gemaakt van gegevens uit een register zware criminaliteit.

*Doelbinding gegevens in categorie C* – Voor een register zware criminaliteit is het voorgaande met name van toepassing op de gegevens in de categorieën *a* (verdachten van misdrijven, waarvoor het register is aangelegd) en *b* (personen, ten aanzien van wie een redelijk vermoeden bestaat dat zij betrokken zijn bij het beramen of plegen van misdrijven als bedoeld onder *a*). Op de gegevens in een register zware criminaliteit die behoren tot categorie *c* (personen die in een bepaalde relatie staan tot degenen, bedoeld onder *a* en *b*) is een afwijkend verstrekkingenregime van toepassing, dat overeenkomt met dat van een voorlopig politieregister.<sup>132</sup> Die gegevens zijn niet beschikbaar voor operationeel gebruik, een verstrekking aan een gewoon politieregister is slechts mogelijk voor het doel waarvoor een register zware criminaliteit (meer in het bijzonder de gegevens in categorie *c*) is aangelegd. Een verstrekking van gegevens uit categorie *c* vindt in dit geval niet plaats ter verrijking van het register zware criminaliteit (meer in het bijzonder de gegevens in categorie *c*), maar ter verrijking van het basisregister en is dan ook niet toegestaan. Ook wanneer een verstrekking van de gegevens uit categorie *c* aan een gewoon politieregister wel voldoet aan het doelbindingscriterium is een verwerking niet mogelijk. Op grond van art. 13d lid 3 WPolr is verwerking immers slechts toegestaan in overeenstem-

---

132. Art. 13b lid 2 WPolr.

ming met het bepaalde in par. 3a WPolr. Bovendien bepaalt art. 13b lid 2, eerste volzin WPolr dat het niet is toegestaan de verstrekte gegevens in enig ander register (dan het register zware criminaliteit) vast te leggen.

### Koppeling

Aangezien bij een verstrekking van gegevens uit een register zware criminaliteit aan een gewoon politieregister in het kader van een ongericht dataminingonderzoek sprake is van een koppeling in de zin van art. 6 WPolr, dient rekening te worden gehouden met de voorwaarden die door de WPolr en het BPolr aan een koppeling worden gesteld.

*Noodzakelijk voor de politietaak* – De aard van de politietaak waarvoor een politieregister in eerste instantie is aangelegd kan mede bepalend zijn voor de vraag, of is voldaan aan de doelbinding. Een koppeling, en daarmee het gebruik, van gegevens uit een register zware criminaliteit dient op grond van art. 6 lid 1 WPolr noodzakelijk te zijn voor een goede uitvoering van de politietaak (in verband met de strafrechtelijke handhaving van de rechtsorde). Hoewel zowel een gewoon politieregister als een register zware criminaliteit met dat doel worden aangelegd, is de uitvoering van de politietaak in het kader van het register zware criminaliteit specifiek gerelateerd aan de misdrijven die tot de zware criminaliteit worden gerekend<sup>133</sup>. Dit blijkt ook uit het rapport van de commissie Van Traa<sup>134</sup>, dat een vergelijkbaar standpunt bevat betreffende de verstrekking van gegevens uit een register zware criminaliteit. Met betrekking tot de koppeling van een register zware criminaliteit met een gewoon politieregister wordt het volgende gesteld:

*‘Koppeling van CID-registers<sup>135</sup> met andere persoonsregistraties vindt eveneens plaats onder dezelfde voorwaarden als die gelden voor de gewone politieregistraties. Met dien verstande dat de voorwaarde – nodig voor de goede uitvoering van de politietaak – wordt uitgelegd overeenkomstig het doel van het CID-register, te weten dat het noodzakelijk moet zijn voor het voorkomen en opsporen van misdrijven die gezien hun ernst en frequentie dan wel het georganiseerd verband waarin ze worden gepleegd een ernstige inbreuk op de rechtsorde opleveren. Verstrekking lijkt daardoor alleen plaats te kunnen vinden aan personen die daarop aanspraak kunnen maken ingevolge hun werkzaamheden bij de CID. Daarop is ten behoeve van het MOT de uitzondering gemaakt dat aan hen die gegevens kunnen worden verstrekt die noodzakelijk zijn om te kunnen vaststellen of een persoon in dat register is opgenomen.’*

---

133. *Kamerstukken II*, 1996/97, 25 398, nr. 3, p. 14.

134. Commissie Van Traa, sectie 8.4 Verstrekking; 8.4.1 Juridische grondslag.

135. De huidige registers zware criminaliteit.

Deze zienswijze aangaande de politietaak, die een nadere specificatie van de doelstelling van een register zware criminaliteit behelst, ondersteunt de opvatting dat de gegevens in dit register alleen (verder) mogen worden verwerkt voor de politietaak voor zover die is gerelateerd aan misdrijven die behoren tot de zware criminaliteit. Wanneer dat niet het geval is kan dat een belangrijke aanwijzing zijn, dat niet aan het doelbindingsbeginsel (of het noodzakelijkheidvereiste) is voldaan. Daarom geldt des te meer dat bij een koppeling met een register zware criminaliteit per geval dient te worden nagegaan of deze een duidelijke, toegevoegde waarde vertegenwoordigt. Daarnaast wordt meer helderheid verschaft over de rol die de doelbinding speelt bij de verwerking van gegevens in een register zware criminaliteit in het kader van het dataminingsproces, waarbij in beginsel steeds sprake van een koppeling is. De bepalingen betreffende de koppeling zijn daardoor ook van belang voor het dataminingsproces als geheel. Nu blijkt dat een koppeling alleen mogelijk is met het oog op de bestrijding van de zware criminaliteit kan worden overwogen, iedere verwerking van gegevens in een register zware criminaliteit afhankelijk te maken van de vraag of die verwerking is gerelateerd aan het doel waarvoor de gegevens in eerste instantie zijn vastgelegd.

*Modelreglement register zware criminaliteit* – Ook in het geval van een koppeling met een register zware criminaliteit dienen de reglementen van beide betrokken politieregisters op grond van art. 6 lid 2 WPolr in die mogelijkheid te voorzien. In het modelreglement van een register zware criminaliteit<sup>136</sup> wordt in art. 17 bepaald dat alleen kan worden gekoppeld voor zover dat noodzakelijk is voor het voorkomen en opsporen van misdrijven die een ernstige inbreuk op de rechtsorde opleveren, en wel aan andere registers zware criminaliteit, voorlopige registers, dan wel gegevensverzamelingen waarvan de doelstelling nauw bij die van het register zware criminaliteit aansluit. Ook deze bepaling lijkt een koppeling met een gewoon politieregister uit te sluiten.

*Koppeling gegevens in categorie C* – Een koppeling (verstrekking) met een gewoon politieregister aangaande gegevens in een register zware criminaliteit die behoren tot categorie *c* is op grond van art. 13*b* lid 3 WPolr uitgesloten en daarmee eveneens de mogelijkheid van een koppeling in het kader van een ongericht dataminingsonderzoek; die gegevens worden immers in een ander, gewoon, politieregister opgeslagen. Bovendien is een koppeling van gegevens omtrent onverdachte personen, waar het hier om gaat, alleen mogelijk in het kader van de bestrijding van de zware criminaliteit.

Het is trouwens de vraag of gegevens in een register zware criminaliteit überhaupt wel mogen worden verwerkt. De MvT<sup>137</sup> bij de bijzondere politieregisters bepaalt met betrekking tot de gegevens in een register zware criminaliteit als bedoeld in art. 13*a* lid 1

---

136. *Stcr.* 12 oktober 2000, nr. 198, p. 17.

137. *Kamerstukken II*, 1996/97, 25 398, nr. 3, p. 19-20.

onder *c* WPolr, dat gedragingen van een ‘contact’ binnen het criminele circuit kunnen aansporen tot nadere politieke aandacht. In dat geval kunnen diens gegevens worden gebruikt in een misdaadanalyse, opdat kan worden vastgesteld of hij in samenhang met andere gegevens als zelfstandig subject in het register zware criminaliteit kan worden opgenomen. Voor dit doel geldt hetzelfde verstrekkingenregime als voor het voorlopige politieregister. Met het oog op het doel van een voorlopig politieregister en art. 13*d* lid 3 WPolr dienen de gegevens dan te worden overgeheveld naar dat politieregister. Met betrekking tot het verstrekkingenregime van het voorlopige register geeft de wetgever aan dat de gegevens niet operationeel kunnen worden aangewend in die zin dat opsporingsbevoegdheden worden aangewend tot nadere informatieinwinning of dat betrokkene in zijn contacten met de politie anders wordt bejegend. Wel kunnen de gegevens worden vergeleken met gegevens uit andere bijzondere politieregisters. Dit leidt tot de conclusie dat een verwerking van de gegevens in een register zware criminaliteit als bedoeld in art. 13*a* lid 1 onder *c* WPolr niet mogelijk is wanneer een geregistreerde daartoe geen aanleiding geeft. Dat impliceert evenwel, dat de gegevens in een register zware criminaliteit die behoren tot categorie *c* nauwelijks kunnen worden benut. Een registratie heeft dan vrijwel uitsluitend een toegevoegde waarde voor het register-MOT. In het kader van de bestrijding van de zware criminaliteit is het echter wenselijk om ook deze categorie van gegevens in een register zware criminaliteit te kunnen vergelijken (koppelen) met gegevens in andere bijzondere politieregisters.

#### **De aard van het ongerichte dataminingonderzoek**

Het verstrekkingenregime van een register zware criminaliteit en dat van een gewoon politieregister staat een koppeling van gegevens behorende tot de categorieën *a* en *b* en de daarmee gepaard gaande registratie van die gegevens in het gewone politieregister niet in de weg. Een dergelijke registratie is evenwel niet in overeenstemming met de voorwaarde van doelbinding, die van invloed is op het verstrekkingenregime van een register zware criminaliteit. Registratie van gegevens in een register zware criminaliteit impliceert een vergaande inbreuk op de persoonlijke levensfeer. Deze inbreuk is gerechtvaardigd door het belang van effectieve bestrijding van de zware criminaliteit. Bij het gebruik van gegevens uit een register zware criminaliteit ten behoeve van een ongericht dataminingonderzoek ontbreekt deze rechtvaardiging in beginsel<sup>138</sup>, hetgeen resulteert in een ontoelaatbare inbreuk op de persoonlijke levenssfeer.

*Gegevens in categorie C* – De gegevens uit een register zware criminaliteit in de categorie *c* hebben betrekking op in eerste instantie onverdachte personen. Dezen zijn in een register zware criminaliteit geregistreerd omdat zij in een bepaalde relatie staan tot personen in de categorieën *a* en *b*. Hoewel gegevens in de categorie *c* al zijn geregistreerd in een

---

138. Zie ook sectie 7.3.4.3 onder het kopje *De doelbinding*.

register zware criminaliteit, voldoen zij noch aan het criterium om als zelfstandig subject in dat register te worden opgenomen, noch aan dat om te worden opgenomen in een voorlopig politieregister. De status van de gegevens in categorie *c* beperkt de mogelijkheid van verwerking daarvan. De wetgever<sup>139</sup> geeft aan dat gegevens die nog niet voor opslag in het register zware criminaliteit in aanmerking komen, vanwege de onzekere aard van de informatie alleen mogen verstrekt met het oog op het verkrijgen van aanvullende informatie en niet in verband mogen worden gebracht met de uitvoering van enige politietaak. Dit betekent dat ten behoeve van het ongerichte dataminingonderzoek van deze gegevens geen gebruik mag worden gemaakt. Het is evenwel denkbaar dat gedragingen van een 'contact' binnen het criminele circuit aanleiding vormen tot nadere politieke aandacht. Teneinde vast te stellen of betrokkene, in samenhang met andere gegevens, als zelfstandig subject in het register zware criminaliteit kan worden opgenomen kunnen diens gegevens worden gebruikt in een (klassieke) misdaadanalyse. Daartoe geldt hetzelfde verstrekkingenregime als voor het voorlopige politieregister (art. 13a lid 2, eerste volzin WPolr). De informatie mag derhalve niet operationeel worden aangewend in de zin, dat opsporingsbevoegdheden worden ingezet tot nadere informatie-inwinning; daarnaast mag de betrokkene in zijn contacten met de politie niet anders dan in die context worden bejegend. Wel kunnen de gegevens worden vergeleken met gegevens uit andere bijzondere politieregisters.<sup>140</sup> Een verwerking van gegevens uit categorie *c* zal dan ook niet eerder mogelijk zijn dan wanneer de, in relatie tot een als zelfstandig subject in een register zware criminaliteit geregistreerde persoon staande, betrokkene zelf aanleiding geeft tot politieke aandacht. Het enkele feit van geregistreerd staan in een register zware criminaliteit zal niet als een zodanige aanleiding kunnen worden bestempeld.

#### Weigering door de beheerder

De beheerder van een politieregister kan een verstrekking weigeren indien dat noodzakelijk is voor de goede uitvoering van de politietaak<sup>141</sup>. Voor een beheerder van een register zware criminaliteit is daarvoor een aparte regeling getroffen in art. 13a lid 3 WPolr. Op grond daarvan staat het hem vrij een verstrekking te weigeren<sup>142</sup>, dan wel om beperkende voorwaarden te stellen aan een verder gebruik van de verstrekte gegevens, indien dat noodzakelijk is voor een goede uitvoering van de politietaak.<sup>143</sup> Daarvan kan sprake zijn wanneer het risico bestaat, dat het onderzoek naar een bepaalde criminele groepering door de verstrekking wordt doorkruist. De weigeringsbevoegdheid dient echter steeds in de context van het verplichte verstrekkingenregime binnen het politieveld te worden geplaatst. Uitgangspunt blijft de verplichting tot verstrekking binnen de politie voor

139. *Kamerstukken II*, 1996/97, 25 398, nr. 3, p. 19.

140. *Kamerstukken II*, 1996/97, 25 398, nr. 3, p. 19.

141. Art 11 lid 3 BPolr, zie ook sectie 7.3.3.5.

142. *Kamerstukken II*, 1997/98, 25 398, nr. 6, p. 3 en 24.

143. Art. 13a lid onder 3 WPolr.

zover nodig voor de uitvoering van de politietaak.<sup>144</sup> Dit betekent dat het vrije verkeer van gegevens behorende tot de categorieën *a* en *b* slechts in zeer beperkte mate kan en mag worden beperkt. Art. 13a lid 3 WPolr is niet van toepassing op het register-MOT. Hoewel aan het register-MOT niet meer informatie behoeft te worden verstrekt dan strikt noodzakelijk is om een eventuele registratie in het register zware criminaliteit te kunnen vaststellen, kunnen aan deze verplichting tot informatieverstrekking geen beperkende voorwaarden worden verbonden.<sup>145</sup> In beginsel zou de beheerder kunnen volstaan met een bevestiging dan wel een ontkenning op de vraag, of een bepaalde persoon in het door hem beheerde register staat geregistreerd.

### Resumerend

Hoewel de gegevens in een register zware criminaliteit in beginsel voor operationeel gebruik zijn bestemd, blijkt de mogelijkheid om deze gegevens te verwerken door een aantal factoren te worden beperkt. Die gegevens zullen namelijk voor een groot deel een zeer gevoelig karakter hebben. Op de gegevens die behoren tot categorie *c* is een verstrekkingenregime van toepassing, dat een verstrekking ten behoeve van een ongericht dataminingonderzoek onmogelijk maakt. De gegevens in categorie *b* mogen in beginsel niet worden geregistreerd in een gewoon politieregister. Hoewel de gegevens in categorie *a* het betrouwbaarst zijn, is het gebruik van alle drie categorieën beperkt door onder meer de doelbinding. Met het oog op de persoonlijke levenssfeer dient te worden getoetst of een verwerking van de gegevens in een register zware criminaliteit in overeenstemming is met de doelstellingen waarvoor dat register kan worden aangelegd. Bij een verstrekking in het kader van een ongericht dataminingonderzoek ter verbetering van de informatiepositie van een gewoon politieregister is daarvan in beginsel geen sprake. Wanneer een verstrekking ten behoeve van een dataminingonderzoek in het kader van een koppeling plaatsvindt, gelden aanvullende voorwaarden. Het modelreglement van een register zware criminaliteit blijkt de mogelijkheid van een koppeling voor het doel van het onderhavige ongerichte dataminingonderzoek uit te sluiten. Bij een ongericht dataminingonderzoek dient er verder rekening mee te worden gehouden, dat een verwerking van gegevens (over onverdachte personen) niet mag resulteren in een ontoelaatbare inbreuk op de persoonlijke levenssfeer.

### 7.4 Afsluitend

In dit hoofdstuk staat de vraag centraal in hoeverre gegevens uit de verschillende aan opsporingsdiensten ter beschikking staande bronnen mogen worden gebruikt in het kader van een ongericht dataminingonderzoek ter verbetering van de informatiepositie van een gewoon politieregister. Alvorens in deze sectie voor elk van de vier vormen van

---

144. *Kamerstukken II*, 1997/198, 25 398, nr. 6, p. 6.

145. Art. 13a lid 1 onder 4 WPolr.

ongericht dataminingonderzoek puntsgewijs zal worden weergegeven of, en zo ja onder welke voorwaarden, dat het geval is, volgen enkele aanbevelingen die uit dit hoofdstuk naar voren komen.

In het streven naar een efficiënte invulling van de opsporingstaak en gelet op de bescherming van de persoonlijke levenssfeer dient te worden gestreefd naar een overkoepelend informatiebeheer. Het verstrekkingenregime van de WPolr kan daarbij gehandhaafd blijven. Er kan gebruik worden gemaakt van verwijssindexen welke ook gegevens bevatten die betrekking hebben op gegevens waarop normaliter een beperkt verstrekkingenregime van toepassing is. Juist voor het bereiken van de doelstellingen waartoe dergelijke zachte informatie wordt verwerkt, is een goede informatievoorziening onontbeerlijk. Om te voorzien in de benodigde waarborgen ter bescherming van de persoonlijke levenssfeer kan worden gekozen voor kwalificatie van een verwijssindex als bijzonder politieregister. Ten behoeve van een goede samenwerking en het verkrijgen van kennis die is gebaseerd op een volledig gegevensbeeld is de toepassing van overkoepelend informatiebeheer in combinatie met dataminingstechnieken een krachtig instrument.

De regeling van art. 13a WPolr voorziet met betrekking tot de verwerking van de gegevens in een register zware criminaliteit in de registratie en de verstrekking van die gegevens. Daarbij worden aan de verstrekking van reeds geregistreerde gegevens nauwelijks voorwaarden gesteld. Een verstrekking kan plaatsvinden voor uiteenlopende doeleinden: een (incidentele) verstrekking in een bepaald geval of een verstrekking in het kader van een koppeling. Voor de verstrekkingen die plaatsvinden in het kader van een koppeling lijkt een bepaling dat een verstrekking uit een register zware criminaliteit slechts mogelijk is voor de doeleinden waarvoor dat register kan worden aangelegd een logische aanpassing van het verstrekkingenregime. Een soortgelijke bepaling vloeit al voort uit het modelreglement van het register zware criminaliteit. Dat reglement staat een incidentele verstrekking uit een register zware criminaliteit voor een ander doel dan waarvoor het is aangelegd echter niet in de weg. In combinatie met het feit dat de gegevens in een register zware criminaliteit geschikt zijn voor operationeel gebruik betekent dit, dat de bescherming van de persoonlijke levenssfeer in het geding kan zijn bij een incidentele bevraging. Het verdient daarom aanbeveling om ook met betrekking tot een incidentele bevraging de voorwaarde van de doelbinding op te nemen in art. 13a WPolr, zodat de bescherming van de persoonlijke levenssfeer van hen die in een register zware criminaliteit zijn geregistreerd niet langer is beperkt tot de registratie in dat register maar zich uitstrekt tot iedere verwerking van die gegevens.

### *Overzicht en schema*

#### 1. Geen gebruik van externe gegevens

##### *Algemene voorwaarden*

- Het onderzoek is noodzakelijk voor een goede uitvoering van de politietaak voor zover het de strafrechtelijke handhaving van de rechtsorde betreft.
- Er is voldaan aan het doelbindingsbeginsel.
- Het onderzoek wordt uitgevoerd door, dan wel onder het gezag van, de beheerder van het desbetreffende politieregister.

##### *Koppeling*

Geen.

##### *Toepassing en specifieke beperkingen*

Naast die gesteld in de algemene voorwaarden gelden in beginsel geen aanvullende beperkingen.

#### 2. Gebruik van gegevens die niet afkomstig zijn uit een politieregister

##### *Algemene voorwaarden*

- Het onderzoek is noodzakelijk voor een goede uitvoering van de politietaak voor zover het de strafrechtelijke handhaving van de rechtsorde betreft.
- Er is voldaan aan het doelbindingsbeginsel.
- Het onderzoek wordt uitgevoerd door, dan wel onder het gezag van de beheerder van het betreffende politieregister.

##### *Koppeling*

Indien sprake is van koppeling<sup>146</sup>, gelden aanvullende voorwaarden.

- Een koppeling dient noodzakelijk te zijn voor de politietaak voor zover het de strafrechtelijke handhaving van de rechtsorde betreft.
- Een eventuele koppeling dient noodzakelijk te zijn voor het doel van het basisregister<sup>147</sup>.
- Om te mogen koppelen dient het reglement van het basis(politie)register in die mogelijkheid te voorzien<sup>148</sup>.

---

146. Er is geen sprake van koppeling indien het gaat om externe gegevens die geen onderdeel uitmaken van een zelfstandig register.

147. Het register waarop het dataminingonderzoek betrekking heeft.

148. Tenzij de externe gegevens geen deel uitmaken van enig (politie)register. In dat geval is er geen sprake van een koppeling in de zin van art. 6 WPolr.

- Met het gebruik van externe gegevens wordt geen ontoelaatbare inbreuk gemaakt op de privacy<sup>149</sup>.
- Het gebruik van (persoons)gegevens uit een openbaar register is in beginsel niet toegestaan.

#### *Toepassing en specifieke beperkingen*

Naast de algemene voorwaarden dient in het geval van een koppeling rekening te worden gehouden met de daarvoor geldende regels.

### **3. Gebruik van gegevens uit een gewoon politieregister**

#### *Algemene voorwaarden*

- Het onderzoek is noodzakelijk voor een goede uitvoering van de politietaak voor zover het de strafrechtelijke handhaving van de rechtsorde betreft.
- Er is voldaan aan het doelbindingsbeginsel.
- Het onderzoek wordt uitgevoerd door, dan wel onder het gezag van, de beheerder van het betreffende politieregister.

#### *Koppeling*

Bij het gebruik van een ander gewoon politieregister is in beginsel steeds sprake van een koppeling.

- Een koppeling dient noodzakelijk te zijn voor de politietaak voor zover het de strafrechtelijke handhaving van de rechtsorde betreft.
- Een eventuele koppeling dient noodzakelijk te zijn voor het doel van het basisregister.
- Om te mogen koppelen dienen de reglementen van de betrokken politieregisters in de mogelijkheid daartoe te voorzien.
- Met het gebruik van externe gegevens wordt geen ontoelaatbare inbreuk gemaakt op de privacy.

#### *Toepassing en specifieke beperkingen*

Naast de algemene en de aanvullende voorwaarden van de koppeling dient rekening te worden gehouden met de beperkende werking van de doelbinding, de politietaak of een weigering door de beheerder van een politieregister.

---

149. In dat geval zou het een ingrijpend middel betreffen, wat in dit stadium van het proces van informatiegaring niet is toegestaan.

*Politietaat*

Het gebruik van politieregisters die niet zijn aangelegd in het kader van de politietaat (betreffende de strafrechtelijke handhaving van de rechtsorde), is niet vanzelfsprekend.

- Gebruik Openbare orde register: beperkt mogelijk wanneer een verstrekking past binnen de bevoegdheid van art. 2 Politiewet.
- Gebruik Hulpverleningsregister: in beginsel niet mogelijk (onder meer op grond van het doelbindingsbeginsel).

*Doelbinding*

- Gebruik Hulpverleningsregister: in beginsel is verstrekking slechts mogelijk wanneer aan het doelbindingsbeginsel is voldaan.
- Gebruik Register-MOT: in beginsel is verstrekking slechts mogelijk wanneer aan het doelbindingsbeginsel is voldaan.
- Gebruik overige gewone politieregisters: mogelijk voor zover dat noodzakelijk is voor het doel waarvoor wordt verstrekt<sup>150</sup>.

*Weigering door beheerder*

De beheerder van een register kan in bepaalde gevallen op grond van art. 11 BPolr een verstrekking weigeren.

**4. Gebruik van gegevens uit een bijzonder politieregister***Algemene voorwaarden*

- Het onderzoek is noodzakelijk voor een goede uitvoering van de politietaat voor zover het de strafrechtelijke handhaving van de rechtsorde betreft.
- Er is voldaan aan het doelbindingsbeginsel.
- Het onderzoek wordt uitgevoerd door, dan wel onder het gezag van, de beheerder van het desbetreffende politieregister.

*Koppeling*

In beginsel is steeds sprake van een koppeling.

- Een koppeling dient noodzakelijk te zijn voor de politietaat voor zover het de strafrechtelijke handhaving van de rechtsorde betreft.
- Een eventuele koppeling dient noodzakelijk te zijn voor het doel van het basisregister.
- Om te mogen koppelen dienen de reglementen van de betrokken politieregisters in de mogelijkheid daartoe te voorzien.

---

150. Art. 4 lid 2 WPolr.

- Met het gebruik van externe gegevens wordt geen ontoelaatbare inbreuk gemaakt op de privacy.

*Toepassing en specifieke beperkingen*

Het gebruik van gegevens uit de bijzondere politieregisters wordt niet alleen beperkt door de algemene voorwaarden en de voorwaarden die gelden voor een koppeling. Het beperkte verstrekkingenregime van de bijzondere politieregisters zal het gebruik van deze gegevens vrijwel steeds in de weg staan.

- Tijdelijk politieregister: het gebruik van dit register is niet mogelijk.
- Voorlopig politieregister: het gebruik van dit register is niet mogelijk.
- Register zware criminaliteit: het gebruik van dit register is slechts (op beperkte schaal) mogelijk ten behoeve van het MOT.

Het bovenstaande resulteert in het volgende schema.

Ongericht datamining-onderzoek	Koppeling	Beperkingen	Gebruik
Geen externe gegevens	Nee	Algemeen	Onbeperkt
Externe gegevens*	Ja**	Algemeen/koppeling	Beperkt
Gegevens uit een gewoon politieregister	Ja	Algemeen/koppeling/specifiek	Beperkt
Gegevens uit een bijzonder politieregister	Ja	Algemeen/koppeling/specifiek	Alleen t.b.v. het register-MOT

\* Externe gegevens afkomstig van buiten de politieke sfeer.

\*\* Tenzij de externe gegevens niet tot enig zelfstandig register behoren.

*Schema 11 Overzicht toepassing ongericht dataminingonderzoek ter verbetering van de informatiepositie van een gewoon politieregister*



---

## 8 Ongericht dataminingonderzoek en het register Ongebruikelijke Transacties

De op 1 februari 1994 in werking getreden Wet Melding Ongebruikelijke Transacties<sup>1</sup> (de Wet MOT) heeft twee doelstellingen, namelijk het voorkomen van misbruik van het financiële stelsel door het witwassen van geld<sup>2</sup> en bijdragen aan de mogelijkheden voor het bestrijden van witwassen van geld. Het Meldpunt heeft tot taak de gegevens die het verkrijgt te verzamelen, te registreren, te bewerken en te analyseren teneinde te bezien, of deze van belang kunnen zijn voor de voorkoming en opsporing van misdrijven.<sup>3</sup> Daarbij fungeert het Meldpunt als buffer zonder opsporingsbevoegdheid tussen de financiële instellingen en de opsporingsinstanties.<sup>4</sup> Hoewel de werkzaamheden van het Meldpunt vooral worden uitgevoerd in een vorm van het houden van toezicht en de gegevens in het register-MOT nog geen strafbare feiten behelzen, is wel sprake van een uitwisseling van gegevens tussen het register-MOT en de overige politieregisters. De bevindingen van het Meldpunt kunnen reden zijn voor nader politieonderzoek. Bovendien kan de Landelijk Officier van Justitie (LOvJ) in het geval van rechtsorde schokkende misdrijven het register-MOT bevragen.

Het register dat het Meldpunt in het kader van bovenstaande taak bijhoudt, is een register in de zin van de WPolr, waarover de MvJ het beheer voert.<sup>5</sup> Bij een verwerking door het Meldpunt dient daarom rekening te worden gehouden met de WPolr en het BPolr. Hoewel het register een beperkt verstrekkingenregime heeft, is het geen bijzonder politieregister.<sup>6</sup> Vanwege deze uitzonderingspositie ten opzichte van de overige gewone politieregisters wordt in dit hoofdstuk stilgestaan bij de mogelijkheid de informatieposi-

- 
1. Wet van 16 december 1993, betreffende melding ongebruikelijke transacties bij financiële dienstverlening, *Stb.* 2001, 665.
  2. *Kamerstukken II*, 1996/97, 25 378, nr. 3, p. 1.
  3. Art. 3 sub *a* Wet MOT.
  4. Terlouw & Aron 1996.
  5. Art. 4 lid 1 Wet MOT.
  6. *Kamerstukken II*, 1996/97, 25 398, nr. 3, p. 2. Hoewel het een beperkt verstrekkingenregime kent, onderscheidt het register-MOT zich van de overige bijzondere politieregisters doordat het niet rechtstreeks ten dienste van de uitvoering van de politietaak is aangelegd en niet door de politie wordt bijgehouden.

tie van dit register te verbeteren met behulp van ongericht dataminingonderzoek.<sup>7</sup> Gestreefd wordt naar het verkrijgen van een zo volledig mogelijk beeld van de mogelijkheden van gegevensverwerking ten behoeve van de opsporingstaak.

#### **Werkwijze van het Meldpunt**

Het Meldpunt onderzoekt en beoordeelt via vier hoofdprocessen of ongebruikelijke transacties verdacht zijn<sup>8</sup>, namelijk:

- een automatische match met de politieregisters voor CIE- en onderzoekssubjecten<sup>9</sup>;
- een periodieke match met BOOM;
- verzoeken om informatie van opsporingsdiensten (LOvJ-verzoeken);
- eigen onderzoek en analyse.

#### **Vergelijking met CIE/MRO-bestanden**

Door het Meldpunt worden dagelijks alle nieuw binnengekomen meldingen vergeleken met de Verwijzingsindex Recherche Onderzoeken & Subjecten (VROS). Daarin staan personen geregistreerd die zich schuldig (gaan) maken aan rechtsorde schokkende misdrijven (CIE-subjecten) en personen die onderwerp zijn van opsporingsonderzoek bij rekercheteams van politie en bijzondere opsporingsdiensten (MRO-subjecten). Het Meldpunt koppelt elke ongebruikelijke transactie, zodra die is geregistreerd, aan deze registers. Wanneer de persoon die de ongebruikelijke transactie heeft verricht in het politieregister voorkomt, is de transactie onherroepelijk verdacht. Verdere beoordeling door het Meldpunt is dan niet meer nodig. Het kan voorkomen dat een persoon die een ongebruikelijke transactie heeft verricht op een later tijdstip door de politie wordt aangemeld als CIE- of MRO-subject. Om te voorkomen dat deze de dans ontspringt, vindt maandelijks een ‘rematch’ plaats, waarbij de gehele inhoud van het register-MOT nog eens naast de VROS wordt gelegd.

---

7. Hoewel een hulpverleningsregister ook een aparte positie inneemt, zal niet nader worden ingegaan op een verbetering van de informatiepositie van dat register. Een zodanige verbetering kan in beginsel namelijk niet worden aangemerkt als een verbetering van de informatiepositie ten behoeve van de strafrechtelijke handhaving van de rechtsorde. Daarvoor staat de doelstelling van het hulpverleningsregister te ver af van het doel waarvoor het dataminingsproces in dit onderzoek wordt gebruikt.

8. *Jaarverslag* 2003, p. 27.

9. Meldingen rechercheonderzoeken. Met de MRO's ontstaat een landelijk overzicht van de onderzoeken die de politie uitvoert. Voor het melden van rechercheonderzoeken geldt een ondergrens. Alle onderzoeken die langer dan een week duren en die gericht zijn op misdrijven waarvoor voorlopige hechtenis is toegelaten worden geregistreerd.

### **Vergelijking BOOM**

Sedert oktober 2002 wordt het register van het Meldpunt ook periodiek vergeleken met het bestand van het Bureau Ontnemingswetgeving Openbaar Ministerie (BOOM). Dit bestand bevat personen tegen wie een strafrechtelijk financieel onderzoek, dan wel een ontnemingsvordering loopt.

### **Verzoek van de LOvJ**

Een registratie in het register-MOT kan ook als verdacht worden aangemerkt naar aanleiding van een verzoek van de LOvJ. In deze verzoeken vragen opsporingsdiensten via de LOvJ het Meldpunt om informatieverstrekking over verdachte personen in een politieonderzoek. Daarbij gaat het om een specifiek (gericht) verzoek tot toetsing van een derde partij, op grond waarvan in het geval van een match de betreffende registratie als verdacht wordt aangemerkt. Deze methode past niet zozeer bij de ongerichte alswel bij de gerichte dataminingsvariant. Het betreft een bevraging waarbij het initiatief niet bij het Meldpunt ligt.

### **Verdenking op andere gronden**

Transacties die na de bovenstaande analyses niet direct verdacht lijken, kunnen op een vierde manier worden geanalyseerd. Met behulp van netwerkanalyses, open bronnen en typologisch onderzoek doorkruist het Meldpunt zijn database en beoordeelt zo transacties op hun verdachtheid. Omdat het praktisch ondoenlijk is al deze transacties afzonderlijk te beoordelen maakt men gebruik van dataminings technieken. Dit is mogelijk aangezien vrijwel alle informatie in digitale vorm wordt aangeleverd en verwerkt. Het Meldpunt filtert de gegevens in het register-MOT aan de hand van diverse criteria; bijvoorbeeld een indicator, een typologie, een bepaalde valuta, een melder of een relevante actualiteit. Verder wordt het register gescand op namen van (rechts)personen. Op basis van eigen kennis, nieuwsberichten in kranten of andere bronnen worden regelmatig ongebruikelijke transacties ontdekt die, na nader onderzoek, verdacht blijken. Aan de hand van één verdachte transactie kunnen volledige netwerken van dergelijke transacties aan het licht komen. Omdat het handmatig nazoeken van personen veel tijd in beslag nam heeft het Meldpunt een programma ontwikkeld, dat de transacties binnen een netwerk automatisch aan elkaar relateert. Gezien de functionaliteit van deze programma-tuur kan worden gesproken van een 'dataminings tool', een stukje software waarmee dataminingsonderzoek kan worden verricht. De methode, gebaseerd op het analyseren van het register-MOT op transactiepatronen die samen een verdacht beeld opleveren<sup>10</sup>, heeft in beginsel alleen betrekking op het register-MOT zelf.

---

10. Terlouw & Aron 1996.

### 8.1 Toepassing van ongericht dataminingonderzoek

Zoals reeds gesteld zijn de mogelijkheden onderzocht ter verbetering van de informatiepositie van het register-MOT met behulp van (onggericht) dataminingonderzoek. Om te beginnen wordt kort ingegaan op de functies van het register-MOT, waarna wordt bekeken of de werkzaamheden van het Meldpunt kunnen worden aangemerkt als dataminingonderzoek. Vervolgens zullen de specifieke eigenschappen van het register-MOT worden getoetst aan de kenmerken van de ongerichte dataminingsvariant.

#### Functies register-MOT en dataminingonderzoek

Bij het register-MOT gaan de functies van registratie en analyse hand in hand. Het register-MOT wordt aangelegd voor het analyseren van gegevens omtrent financiële transacties. Gegevens over ongebruikelijke transacties, die verplicht aan het Meldpunt worden verstrekt, worden als zelfstandig subject geregistreerd. In het kader van de analyse van deze gegevens worden gegevens in het register-MOT vastgelegd. Ten aanzien van het gebruik van de gegevens vormt dit onderscheid naar registratiegrond nauwelijks een probleem. Gezien de gevoelige aard van de gegevens die worden verwerkt, voorziet het register namelijk middels een beperkt verstrekkingenregime in een verantwoorde registratie. Op grond daarvan kunnen de gegevens in het register-MOT, ongeacht de registratiegrond<sup>11</sup> in beginsel niet worden geraadpleegd. Dat sluit de mogelijkheid om deze aan te wenden in het kader van een dataminingonderzoek met betrekking tot een ander register welhaast uit. Voor een dataminingonderzoek met betrekking tot het register-MOT zelf opent het echter wel perspectieven.<sup>12</sup>

#### Datamining of registervergelijking?

Ter beantwoording van de vraag of het mogelijk is om (onggericht) dataminingonderzoek te verrichten met betrekking tot het register-MOT dient te worden vastgesteld of de werkzaamheden die het Meldpunt verricht kunnen worden aangemerkt als dataminingonderzoek. Over die werkzaamheden kan worden gesteld, dat aan het algemeen beheer van het register-MOT en de daarbij horende taken vorm gegeven kan worden met behulp van dataminingonderzoek. Het verrichten van een ongericht dataminingonderzoek kan in dat verband worden gerekend tot het beheer van het register-MOT. Ook een toetsing van het register-MOT met een CIE/MRO-bestand kan worden uitgelegd als 'het trekken van kennis uit de database'. Er is sprake van een verwerking aan de hand waarvan men (nieuwe) kennis tracht te destilleren uit de gegevens in het register-MOT. Zonder een dergelijke toetsing is het veel moeilijker, zo niet onmogelijk, om een eventuele match te ontdekken. De analysemethoden van het Meldpunt lijken daarmee te vol-

---

11. De gegevens in het datawarehouse worden uitsluitend gebruikt in het kader van de analyse waartoe ze zijn vastgelegd.

12. Zie ook sectie 8.2.4.

doen aan de (ruwe) definiëring van datamining: het in het kader van het dataminingsproces bewerken van gegevens(bestanden), ter verkrijging van informatie die zonder deze bewerking niet zichtbaar/voorhanden is (of slechts met veel grotere inspanning kan worden verkregen).<sup>13</sup>

Het Meldpunt stelt zich echter op het standpunt dat de hierboven beschreven analysemethoden niet als datamining kunnen worden aangemerkt, omdat bij de aanvang daarvan reeds bekend is waarnaar wordt gezocht.<sup>14</sup> Dat feit behoeft echter geen belemmering te vormen om te kunnen spreken van dataminingonderzoek. Bij ieder dataminingonderzoek dient, ten minste in grote lijnen, om de volgende twee redenen een doelstelling aanwezig te zijn. Gegevens die in het kader van een dataminingonderzoek worden verwerkt kunnen in beginsel steeds worden aangemerkt als informatie. Zij hebben een bepaalde betekenis voor het onderzoek en zijn op grond daarvan geselecteerd. Een zodanige selectie is slechts mogelijk wanneer tot op zekere hoogte bekend is waarnaar men op zoek is. In die zin is dus sprake van een doel. Daarnaast is ook voor een juridische grondslag voor het mogen verwerken van gegevens een duidelijk doel noodzakelijk. Met het oog op de bescherming van de persoonlijke levenssfeer is een willekeurige verwerking van persoonsgegevens uitgesloten. Of er sprake is van dataminingonderzoek wordt bepaald door het antwoord op de vraag, of de bewerking die plaatsvindt betrekking heeft op een bepaalde of op een onbepaalde groep van personen.<sup>15</sup> Alleen in het laatste geval is sprake van dataminingonderzoek, aangezien een bewerking in het eerste geval gericht is op een verificatie van gegevens waarover al wordt beschikt.

### Commissie Mevis

De visie van de commissie Mevis vertoont raakvlakken met die van het Meldpunt waar het gaat om de kwalificatie van de werkzaamheden van de laatste. Volgens de commissie is een verstrekking van gegevens uit een register zware criminaliteit ten behoeve van het register-MOT registervergelijking, en geen datamining.<sup>16</sup> Onder registervergelijking verstaat de commissie het genereren van nieuwe gegevens door het koppelen *of* vergelijken van registers. Bij het koppelen of vergelijken van registers worden gegevens vergaard,

13. Zie ook sectie 1.3.2.

14. *Jaarverslag* 2001, p. 9, 'Toch bestaat er een manier om gegevens uit de database te halen zonder dat je van tevoren weet waar je naar zoekt. Deze selectieprocedure, die het Meldpunt in 2001 verder uitbouwt, heet data mining. Data mining is te omschrijven als "kennis uit de database trekken". Daar waar het Meldpunt tijd-winst heeft gecreëerd met de doormeldmodule, heeft het ruimte om de schat aan informatie, die het in alle jaren heeft verzameld, adequaat te gebruiken. Data mining ontdekt, met behulp van analysetechnieken, onbekende patronen in een grote hoeveelheid gegevens. Het Meldpunt verwacht in 2001 de eerste stappen te zetten om data mining in te voeren.'

15. Zie hoofdstuk 6.

16. Commissie Mevis 2001, p. 31.

waarna de gegevens uit het ene register als het ware naast de gegevens uit het andere register worden gelegd. Zo kunnen gegevens worden vergeleken of aangevuld, waardoor nieuwe informatie ontstaat. De commissie stelt zich op het standpunt dat dergelijk gericht onderzoek niet strookt met de aard van datamining. Dit standpunt strookt echter niet met de eerder uit dit dissertatieonderzoek voortgekomen vaststelling, dat ook een onderzoek waarbij gericht wordt gezocht als dataminingonderzoek kan worden aange-merkt. Registervergelijking en datamining dienen niet als twee los van elkaar staande zaken te worden gezien. Registervergelijking staat niet naast (het) datamining(sproces), maar maakt daar als bewerking van de verkregen informatie deel van uit. In die zin kan in het kader van de werkzaamheden van het Meldpunt wel degelijk worden gesproken van toepassing van dataminingonderzoek.

Alvorens de toepassing van het ongericht dataminingonderzoek aan bod komt, dient eerst te worden vastgesteld of het mogelijk is om met een ongericht dataminingonderzoek een verbetering van de informatiepositie van het register-MOT na te streven. Daartoe is de verwerking die in kader van het register-MOT plaatsvindt getoetst aan de kenmerken van een ongericht dataminingonderzoek.

### Doel

Het register-MOT dient een specifieke taak, hetgeen blijkt uit de beperkte doelstelling van dit register. Hoewel de nadruk ligt op het bestrijden van het witwassen van geld, is het register tevens een instrument voor de bestrijding van misdrijven in meer algemene zin. Dankzij de meldingsplicht wordt de informatiepositie van de overheid bij de rechtshandhaving versterkt<sup>17</sup> en wordt zicht verkregen op degenen die crimineel verworven middelen via het financiële stelsel proberen wit te wassen. Het Meldpunt heeft onder meer tot taak de gemelde gegevens te analyseren en te vergelijken met andere gegevensbestanden, waardoor feiten kunnen worden ontdekt die voor de opsporing en vervolging van misdrijven van belang zijn. Aangezien het register-MOT dus niet op één, maar op alle ongebruikelijke transacties die in dit centrale register worden vastgelegd ziet, zal het onderzoek gericht zijn op de informatieverbetering van een volledig register en niet op die van een bepaald geval. Gezien de aard van een ongericht dataminingonderzoek ligt de toepassing daarvan op die kerntaak van het Meldpunt dan ook het meest voor de hand. Met het oog op het doel van het register-MOT is besloten dat, alvorens daarvan reeds sprake is, een onderzoek naar eventuele verdachte transacties mogelijk dient te zijn middels systematische controle van in het register opgeslagen gegevens. Dit betekent dat, anders dan normaliter toegestaan, ongericht onderzoek wordt verricht naar in beginsel onverdachte personen; dit op grond van, aan de hand van een aantal indicatoren<sup>18</sup>,

---

17. *Kamerstukken II*, 1993/94, 23009, nr. 12, p. 791.

18. Art. 8 lid 1 Wet MOT.

geselecteerde ongebruikelijke transacties. Eerst daarna wordt gecontroleerd of die transacties een verdenking opleveren.<sup>19</sup>

### **Inbreuk privacy**

Met een ongericht dataminingonderzoek mag geen ontoelaatbare inbreuk op de persoonlijke levenssfeer worden gemaakt. Het is een ingrijpend middel, waarvoor een wettelijke grondslag aanwezig dient te zijn. Een verwerking in het kader van het register-MOT heeft per definitie betrekking op onverdachte personen<sup>20</sup>, hetgeen een inbreuk op de persoonlijke levenssfeer met zich kan meebrengen. Bij de afweging van het belang van de burger bij de bescherming van zijn persoonlijke levenssfeer tegenover het maatschappelijk belang bij het voorkomen van misbruik van het financiële stelsel, heeft men het laatste laten prevaleren en daarvoor een wettelijke grondslag gecreëerd. Het beperkte verstrekkingenregime van het register-MOT moet voorkomen, dat de betreffende gegevens buiten de genoemde rechtvaardigingsgrond om worden verwerkt. Dit laat onverlet, dat niet op een wettelijke grondslag berustende verwerking van gegevens ten behoeve van het register-MOT in beginsel steeds resulteert in een ontoelaatbare inbreuk op de privacy.

### **Tijdelijk of permanent karakter**

Een ongericht dataminingonderzoek met betrekking tot het register-MOT is in beginsel permanent van aard. Er wordt voortdurend gestreefd naar een zo optimaal mogelijk gebruik van de gegevens in het register. De behoefte aan een goede informatiepositie is daarbij constant aanwezig en het register wordt dan ook voortdurend aangevuld en bijgewerkt met nieuwe gegevens. Hoewel de samenstelling van het register-MOT dus steeds verandert, zal het onderzoek zelf gewoon doorlopen. De vraag waarin het register-MOT specifiek voorziet is daardoor steeds aanwezig. Voor de kwalificatie van het register-MOT heeft de wetgever derhalve niet gekozen voor een tijdelijk, maar voor een gewoon politieregister met een in beginsel permanent karakter. Dit karakter is typerend voor de ongerichte dataminingsvariant.

### **Gebruik van externe gegevens**

Bij een verwerking van gegevens in het kader van het register-MOT zal overwegend gebruik worden gemaakt van externe gegevens. Eventuele inbreuken op de persoonlijke levenssfeer worden in beginsel gerechtvaardigd door de wettelijke grondslag waarop die verwerking berust. Hetzelfde geldt voor het gebruik van externe gegevens, waarmee

---

19. Hier kan een vergelijking worden getrokken met de praktijk van het preventief fouilleren. Ook daarbij mag (preventief) worden opgetreden zonder dat sprake is van een gerichte verdenking. De beslissing om daarbij over te gaan tot een actief overheidsoptreden tegen burgers wordt genomen aan de hand van een aantal algemene indicatoren en op basis van een wettelijke grondslag.

20. *Kamerstukken II*, 1997/98, 25 398, nr. 6, p. 5.

terughoudend dient te worden omgegaan. Dit is dan ook alleen toegestaan voor zover vallende binnen de grenzen van de wettelijke regeling voor het register-MOT. Daarbij is de bevoegdheid voor een verstrekking van gegevens aan het register, die daaraan kan worden ontleend, beperkt. Een verstrekking aan het register zal in beginsel een gericht (lees: beperkt), karakter hebben. Een verstrekking van gegevens aan het Meldpunt is toegestaan, wanneer en voor zover het Meldpunt die gegevens nodig heeft voor een goede uitvoering van haar taak.<sup>21</sup> Dit betekent in de praktijk, dat kan worden volstaan met een minimale verstrekking. De bijzondere positie van het register-MOT verschaft de mogelijkheid tot het verwerken van gegevens op een wijze, die zonder de wettelijke regeling voor dit register niet mogelijk zou zijn. Vanwege die uitzonderingspositie ligt een restrictieve hantering van de bevoegdheden van het Meldpunt voor de hand.

### Resumerend

Er zijn geen directe belemmeringen voor de verbetering van de informatiepositie van het register-MOT met behulp van ongericht dataminingonderzoek.

## 8.2 Vier verschillende onderzoeksmogelijkheden

In de hierna volgende secties wordt onderzocht welke gegevens uit welke (politie)registers gebruikt mogen worden ten behoeve van een ongericht dataminingonderzoek, en wel aan de hand van de volgende situaties:

- er wordt geen gebruik gemaakt van externe gegevens;
- er wordt gebruik gemaakt van externe gegevens die niet afkomstig zijn uit een politie-register;
- er wordt gebruik gemaakt van externe gegevens afkomstig uit een gewoon politieregister;
- er wordt gebruik gemaakt van externe gegevens afkomstig uit een bijzonder politie-register.

### 8.2.1 Geen gebruik externe gegevens

Het is mogelijk te streven naar een efficiënter gebruik van de gegevens in het register-MOT zonder daarvoor gebruik te maken van externe gegevens. Reeds geregistreerde transacties kunnen in samenhang met elkaar voldoende reden vormen om een bepaalde transactie als verdacht aan te merken. Een dergelijk onderzoek kan plaatsvinden door het register aan de hand van verscheidene indicatoren te analyseren op transactiepatronen die samen een verdacht beeld opleveren<sup>22</sup>; daarvoor bestaan in beginsel geen juridische belemmeringen. Het staat de beheerder van het register-MOT vrij, rechtmatig verkregen

---

21. Art. 14 lid 3 BPolr.

22. Terlouw & Aron 1996.

gegevens te bewerken teneinde het nut ervan te vergroten. Omdat het register-MOT een politieregister is in de zin van art. 1 lid 1 onder *c* WPolr dient – in het geval van een ongericht dataminingonderzoek met betrekking tot dit register – rekening te worden gehouden met de voorwaarden die voortvloeien uit de WPolr en het BPolr en samenhangen met de politietaak, het doelbindingsbeginsel en de uitvoering van het onderzoek. Dit gegeven wordt onderstaand nader uitgewerkt. Daarnaast wordt kort ingegaan op de kwalificatie van het datawarehouse voor het register-MOT.

### **De politietaak**

Hoewel de specifieke taak van het Meldpunt nauw gerelateerd is aan de politietaak, wordt het register-MOT niet rechtstreeks ten dienste van de uitvoering van die taak aangelegd en wordt niet door de politie bijgehouden.<sup>23</sup> Toch vervult het een belangrijke rol bij de bestrijding van het misbruik van het financiële stelsel. Een goede informatiepositie vormt de basis voor een succesvolle uitvoering van de opsporingstaak. Het register draagt bij aan de politietaak voor zover het de strafrechtelijke handhaving van de rechtsorde betreft. Voor het verkrijgen van een informatiepositie kan gebruik worden gemaakt van het dataminingsproces. Daarbij dient het – ongerichte – dataminingonderzoek met het oog op de specifieke taak van het Meldpunt steeds noodzakelijk te zijn. Op grond van art. 2 lid 2 onder *c* Wbp is de Wbp niet van toepassing op de verwerking van persoonsgegevens ten behoeve van de uitvoering van de politietaak, omschreven in art. 2 Politiewet 1993. Gezien het feit dat het register-MOT niet direct wordt bijgehouden in het kader van de politietaak is het wenselijk, dat duidelijker wordt aangegeven welke positie dat register nu precies inneemt. Die positie is immers bepalend voor de vraag of de Wbp al dan niet van toepassing is op een gegevensverwerking door het Meldpunt.

### **Het doelbindingsbeginsel**

Zoals reeds opgemerkt dient het ongerichte dataminingonderzoek met het oog op de specifieke taak van het Meldpunt noodzakelijk te zijn. Dit vloeit voort uit het doelbindingsbeginsel en is voor een ongericht dataminingonderzoek in beginsel altijd het geval, aangezien daarmee wordt gestreefd naar een verbetering van de informatiepositie van het basisregister.<sup>24</sup>

### **Uitvoering**

Het is wenselijk dat het ongerichte dataminingonderzoek wordt uitgevoerd door, dan wel onder het gezag van de beheerder van het register-MOT. De beheerder heeft met betrekking tot het door hem beheerde register een algemene zorgplicht.<sup>25</sup> Daartoe kan

---

23. *Kamerstukken II*, 1996/97, 25 398, nr. 3, p. 2.

24. Zie sectie 7.3.1.2

25. Art. 7 WPolr.

ook het streven naar een zo hoog mogelijk rendement van het register worden gerekend. Bovendien wordt hiermee voorkomen dat in het kader van het ongericht dataminingonderzoek een verstrekking plaatsvindt. Van een zodanige verstrekking is sprake wanneer het onderzoek door een derde wordt uitgevoerd. In dat laatste geval (bij een zodanige verstrekking) zijn de waarborgen die gelden bij een intern onderzoek en samenhangen met de kwalificatie van het datawarehouse niet langer per definitie aanwezig.

#### **Kwalificatie datawarehouse**

Voor een ongericht dataminingonderzoek met betrekking tot een gewoon politieregister geldt in beginsel dat het niet noodzakelijk is te voorzien in een apart datawarehouse en een bijbehorend reglement. Het onderzoek kan worden uitgevoerd binnen de kaders van het reeds bestaande register en reglement. Aangezien het register-MOT een gewoon politieregister is, kan het in geval van een ongericht dataminingonderzoek als basisregister worden gebruikt; de inhoud van het datawarehouse zal immers overeenkomen met de inhoud van dat register. Daarnaast impliceert de specifieke aard van het register-MOT, dat met een ongericht dataminingonderzoek uitvoering wordt gegeven aan de kerntaak van dat register. Anders dan bij de overige gewone politieregisters, die de algemene politietaken dienen en waarbij het verkrijgen van een goede informatiepositie onderdeel uitmaakt van de toepassingsmogelijkheden van het register, kan van een register-MOT worden gezegd dat een verbetering van de informatiepositie (met behulp van bijvoorbeeld dataminingstechniek) behoort tot de standaardactiviteiten die van de beheerder van dat register verwacht mogen worden. Ook als basisregister zal het register-MOT, in combinatie met het bestaande reglement, afdoende voorzien in de verwerkingsmethoden die worden gebruikt bij het vervullen van de kerntaken van dat register. Het ligt daarom voor de hand het onderzoek uit te voeren binnen de bestaande kaders van dat register.

#### *8.2.2 Het gebruik van externe, niet uit een politieregister afkomstige gegevens*

Het uitvoeren van een ongericht dataminingonderzoek zonder daarbij gebruik te maken van externe gegevens is slechts één van de manieren waarop het Meldpunt uitvoering geeft aan haar taak. Zonder externe gegevens is het echter onmogelijk om de toetsing in het kader van het register-MOT te realiseren. De noodzaak van verstrekking van gegevens door derden bij toetsing wordt ook door de wetgever onderkend en blijkt uit een aparte regeling in de WPolr en het BPolr inzake de gegevensverstrekking ten behoeve van het register-MOT.<sup>26</sup>

In deze sectie wordt onderzocht in hoeverre het Meldpunt bij een ongericht dataminingonderzoek gebruik kan maken van gegevens die afkomstig zijn van bronnen buiten de politieke sfeer. Daarbij geldt wederom dat een verwerking noodzakelijk dient te zijn; gezien het doel van het register-MOT, waarbij het gaat om misdrijven, lijkt een ver-

---

26. Art. 13a lid 4 en 13b lid 2 WPolr en art. 14 lid 3 BPolr.

werking aanvaardbaar. Daarnaast dient sprake te zijn van een wettelijke grondslag. Wanneer het gaat om gegevens, niet zijnde persoonsgegevens, kan een verwerking daarvan worden gerechtvaardigd door art. 3 Wet MOT. Daar is bepaald dat het Meldpunt de gegevens die het verkrijgt verzamelt, registreert, bewerkt en analyseert, teneinde te bezien of zij van belang kunnen zijn voor de voorkoming en opsporing van misdrijven. Het artikel spreekt duidelijk over 'gegevens die het Meldpunt verkrijgt'. Dit lijkt erop te wijzen dat het Meldpunt in beginsel een passieve rol heeft bij het verzamelen van gegevens. Aangezien het Meldpunt de verkregen gegevens echter ook dient te analyseren is voor de verwerking van externe gegevens, niet-zijnde persoonsgegevens, voor die taak in art. 3 Wet melding ongebruikelijke transacties een wettelijke grondslag gelegd. Die algemeen gestelde grondslag volstaat niet voor de verwerking van externe gegevens die wel als persoonsgegevens kunnen worden aangemerkt. Het gebruik van die categorie externe gegevens kan verder worden beperkt door de aard van de gegevens en die van het ongerichte dataminingonderzoek, alsmede van de koppelingsregeling van art. 6 WPolr.

#### 8.2.2.1 *De aard van ongericht dataminingonderzoek*

Het adagium 'if there is no crime, there is no investigation' impliceert, dat het de politie niet is toegestaan registers waarin onverdachte burgers zijn geregistreerd, te koppelen. Daarnaast is het Meldpunt geen opsporingsinstantie en heeft zelf geen (strafrechtelijke) opsporingsbevoegdheden.<sup>27</sup> Wanneer het Meldpunt een ongericht dataminingonderzoek verricht is dat geen 'politiële' activiteit. Uit art. 3a Wet MOT<sup>28</sup> kan wel worden afgeleid dat een zodanig dataminingonderzoek (indirect) gericht is op de strafrechtelijke handhaving van de rechtsorde. In het kader hiervan is het onwenselijk dat gebruik wordt gemaakt van gegevens die betrekking hebben op onverdachte burgers. Bepaalde situaties kunnen aanleiding vormen tot het volgen van onverdachte burgers in bepaalde aspecten van hun gedrag teneinde vast te stellen, of dezen zich schuldig maken (of hebben gemaakt) aan strafbare feiten. Deze activiteit is veeleer een vorm van toezicht, aangezien nog geen sprake is van enig strafbaar feit. De daaraan gerelateerde bestanden zijn daarom afgescheiden van de overige politieregisters, zoals ook het register-MOT.<sup>29</sup>

De Nota WES maakt duidelijk dat vooral bij het bevragen van bestanden op een op voorhand onbepaalde groep van personen terughoudendheid dient te worden betracht. Een verwerking van deze gegevens betreft een ingrijpend middel, waarmee inbreuk wordt gemaakt op de persoonlijke levenssfeer. In beginsel behoeven degenen die in het register-MOT zijn geregistreerd zich die bemoeienis slechts te laten welgevalen, wanneer

27. Zie *Richtsnoeren* 2003.

28. Het Meldpunt heeft tot taak: het verzamelen, registreren, bewerken en analyseren van de gegevens die het verkrijgt, teneinde te bezien of deze gegevens van belang kunnen zijn voor de voorkoming en opsporing van misdrijven.

29. *Kamerstukken II*, 1997/198, 25 880, nrs. 1-2, p.84.

het doel van een verwerking uitdrukkelijk wordt gerechtvaardigd. Wanneer een expliciete wettelijke bevoegdheid daartoe ontbreekt, mag niet worden gekoppeld met (andere) bestanden waarin onverdachte burgers zijn geregistreerd. Het actief en gericht speuren naar externe gegevens naar aanleiding van een registratie in het register-MOT buiten de wettelijke grondslag om is een ontoelaatbare inbreuk op de persoonlijke levenssfeer, aangezien dit leidt tot een bemoeienis met personen ten aanzien waarvan nog geen enkel aanknopingspunt bestaat dat zij in enige relatie staan tot strafbaar gedrag.<sup>30</sup>

#### **Registratie onverdachte personen**

In art. 5a WPolr wordt bepaald, dat de opslag van zachte opsporingsinformatie ten behoeve van de opsporing in een gewoon politieregister (ongeacht het strafbare feit) slechts mogelijk is voor korte duur. Alleen wanneer gegevens over onverdachte personen voldoen aan de voor de bijzondere politieregisters geldende criteria kunnen zij worden opgenomen in een bijzonder politieregister overeenkomstig de regels van par. 3a WPolr. Gezien de met art. 5a WPolr gepaard gaande beperking van de mogelijkheid van analyse van de in het (gewone) register-MOT opgenomen gegevens, is voor dat register daarop een uitzondering gemaakt in art. 5a lid 1 onder b WPolr. Het belang van het register-MOT kan een vergaande inbreuk op de persoonlijke levenssfeer rechtvaardigen.

Met het oog op de bescherming van de persoonlijke levenssfeer is voor de bijzondere politieregisters duidelijk vastgelegd wanneer (zachte) gegevens verwijderd en vernietigd dienen te worden. In de Wet MOT ontbreekt een dergelijke termijnstelling echter. Het reglement bij het register-MOT kent wel bepalingen betreffende de verwijdering en vernietiging van de in het register opgenomen gegevens. Op grond van art. 8 lid 1 van het reglement worden de gegevens in het register-MOT verwijderd, wanneer deze niet meer noodzakelijk zijn voor het doel van het register. Het tweede lid van art. 8 bepaalt dat na verloop van vijf jaren na datum van laatste opname de registratie van de gegevens niet langer noodzakelijk is voor het doel van het register.<sup>31</sup> Voor de registratie van personen die betrokken zijn bij een verdachte transactie geldt een uitzondering. Die gegevens behoeven pas na verloop van tien jaar na datum van de laatste opname worden verwijderd. Het is echter de vraag of deze regeling, in navolging van de bijzondere politieregisters, geen wettelijke grondslag behoeft.

#### *8.2.2.2 Koppeling*

Omdat het register-MOT betrekking heeft op een onbepaalde groep van personen, is bij een verwerking van externe gegevens in beginsel sprake van een koppeling (en niet van

---

30. Bij de personen ten aanzien waarvan nog geen enkel aanknopingspunt bestaat dat zij in enige relatie staan tot strafbaar gedrag, kan het gaan om de personen in een register-MOT maar ook om de personen waarop de externe gegevens betrekking hebben.

31. Aldus ook *Kamerstukken I*, 1993/94, 23 008 en 23 009, nr. 76b, p. 2.

een incidentele bevraging). In de praktijk zal onvermijdelijk sprake zijn van een grijs gebied wanneer het gaat om de vraag, wanneer nog kan worden gesproken van meerdere individuele bevragingen en het moment waarop sprake is van koppeling. Omdat een ongericht dataminingonderzoek gericht is een verbetering van de informatiepositie van het register als geheel zal het hierbij in beginsel om een koppeling gaan. Dit betekent dat het reglement van het register-MOT op grond van art. 6 lid 2 in de mogelijkheid van een koppeling dient te voorzien. Van een koppeling is geen sprake indien de betreffende externe gegevens geen deel uitmaken van enig register, hetgeen het geval is bij gegevens uit de media of uit eigen kennis. Een koppeling is alleen mogelijk met een ander politieregister of met een persoonsregistratie van het Rijk, provincies, gemeenten en andere openbare lichamen, met inbegrip van de daaronder ressorterende diensten, instellingen en bedrijven<sup>32</sup>. Een koppeling met andere bestanden is niet mogelijk.<sup>33</sup> Dit impliceert dat een incidentele bevraging van gegevens op het internet eventueel mogelijk is, maar een koppeling met die gegevens niet. Bij een koppeling in het kader van een ongericht dataminingonderzoek zullen externe gegevens worden vastgelegd in het register-MOT. Op grond van art. 4 lid 2 WPoI dient in dat geval die registratie (en daarmee ook de koppeling) van externe (persoons)gegevens in het register-MOT noodzakelijk te zijn voor het doel van het register. Hiermee is sprake van een indirecte doelbinding.

### Privacyreglement MOT

Het Privacyreglement Meldpunt Ongebruikelijke Transacties 1999 (hierna: reglement) van het register-MOT voorziet in de mogelijkheid om te koppelen. In art. 13 lid 1 onder *a* van het reglement wordt bepaald dat een koppeling met een ander politieregister of een register als bedoeld in art. 17 aanhef en onder *a* Wpr mogelijk is, voor zover deze koppeling noodzakelijk is voor het doel van het register-MOT. Daarmee wordt het belang van de doelbinding bevestigd.

#### 8.2.2.3 *Vrijwillige verstrekking van gegevens*

Persoonsgegevens die buiten de wettelijke regeling om, op vrijwillige basis, worden verstrekt aan het Meldpunt zullen, gezien de inbreuk op de persoonlijke levenssfeer en het doelbindingsbeginsel, in principe niet mogen worden verwerkt.<sup>34</sup> Het alternatief van de vrijwilligheid voorziet niet in een regeling die voldoet aan de eisen van art. 10 Gw en art. 8 EVRM. In die eisen wordt gesteld dat bevoegdheden die een inbreuk op de persoonlijke levenssfeer kunnen inhouden bij wet moeten zijn voorzien, en dat die wette-

32. Zoals bedoeld in art. 17, aanhef en onder *a* Wpr.

33. Art. 4 lid 1 BPolr.

34. Zie ook *Kamerstukken II*, 2001/02, 28 059, nr. 3, p. 20 Wanneer met het wetsvoorstel 'Vorderen gegevens telecommunicatie' wordt voorzien in een wettelijke regeling om bepaalde gegevens te vorderen, sluit dat een verstrekking van gegevens op vrijwillige basis in beginsel uit.

lijke regeling moet voldoen aan eisen van toegankelijkheid en voorzienbaarheid en waarborgen moet bevatten tegen willekeur. Indien vrijwilligheid voorop staat en de tot opsporing bevoegde instantie in overleg met de houder van de gegevens komt tot afspraken aangaande welke gegevens in een bepaald geval verstrekt zullen worden, is van een wettelijke regeling die aan deze eisen voldoet geen sprake.<sup>35</sup> Doorslaggevend is de vraag, wie het initiatief tot een vrijwillige verstrekking neemt. Het Meldpunt kan zelf niet om een verstrekking verzoeken. In het geval van een tip zal de informatie wel gebruikt kunnen worden, en wel door deze te vergelijken met de reeds in het register-MOT aanwezige gegevens.

#### *8.2.2.4 Gebruik van gegevens uit openbare registers*

Het lijkt in beginsel niet mogelijk om gebruik te maken van persoonsgegevens uit openbare registers ten behoeve van ongericht dataminingonderzoek ter verbetering van de informatiepositie van het register-MOT. Buiten een verkennend onderzoek, verdenking of een andere 'uitvoering van de politietaak in een bepaald geval' mag niet zonder meer gebruik worden gemaakt van gegevens uit een openbaar register ten behoeve van de opsporing.<sup>36</sup> Hoewel het register-MOT niet door de politie wordt bijgehouden, vindt de verwerking van de gegevens in dit register plaats met het oog op de opsporing.

Op grond van art. 4 WPolr mogen persoonsgegevens alleen worden verwerkt indien dat noodzakelijk is voor de uitvoering van de politietaak. Dit betekent dat het niet mogelijk is om gegevens te vergaren over een onbepaalde groep van burgers voor algemene politieke doeleinden, ook niet uit openbare bronnen. Hoewel het Meldpunt gegevens vergaart met het oog op een bepaald doel, ligt aan die vergaring geen verdenking ten grondslag. Er is geen sprake van een verkennend onderzoek, verdenking of andere 'uitvoering van de politietaak in een bepaald geval'. In dit verband zij daarom nogmaals gewezen op het belang om aan een ongebruikelijke transactie de kwalificatie van verdenking te koppelen. Daardoor wordt het mogelijk om ook gebruik te maken van openbare bronnen. Nu dit (nog) niet het geval is, lijkt het gebruik van openbare bronnen slechts mogelijk indien en voor zover hiervoor een uitdrukkelijke wettelijke grondslag aanwezig is.

#### **Resumerend**

Het gebruik van externe gegevens die afkomstig zijn van buiten de politieke sfeer is in beginsel beperkt tot het open houden van ogen en oren of door de verwerking van algemene<sup>37</sup> resultaten van een fenomeenonderzoek die voor het register-MOT een toegevoegde waarde (kunnen) vertegenwoordigen. Zo kan het Meldpunt op basis van eigen

---

35. *Kamerstukken II*, 2001 /02, 28 366, nr. 1, p. 5.

36. *Kamerstukken II*, 1998 /99, 26 410, nr. 3.

37. Met 'algemeen' wordt hier bedoeld dat de gegevens niet in enig stadium zijn te herleiden tot een individueel natuurlijk persoon.

kennis of door nieuwsberichten op ongebruikelijke transacties stuiten, die na nader onderzoek verdacht blijken.<sup>38</sup> Het actief zoeken naar, dan wel het koppelen met, persoonsgegevens zonder dat hiervoor een wettelijke grondslag is, lijkt niet mogelijk. Een verwerking van persoonsgegevens ten behoeve van de werkzaamheden van het Meldpunt dient voorts te voldoen aan het noodzakelijkheidsvereiste. Met het oog hierop kan worden overwogen om niet te spreken van een ongebruikelijke transactie, maar van een verdenking dan wel vermoeden van een strafbaar feit.

### 8.2.3 Gebruik van gegevens uit een gewoon politieregister

In deze sectie wordt ingegaan op de vraag op welke wijze bij een ongericht dataminingonderzoek gebruik kan worden gemaakt van de externe gegevens die in de overige gewone politieregisters zijn opgeslagen. Met betrekking tot de gegevens in de gewone politieregisters is in beginsel sprake van een vrij verkeer van informatie binnen het politieapparaat.<sup>39</sup> De gegevens zijn daarbij zonder nadere voorwaarden bruikbaar in het kader van de vervulling van de politietaak<sup>40</sup>, waarbij voor de houder van een politieregister over het algemeen een verplichting tot verstrekken bestaat.<sup>41</sup> Omdat de gegevens in het register-MOT betrekking hebben op onverdachte personen, dienen de gegevens in dit register afgescheiden te zijn van de overige politieregisters.<sup>42</sup> Het register-MOT wordt niet rechtstreeks ten behoeve van de politietaak bijgehouden.<sup>43</sup> De verplichte verstrekking, ofwel de zogenaamde 'free flow' van gegevens, betreft in beginsel slechts de verstrekking binnen het politieveld. Aangezien een verstrekking aan het Meldpunt kan worden beschouwd als een verstrekking aan een derde geldt daarvoor een regime dat inhoudt, dat slechts kan worden verstrekt aan bij de wet of AMvB aangewezen personen en instanties voor daarbij aangegeven doeleinden.<sup>44</sup> De mogelijkheden om die externe gegevens te verwerken kunnen onder meer worden beperkt door het doelbindingsbeginsel, het noodzakelijkheidsbeginsel en de aard van een ongericht dataminingonderzoek. Hierna wordt nader ingegaan op deze en andere factoren die een rol spelen bij een verwerking van gegevens in de gewone politieregisters.

38. *Jaarverslag* 2001, p. 9.

39. *Kamerstukken II*, 1996/97, 25 398, nr. 3, p. 4.

40. *Kamerstukken II*, 1995/96, 24 072, nrs. 10-11, p. 283.

41. *Kamerstukken II*, 1995/96, 24 072, nr. 14, p. 376. Van deze verplichting zijn onder omstandigheden uitgezonderd de registers zware criminaliteit, de tijdelijke registers, de voorlopige registers en de registers aangelegd ten behoeve van de hulpverlenende taak van de politie. Voor de registers die bij de politie worden gehouden, maar die niet zijn terug te voeren op de politietaak ex art. 2 Politiewet 1993 geldt het regime van de Wbp. Dit betekent bij bevraging voor de houder van het register dat hij een afweging van belangen moet maken.

42. *Kamerstukken II*, 1997/98, 25 880, nrs. 1-2, p. 84.

43. *Kamerstukken II*, 1996/97, 25 398, nr. 3, p. 2.

44. *Kamerstukken II*, 1996/97, 25 398, nr. 3, p. 4. Zie ook art. 18 lid 3 WPoLr.

### 8.2.3.1 De doelbinding

Noch de WPolr noch het BPolr stellen het doelbindingsbeginsel als algemene voorwaarde voor verstrekking uit een gewoon politieregister. Alleen het hulpverleningsregister en het register-MOT vormen daarop een uitzondering.<sup>45</sup> Toch dient met het oog op de Wbp ook bij een verstrekking van gegevens uit het register-MOT rekening te worden gehouden met de doelbinding. Een verstrekking van gegevens aan een register-MOT resulteert in een registratie van die gegevens in dat register. Op grond van art. 4 WPolr is een zodanige registratie (en daarmee ook de verstrekking) slechts mogelijk indien dat noodzakelijk is voor het doel van het register-MOT. Het is de vraag of het gebruik van gegevens uit de gewone politieregisters als zodanig kan worden aangemerkt. Het register-MOT heeft een zeer specifiek doel<sup>46</sup>, hetgeen betekent dat de verstrekte gegevens door het Meldpunt vaak voor een ander doel worden gebruikt dan waarvoor zij zijn verkregen. Wanneer het doel van een gewoon politieregister en dat van het register-MOT te veel afwijken is het zeer de vraag, of het gebruik van de gegevens een toegevoegde waarde (noodzaak) vertegenwoordigt. Indien die noodzaak niet onomstotelijk blijkt, kan zelfs een beperkt gebruik van de gewone politieregisters (bijvoorbeeld door middel van een verwijsindex) ongewenst zijn. Van strijdigheid met het doelbindingsbeginsel kan onder meer sprake zijn wanneer de gegevens die men wil gebruiken ten behoeve van het register-MOT zijn vergaard in het kader van een andere politietaak of wanneer het gegevens betreft uit politieregisters die niet zijn aangelegd in het kader van de politietaak zoals omschreven in art. 2 Politiewet 1993.

### 8.2.3.2 De aard van de politietaak

Bepaalde politieregisters zijn niet aangelegd ten behoeve van de politietaak zoals omschreven in art. 2 Politiewet 1993. Met betrekking tot de gegevens in deze politieregisters is geen sprake van een 'free flow' van informatie binnen het politieapparaat. Op grond van het hierboven behandelde doelbindingsbeginsel is het gebruik van deze politieregisters in beginsel uitgesloten.

### De handhaving van de openbare orde

Gegevens in een register 'openbare-ordehandhaving' (OOH-register) kunnen onder omstandigheden worden verstrekt ten behoeve van een ongericht dataminingonderzoek dat betrekking heeft op (andere) gewone politieregisters. Een wettelijke basis is niet per definitie vereist<sup>47</sup>, aangezien het in beginsel oppervlakkige informatie betreft waarmee

---

45. Art. 12 BPolr.

46. *Kamerstukken I*, 2001 /02, 28 018, nr. 116*b*, p. 1 en art. 3 sub *a* Wet MOT: het Meldpunt heeft tot taak: het verzamelen, registreren, bewerken en analyseren van de gegevens die het verkrijgt, teneinde te bezien of deze gegevens van belang kunnen zijn voor de voorkoming en opsporing van misdrijven.

47. *Kamerstukken II*, 1999 /00, 25 232, nr. 18, p. 6.

geen volledig beeld wordt verkregen van bepaalde aspecten van iemands leven. Ook de wijze waarop de gegevens in een OOH-register worden vergaard past binnen de ongerichte dataminingsvariant. Daarom lijkt het gebruik van deze gegevens in het kader van een ongericht dataminingonderzoek met betrekking tot het register-MOT niet uitgesloten. Op grond van het doelbindingsbeginsel zal dan echter wel een aantoonbare noodzaak aanwezig moeten zijn voor het gebruik van de gegevens in het kader van het onderhavige ongerichte dataminingonderzoek. Het is de vraag of deze gegevens een noodzakelijke bijdrage kunnen leveren aan de informatiepositie van het Meldpunt.

### **De hulpverleningstaak**

Het is uitgesloten dat ten behoeve van het onderhavige dataminingonderzoek gebruik kan worden gemaakt van politieregisters die zijn aangelegd ten behoeve van de hulpverleningstaak. Uit deze registers wordt slechts verstrekt overeenkomstig het doel waarvoor zij zijn aangelegd.<sup>48</sup> Hoewel een verstrekking volgens het BPolr wel mogelijk is indien de geregistreeerde daarmee uitdrukkelijk heeft ingestemd, lijkt ook dit geen mogelijkheid te bieden voor een verwerking van gegevens uit een hulpverleningsregister. Het passieve, ongerichte karakter van het dataminingonderzoek zal het verkrijgen van de bedoelde, uitdrukkelijke instemming in de weg staan. Bovendien ziet deze instemming vooral op individuele gevallen en niet op bulkverstrekkingen in het kader van een koppeling ten behoeve van een ongericht dataminingonderzoek.

#### *8.2.3.3 Koppeling*

Bij een verwerking van gegevens uit een ander gewoon politieregister is hier sprake van koppeling. Deze dient noodzakelijk te zijn voor een goede uitvoering van de politietaak voor zover het de strafrechtelijke handhaving van de rechtsorde betreft. Dit beperkt de mogelijkheid om gebruik te maken van registers die niet in het kader van deze politietaak zijn aangelegd en worden bijgehouden. Omdat bij de koppeling twee politieregisters zijn betrokken, dient zowel het reglement van het register-MOT als het reglement van het register waarmee wordt gekoppeld in die mogelijkheid te voorzien.

### **Privacyreglement MOT**

Het reglement van het register-MOT voorziet in een koppeling met een ander politieregister wanneer dit noodzakelijk is voor het doel van het register-MOT.<sup>49</sup> Met betrekking tot een aantal registers, waaronder het register zware criminaliteit en het voorlopige politieregister, wordt de mogelijkheid van koppeling daarmee expliciet genoemd. Van die koppelingen behoeft op grond van art. 13 lid 4 van het reglement geen proces-verbaal te worden opgemaakt. Deze verplichting bestaat wel wanneer het register MOT wordt

---

48. Art. 12 lid 1a BPolr.

49. Art. 13 lid 1 onder a en lid 2 Privacyreglement MOT.

gekoppeld met andere politieregisters of persoonsregistraties als bedoeld in art. 17 aanhef en onder *a* Wpr. Ook dient het CBP van die gevallen in kennis te worden gesteld.

#### *8.2.3.4 De aard van ongericht dataminingonderzoek*

Waar het gaat om een ongericht dataminingonderzoek dient terughoudend te worden omgegaan met het gebruik van externe gegevens. Het gebruik van externe gegevens dient noodzakelijk dient te zijn voor het doel van het register-MOT.<sup>50</sup> Bij geautomatiseerde bevragingen<sup>51</sup> kan hiermee rekening worden gehouden door informatie in verwijnsindexen tot een minimum te beperken. Met het oog op het doel van het register-MOT en de manier waarop gegevens in het kader van daarvan worden verwerkt, bestaat in beginsel geen noodzaak voor een volledige koppeling met andere gewone politieregisters. Een eenvoudige en passieve vergelijking met een namenindex (verwijsindex) volstaat in beginsel om vast te stellen of sprake is van een match. Er wordt niet actief en gericht gezocht in andere politieregisters, maar slechts gekoppeld met een uittreksel van de gegevens die men daaruit nodig heeft. Hierbij wordt geen overbodige informatie verstrekt, waardoor inbreuken op de persoonlijke levenssfeer beperkt blijven.

Op grond van art. 13a lid 4 WPolr kan een verstrekking uit een register zware criminaliteit aan het Meldpunt niet worden geweigerd, noch aan beperkende voorwaarden gebonden, in het geval het gaat om gegevens die noodzakelijk zijn om te kunnen vaststellen of een persoon geregistreerd staat in het register zware criminaliteit.<sup>52</sup> Het feit dat alleen ten aanzien van deze identificerende gegevens een daadwerkelijke verplichting tot verstrekken bestaat, lijkt bovenstaand standpunt aangaande een verstrekking te bevestigen. Ook met het oog op de verwerking van gegevens door het Meldpunt lijkt een minimale verstrekking niet bezwaarlijk. Hierbij gaat het immers om een dagelijkse vergelijking tussen de subjecten die zijn betrokken bij de ongebruikelijke transacties en de subjectenindex (CIESI) van de Criminele Inlichtingen Dienst (CIE) en die van het MRO. Blijkt een betrokkene als subject voor te komen in de CIESI/MRO dan is de transactie automatisch verdacht (in dat geval spreekt men van een 'hit'). Het rechtmatig gebruik van verwijnsindexen zal afhangen van de vraag, of het Meldpunt kan beschikken over de gegevens in de politieregisters waaruit de verwijnsindexen worden samengesteld. In de volgende sectie wordt hierop nader ingegaan.

#### *8.2.3.5 Het gebruik van de MRO-verwijsindex*

Het Meldpunt vergelijkt het register-MOT onder meer met de Verwijzingsindex Recherche Onderzoeken & Subjecten (VROS). Hierin staan personen die zich schuldig

---

50. Uit de art. 4 lid 2 en 6 lid 1 WPolr kan worden afgeleid dat de verwerking van externe gegevens noodzakelijk dient te zijn voor het doel van het register-MOT.

51. *Kamerstukken II*, 1997/98, 25 398, nr. 6, p. 7-8.

52. Zie ook commissie Van Traa, sectie 8.4 Verstrekking; 8.4.1 Juridische grondslag.

(gaan) maken aan rechtsorde schokkende misdrijven (CIE-subjecten) en personen die voorwerp zijn van opsporingsonderzoek bij rechteerteams van politie en bijzondere opsporingsdiensten (MRO-subjecten). Het betreft politieregisters omtrent natuurlijke personen en rechtspersonen die voor opsporingsdiensten relevant zijn.<sup>53</sup> Het register-MOT leent zich bij uitstek voor vergelijkingen met verwijzindexen. Daarmee kan een eventuele match relatief snel kan worden gevonden. In het vorige hoofdstuk<sup>54</sup> kwam het gebruik van verwijzindexen reeds aan bod. In deze sectie wordt ingegaan op de vergelijking die het Meldpunt maakt met het Bestand Meldingen Districtelijke Recherche-Onderzoeken (MRO-bestand), een gewoon politieregister en een verwijzindex. De MRO-bestanden vormen een overzicht van de door de politie uitgevoerde onderzoeken en hebben als doel, de onderzoeken tussen de verschillende korpsen te coördineren zodat een landelijk overzicht ontstaat van alle rechercheonderzoeken zoals bedoeld in de art. 126gg en 132a Sv. Dit betekent dat de gegevens uit de MRO-bestanden van alle korpsen via geautomatiseerde weg met elkaar worden vergeleken. Zo wordt duidelijk wanneer eenzelfde persoon bij meerdere korpsen voorwerp van onderzoek is of dat een voertuig in een rechercheonderzoek van een bepaald korps tevens voorkomt in een onderzoek van een ander korps. Met het bestand wordt de informatievoorziening in het kader van de uitvoering van art. 2 Politiewet 1993 binnen het korps mogelijk gemaakt voor zover het betreft:

- het verkrijgen van inzicht in een rechercheonderzoek dat in behandeling is bij een dienstonderdeel van het korps met betrekking tot de verdachten die betrokken zijn bij een rechercheonderzoek als bedoeld in de art. 126gg en 132a Sv; teneinde verbanden te onderkennen met andere rechercheonderzoeken binnen het korps;
- de inzet van opsporingsmiddelen voor de onder 1. genoemde rechercheonderzoeken binnen het korps;
- het verstrekken van daarvoor in aanmerking komende gegevens voor de VROS<sup>55</sup>.

Op een formulier-MRO moeten – behalve CIE-subjecten – ook andere onderzoeksgegevens worden ingevuld, zoals objecten, contactpersoon en de start- en de te verwachten einddatum van het onderzoek. In een MRO-bestand worden alle onderzoeken geregistreerd die langer dan een week duren en die gericht zijn op misdrijven waarvoor voorlopige hechtenis is toegelaten.<sup>56</sup> Op grond van art. 5 Privacyreglement Meldingen Districtelijke Rechercheonderzoeken kunnen in een MRO-bestand gegevens worden

53. *Jaarverslag* 2003, p. 27.

54. Sectie 7.3.3.4 onder het kopje *Doelbinding*.

55. Art. 2 Privacyreglement Meldingen Districtelijke Recherche-Onderzoeken (MRO).

56. *Kamerstukken II*, 1998/99, 26 269, nrs. 4-5, p. 124. (Commissie-Kalsbeek).

opgenomen omtrent verdachten, slachtoffers van een delict en opsporingsambtenaren. Daarbij kan het gaan om de volgende soorten van gegevens<sup>57</sup>:

- volledige personalia;
- adresgegevens en postcode;
- geboortegegevens;
- telecommunicatiegegevens;
- gebruikte vervoermiddelen;
- datum, tijdstip, plaats, aard en andere op het misdrijf betrekking hebbende gegevens;
- relaties voor zover deze zijn opgenomen in het register zware criminaliteit;
- het soort opsporingsonderzoek en een beschrijving van de soort actie;
- een weergave van de ingezette c.q. in te zetten opsporingsmiddelen.

In hoofdstuk zeven bleek het gebruik van verwijsindexen niet zonder meer mogelijk. In het hierna volgende wordt kort ingegaan op de vergelijking van dergelijke registers met een register-MOT (in het kader van een koppeling).

#### **MRO-bestand en tijdelijke politieregisters**

Een MRO-bestand bevat als verwijsindex gegevens (die verwijzen naar gegevens) uit andere politieregisters. Op gegevens in een verwijsindex die afkomstig zijn uit andere gewone politieregisters is hetzelfde verstrekkingenregime van toepassing als op het MRO-bestand en het register-MOT. Bij de registratie in een MRO-bestand van gegevens die afkomstig zijn uit (of betrekking hebben op) een bijzonder politieregister is dat niet het geval. De bijzondere registers kenmerken zich door een beperkt verstrekkingenregime, dat afwijkt van het open verstrekkingenregime dat van toepassing is op een MRO-bestand en het register-MOT. Dit afwijkende verstrekkingenregime kan een obstakel vormen voor een verstrekking van gegevens uit een bijzonder politieregister aan een MRO-bestand, hetgeen weer gevolgen kan hebben voor een verstrekking uit een MRO-bestand aan het register-MOT. Een registratie (en verwerking<sup>58</sup>) van persoonsgegevens in politieregisters is met het oog op de persoonlijke levenssfeer slechts toegestaan voor bepaalde doeleinden en onder bepaalde voorwaarden. Het verstrekkingenregime waarborgt dat dit in de praktijk ook gebeurt.

Een MRO-bestand is vooral bedoeld om een overzicht te geven van rechercheonderzoeken als bedoeld in de art. 126<sup>gg</sup> en 132<sup>a</sup> Sv. Voor dergelijk onderzoek kan gebruik worden gemaakt van een tijdelijk politieregister. Dit bijzondere politieregister heeft een

---

57. Art. 6 lid 1 en 2 Privacyreglement MRO. Het soort gegevens dat mag worden opgeslagen over opsporingsambtenaren is beperkt.

58. In beginsel voorziet het huidige verstrekkingenregime van de WPolr niet in elke verwerking zoals bedoeld in de Wbp.

beperkt verstrekkingenregime. Bij de vergelijking die plaatsvindt maakt het Meldpunt gebruik van een aangeleverde namenindex, waarbij geen onderscheid wordt gemaakt naar de afkomst van de gegevens in het MRO-bestand.<sup>59</sup> Het is echter de vraag of de gegevens in het MRO-bestand, voor zover die afkomstig zijn uit een tijdelijk politieregister, wel verder verwerkt mogen worden. Wanneer gegevens uit een tijdelijk politieregister worden verstrekt aan en vastgelegd in een MRO-bestand of het register-MOT leidt dat tot een dubbele registratie van deze gegevens binnen het politieveld. Het verschil tussen een verwijzing en een dubbele registratie van gegevens is afhankelijk van de vraag, welke gegevens worden vastgelegd in een verwijsindex. Wanneer wordt gewerkt met geanonimiseerde gegevens, zoals nummers die naar bepaalde gegevens verwijzen, zal noch sprake zijn van een dubbele registratie, noch van een ontoelaatbare inbreuk op de persoonlijke levenssfeer. Bij een gedeeltelijke of volledige overname echter is daarvan wel sprake. Met het oog op in sectie 8.2.3.5 genoemde aard van de gegevens die in een MRO-bestand kunnen worden vastgelegd gaat het daarbij in beginsel steeds om persoonsgegevens. Wanneer die betrekking hebben op gegevens uit een ander register kan van een dubbele registratie worden gesproken.

Een dubbele registratie van gegevens is, wanneer de gegevens rechtmatig binnen het politieapparaat aanwezig zijn, in beginsel rechtmatig. Dit kan anders zijn wanneer op de gegevens een beperkt verstrekkingenregime van toepassing is. Het belang van de waarborging van het afwijkende verstrekkingenregime kan een dubbele registratie in de weg staan. Het verstrekkingenregime van een tijdelijk politieregister pleegt te voorzien in de bescherming van de persoonlijke levenssfeer van de in dat register geregistreerde personen.<sup>60</sup> Wanneer gegevens uit een tijdelijk politieregister in een MRO-bestand worden vastgelegd, is die bescherming niet langer gewaarborgd. In dat geval wordt het systeem van de sociale compartimentering doorkruist voor zover het de interne opsplitsing van het WPoI-compartiment betreft.<sup>61</sup> Dit betekent in beginsel dat ook de koppeling van een MRO-bestand met het register-MOT onrechtmatig is voor zover daarbij gegevens uit een tijdelijk politieregister worden verwerkt.<sup>62</sup> Daarvan zal in ieder geval sprake zijn wanneer ook een rechtstreekse koppeling van een tijdelijk politieregister met een register-MOT niet mogelijk is. Met een koppeling van het register-MOT en het MRO-bestand wordt immers het verstrekkingenregime van het tijdelijke politieregister omzeild. Of een koppeling van een MRO-bestand (voor zover het gegevens betreft die afkomstig zijn uit een tijdelijk politieregister) met het register-MOT (C) rechtmatig is, hangt af van de vraag of de volgende koppelingen mogelijk zijn:

---

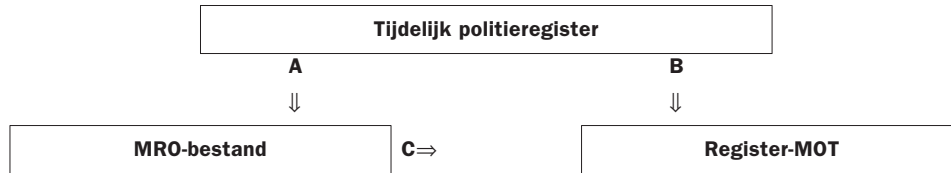
59. Het Meldpunt is hiertoe ook niet in staat op dit moment.

60. *Kamerstukken II*, 1996/197, 25 398, nr. 3, p. 4.

61. Van Ruth & Schreuders 2000.

62. De gegevens uit het tijdelijke politieregister zijn dan onrechtmatig verkregen hetgeen in strijd is met art. 4 lid 2 WPoI.

- a. de koppeling van een tijdelijk politieregister met een MRO-bestand (A);  
 b. de koppeling van een tijdelijk politieregister met het register-MOT (B).



### Koppeling van tijdelijk politieregister met MRO-bestand

De verwerking van gegevens in een tijdelijk politieregister wordt in sterke mate beperkt door het verstrekkingenregime van dat register.

*Doelbinding* – Op grond van art. 13 lid 2 WPolr is een verstrekking uit een tijdelijk register in beginsel slechts mogelijk voor het specifieke doel waarvoor dat register is aangelegd, bijvoorbeeld verrijking van de al in het register opgeslagen gegevens via misdaadanalyse.<sup>63</sup> Bij misdaadanalyse gaat het om het opsporen en inzichtelijk maken van verbanden tussen criminaliteitsgegevens onderling en andere mogelijk relevante gegevens met het oog op de praktijk van politie en justitie. Omdat de klassieke misdaadanalyse niet in de wet is geregeld, dient het te gaan om een niet-ingrijpend middel. Een verstrekking buiten het doel van het tijdelijke politieregister om is slechts mogelijk in een beperkt aantal, limitatief in de wet opgesomde, gevallen.<sup>64</sup> Algemeen geldt dat de verstrekking uit een tijdelijk register ten behoeve van de opsporing van andere misdrijven dan die waarvoor het register zware criminaliteit kan worden aangelegd, onwenselijk is.<sup>65</sup>

Een verstrekking aan een MRO-bestand is alleen mogelijk voor het doel waarvoor het tijdelijke politieregister is aangelegd. In beginsel zal een tijdelijk politieregister een ander doel hebben dan een MRO-bestand. Men kan zich op het standpunt stellen, dat een verstrekking aan een MRO-bestand plaatsvindt in het kader van een verrijking van het tijdelijke politieregister. Een verstrekking aan een MRO-bestand kan (indirect) leiden tot een verrijking van het tijdelijke politieregister, bijvoorbeeld doordat een verstrekking aan een MRO-bestand laat zien dat sprake is van een elders lopend onderzoek naar een persoon die ook geregistreerd staat in het tijdelijke politieregister. De vraag blijft of een zodanige verstrekking niet leidt tot een ontoelaatbare inbreuk op de persoonlijke levenssfeer. Wanneer gegevens uit een bijzonder politieregister worden gebruikt in een misdaadanalyse mogen die gegevens niet operationeel worden ingezet in de zin, dat opsporingsbevoegdheden worden aangewend tot nadere informatie-inwinning of dat betrokkene in

63. *Kamerstukken II*, 1996/97, 25 398, nr. 3, p. 4.

64. *Kamerstukken II*, 1997/98, 25 398, nr. 6, p. 3.

65. *Kamerstukken I*, 1998/99, 25 398, nr. 63b, p. 3.

zijn contacten met de politie anders wordt bejegend. Wel wordt de mogelijkheid openge-  
laten om de gegevens te vergelijken met gegevens uit andere bijzondere politieregisters.  
Bij een verstrekking aan een MRO-bestand vindt echter een vergelijking plaats van gege-  
vens uit een bijzonder politieregister met een gewoon politieregister.<sup>66</sup> In dat geval lijkt  
een specifieke wettelijke grondslag vereist.

*Koppeling* – Een verstrekking van gegevens uit een tijdelijk politieregister aan een MRO-  
bestand zal plaatsvinden in het kader van een koppeling. Op grond van art. 4 lid 2 BPolr  
kan een tijdelijk politieregister slechts worden gekoppeld indien dat noodzakelijk is voor  
het doel van dat register. Wanneer het initiatief om te verstrekken uit een tijdelijk regis-  
ter uitgaat van het MRO-bestand is het de vraag, of in dat verband wel kan worden  
gesproken van een noodzakelijkheid. Een verstrekking lijkt slechts mogelijk wanneer een  
eventuele positieve bijdrage, voortkomende uit een verstrekking aan het MRO-bestand,  
als noodzakelijk voor het tijdelijke register wordt aangemerkt. Wanneer twee politieregis-  
ters worden gekoppeld dienen de reglementen van die registers op grond van art. 6 lid 2  
WPolr in de mogelijkheid daartoe te voorzien. Een tijdelijk politieregister is van deze  
verplichting uitgezonderd. Het reglement van het register-MOT voorziet in art. 13 lid 2  
in de mogelijkheid van een koppeling met een tijdelijk politieregister, aangezien het  
gebruik van (en daarmee in beginsel ook de koppeling met) externe gegevens cruciaal is  
voor het goed functioneren van dat register.

*Geen operationeel gebruik* – Uit een tijdelijk politieregister mogen geen gegevens worden  
verstrekkt voor operationeel gebruik.<sup>67</sup> Gegevens zijn geschikt voor operationeel gebruik  
door de politie, indien zij uit politieregisters verstrekt mogen worden anders dan alleen  
ter verrijking van de reeds daarin opgeslagen informatie. In beginsel zijn onder de WPolr  
alle gegevens in de gewone politieregisters bestemd voor operationeel gebruik. Aangezien  
een MRO-bestand een gewoon politieregister is, kan een verstrekking uit een tijdelijk  
politieregister aan een MRO-bestand worden aangemerkt als een verstrekking voor ope-  
rationeel gebruik. Dit is anders wanneer de gegevens uit het tijdelijke register ‘zelfstan-  
dig’ in aanmerking komen voor registratie in een register zware criminaliteit. Ook is  
geen sprake van een verstrekking voor operationeel gebruik wanneer het MRO-bestand  
als datawarehouse wordt aangemerkt en waarbij de gegevens enkel worden verwerkt voor  
het doel van dat bestand. Het resultaat van de verwerking kan door de beheerder van het  
MRO-bestand aan de belanghebbende partijen worden meegedeeld. Met deze werkwijze

66. *Kamerstukken II, 1996/197, 25 398, nr. 3, p. 19.*

67. *Kamerstukken II, 1997/198, 25 398, nr. 6, p. 24 en Kamerstukken II, 1996/197, 25 398, nr. 3, p. 3-4.* Wanneer de informatie ten minste voldoet aan het criterium voor de opslag in het register zware criminaliteit, kunnen de gegevens ook operati-  
oneel worden gebruikt.

wordt voorkomen dat informatie uit een tijdelijk politieregister, via het MRO-bestand, beschikbaar komt voor operationeel gebruik.

*Doorverstrekken* – Voor een voorlopig politieregister heeft de wetgever voorzien in een duidelijke wettelijke regeling met betrekking tot een doorverstreking. Om oneigenlijk gebruik van een voorlopig politieregister tegen te gaan<sup>68</sup> verbiedt de WPolr<sup>69</sup> dat gegevens die in het kader van een verrijking uit dat register worden verstrekt in enig ander register worden vastgelegd. Hieruit kan worden afgeleid dat een verstreking voor het doel van een voorlopig register enkel mogelijk is ter directe verrijking van dat voorlopige register. Een indirecte verrijking van het voorlopige register, waarbij de verstrekte gegevens elders worden vastgelegd en verwerkt, is niet mogelijk.

Terwijl de registratie en verstreking van gegevens in een tijdelijk politieregister uitvoerig is geregeld, is dat niet het geval voor de manier waarop de eenmaal uit een tijdelijk politieregister verstrekte gegevens verder mogen worden verwerkt. Voor het tijdelijke politieregister ontbreekt een regeling zoals die van het voorlopige politieregister. Wanneer gegevens eenmaal uit een tijdelijk politieregister zijn verstrekt, stelt art. 13 WPolr geen beperkingen aan de wijze waarop die gegevens vervolgens mogen worden verwerkt. In dit verband zij ook gewezen op art. 30 WPolr, dat het sluitstuk vormt van het gesloten verstrekingenregime van de WPolr. Op grond van dit artikel mag eenieder die krachtens de WPolr de beschikking heeft gekregen over persoonsgegevens deze alleen (verder) verstrekken indien een op de WPolr gebaseerd voorschrift mededeling toelaat, dan wel indien de uitvoering van de taak waarvoor de gegevens (eerder) zijn verstrekt dan wel ontvangen tot het ter kennis brengen daarvan noodzaakt. Schreuders<sup>70</sup> geeft aan dat het gebruik van art. 30 WPolr als (zelfstandige) grondslag voor het verstrekken van gegevens op gespannen voet staat met de bedoeling van die bepaling en de uitgangspunten en achtergronden van het gesloten verstrekingenregime van de WPolr. Bovendien is het bepaalde in art. 30 lid 1 WPolr bedoeld voor verstrekingen in bijzondere gevallen. Het kan dan ook geen basis vormen voor systematische informatie-uitwisseling en informatiestromen.

#### **Doorverstreking aan register-MOT**

Een verstreking van gegevens uit een tijdelijk register aan een MRO-bestand lijkt niet steeds mogelijk. Die beperking blijkt des te meer, wanneer die (uit een verstreking uit een tijdelijk register voortgekomen) gegevens in het MRO-bestand vervolgens middels een koppeling worden (door)verstrekt aan het register-MOT.

---

68. *Kamerstukken II*, 1997/98, 25 398, nr. 6, p. 23.

69. Art. 13b lid 3 WPolr.

70. Schreuders 1995.

*Doelbinding en register-MOT* – Een verstrekking van gegevens uit een tijdelijk register aan een MRO-bestand dient noodzakelijk te zijn voor het doel van het tijdelijke register. Daartoe dient een verstrekking aan een MRO-bestand plaats te vinden in het kader van een verrijking van het tijdelijke politieregister. Wanneer de, uit het tijdelijke politieregister afkomstige, gegevens in het MRO-bestand worden doorverstrekt aan het register-MOT kan moeilijk worden volgehouden, dat die verstrekking nog plaatsvindt voor het doel waarvoor de gegevens in eerste instantie aan het MRO-bestand zijn verstrekt. Aangezien voor het vinden van een mogelijke match van de gegevens uit het tijdelijke politieregister met gegevens in het MRO-bestand de noodzakelijkheid ontbreekt van een doorverstreking van gegevens uit het MRO-bestand aan het register-MOT kan worden gesteld, dat een dergelijke doorverstreking in strijd is met het beperkte verstrekkingenregime van het tijdelijke politieregister.

*Koppeling en register-MOT* – Terwijl een koppeling van een tijdelijk register met een MRO-bestand noodzakelijk kan zijn voor het doel van het betreffende tijdelijke politieregister, is dat anders wanneer het MRO-bestand vervolgens wordt gekoppeld met het register-MOT. Het verstrekkingenregime legitimeert een dergelijke doorverstreking niet. De doorverstreking van gegevens uit het MRO-bestand (die betrekking hebben op een tijdelijk politieregister) aan het register-MOT is niet noodzakelijk voor het tijdelijke register en dient enkel de belangen van het Meldpunt.

*Verbod operationeel gebruik en register-MOT* – Wanneer gegevens uit een MRO-bestand (met betrekking tot een tijdelijk politieregister) worden doorverstrekt aan het register-MOT kan worden gesteld dat de gegevens uit het tijdelijke politieregister daarmee operationeel worden gebruikt. De oorspronkelijke verstrekking van gegevens uit een tijdelijk politieregister aan een MRO-bestand heeft dan niet enkel meer plaatsgevonden ten behoeve van het MRO-bestand (en indirect ter verrijking van het tijdelijke politieregister). Omdat wordt verstrekt aan het MRO-bestand, dat vervolgens wordt geraadpleegd door het register-MOT, kan worden gesproken van een verstrekking voor operationeel gebruik. Bovendien ligt het initiatief tot de koppeling met het MRO-bestand in beginsel bij het Meldpunt.

*Doorverstreken* – Hoewel art. 13 WPoI geen rechtstreekse beperkingen stelt aan een eventuele doorverstreking, staat het verstrekkingenregime hieraan indirect wel in de weg. In dat geval wordt niet langer voldaan aan de doelbinding, het noodzakelijkheidsvereiste en het verbod om de gegevens in een tijdelijk register te verstrekken voor operationeel gebruik.

*Wettelijke regeling verstrekking register-MOT* – Ook de wijze waarop de verstrekking van gegevens uit een bijzonder politieregister ten behoeve van het register-MOT is geregeld

is van invloed op de legitimiteit van doorverstrekking van gegevens uit een tijdelijk register aan het register-MOT.

Het register zware criminaliteit en het voorlopige politieregister kennen een eigen regeling<sup>71</sup> voor het verstrekken van gegevens aan het register-MOT. Een verstrekking uit een register zware criminaliteit vindt in beginsel plaats voor het doel waarvoor het register is aangelegd, namelijk de bestrijding van de zware criminaliteit, waartoe ook het witwassen van geld kan worden gerekend. Hoewel het hier een bijzonder politieregister betreft, zijn de gegevens in het register bestemd voor operationeel gebruik. Voor een verstrekking uit een register zware criminaliteit aan het Meldpunt bepaalt art. 13a lid 4 WPolr dat deze niet mag worden geweigerd. Ook mogen geen beperkingen worden gesteld aan het verdere gebruik van de verstrekte gegevens. Wanneer het gaat om de gegevens bedoeld in art. 13a lid 1 onder *c* die betrekking hebben op onverdachte personen, is het verstrekkingenregime van het voorlopige politieregister van toepassing. Voor een verstrekking van deze gegevens uit een register zware criminaliteit is een wettelijke grondslag nodig. De gegevens worden in dat geval niet verstrekt voor het doel waarvoor ze zijn vastgelegd, maar de verstrekking berust op een afzonderlijke wettelijke grondslag, te weten art. 13b lid 2, tweede volzin WPolr.

Voor een verstrekking van gegevens uit een voorlopig politieregister aan het Meldpunt wordt in art. 13b lid 2 WPolr een afzonderlijke grondslag genoemd om te mogen verstrekken, waaruit kan worden geconcludeerd dat een verstrekking niet kan worden gerechtvaardigd door de eventuele indirecte verrijking van het voorlopige politieregister die het resultaat kan zijn van een verstrekking aan een register-MOT. Een voorlopig politieregister heeft niet direct tot doel om de zware criminaliteit te bestrijden, maar dient om vast te kunnen stellen of de gegevens in het voorlopige politieregister eventueel kunnen worden overgeheveld naar een register zware criminaliteit. Hoewel een verstrekking aan het register-MOT mogelijk een match kan opleveren op grond waarvan een zodanige overheveling kan plaatsvinden, is gekozen voor een aparte wettelijke verstrekkinggrond. Dit valt mogelijk te verklaren uit het feit dat in een voorlopig politieregister gegevens omtrent onverdachte personen kunnen worden vastgelegd.

Uit de wijze waarop de verstrekking van gegevens uit de bovenstaande bijzondere politieregisters aan het register-MOT is geregeld blijkt, dat de gegevens waarvoor een afzonderlijke wettelijke grondslag geldt betrekking hebben op onverdachte personen. Ook een tijdelijk politieregister biedt de mogelijkheid om gegevens te verwerken die betrekking hebben op onverdachte personen. Met het oog hierop kan worden gesteld dat een verstrekking van gegevens uit dit register aan het register-MOT (en in geval van doorverstrekking ook aan een MRO-bestand) onwenselijk is wanneer een wettelijke grondslag daarvoor ontbreekt. Dit lijkt te worden bevestigd door hetgeen in de kamer-

---

71. Art. 13a lid 4 en art. 13b lid 2 WPolr.

stukken wordt opgemerkt met betrekking tot het verstrekkingenregime van een voorlopig politieregister:

*'Anders dan bij het tijdelijk register worden bovendien gegevens verstrekt aan het Meldpunt Ongebruikelijke Transacties'.<sup>72</sup>*

Een verstrekking uit een voorlopig politieregister vindt niet plaats voor het doel, c.q. ter verrijking, van het voorlopige politieregister. Hieruit kan worden geconcludeerd dat een eventuele indirecte verrijking van een voorlopig politieregister die kan voortkomen uit een verstrekking aan het register-MOT niet kan worden aangemerkt als een verstrekking voor het doel van het voorlopige politieregister. In het geval van een verstrekking uit een register zware criminaliteit is dit wel mogelijk, omdat die gegevens zijn bestemd voor operationeel gebruik. Omdat een tijdelijk politieregister, evenals een voorlopig politieregister, een zeer beperkt verstrekkingenregime heeft, lijkt een verstrekking aan een MRO-bestand of een register-MOT voor het doel, c.q. de verrijking van het tijdelijke politieregister, niet mogelijk. Aangezien een tijdelijk politieregister geen uitzondering kent op het verstrekkingenregime die een verstrekking aan een MRO-bestand of het register-MOT mogelijk maakt, lijkt een verstrekking uitgesloten.

### Resumerend

Bij een koppeling van het register-MOT met een verwijsindex dient rekening te worden gehouden met de mogelijkheid dat daarbij gegevens worden verwerkt waarop een afwijkend verstrekkingenregime van toepassing is. Zo is het mogelijk dat in het kader van een koppeling van een MRO-bestand met het register-MOT gegevens worden verwerkt die afkomstig zijn uit een tijdelijk politieregister. Wanneer een rechtstreekse verstrekking van gegevens uit een tijdelijk politieregister aan een MRO-bestand of een register-MOT niet mogelijk is dient te worden voorkomen, dat dit alsnog gebeurt door de koppeling van een MRO-bestand met het register-MOT. Wanneer een registratie van gegevens uit een tijdelijk politieregister in een MRO-bestand ertoe leidt dat het verstrekkingenregime van een tijdelijk register, en daarmee de bescherming van de persoonlijke levenssfeer, niet voldoende is gewaarborgd, zal een verstrekking niet mogelijk zijn.

Teneinde de gegevens uit een tijdelijk politieregister beschikbaar te maken voor het Meldpunt kan worden overwogen, de status van een MRO-bestand te herzien. In navolging van het register-MOT zou een MRO-bestand kunnen worden gekwalificeerd als een gewoon politieregister met een beperkt verstrekkingenregime. Dit betekent dat de gegevens niet langer beschikbaar zijn voor operationeel gebruik. Met het oog op de toegevoegde waarde van verwijsindexen voor de opsporingstaak gaat de voorkeur uit naar een oplossing die niet alleen ziet op MRO-bestanden. Door een verwijsindex als bijzonder

---

72. *Kamerstukken II, 1996/97, 25 398, nr. 3, p. 19.*

politieregister te kwalificeren wordt het probleem van het afwijkende verstrekkingenregime voor alle verwijsindexen ondervangen. Om ten behoeve van het register-MOT gebruik te maken van gegevens uit een tijdelijk politieregister kan worden overwogen om, overeenkomstig de regeling voor het voorlopige politieregister, te voorzien in een aparte mogelijkheid daartoe.

#### *8.2.3.6 Weigering door de beheerder*

De beheerder van een gewoon politieregister heeft de mogelijkheid om (onder meer op grond van art. 11 BPolr) de vrije verstrekking van gegevens uit een gewoon politieregister te beperken. Vrije verstrekking binnen het politieapparaat is echter de regel.<sup>73</sup> De registerbeheerder beschikt slechts over beperkte mogelijkheden ter controle van de noodzakelijkheid van een verstrekking binnen het politieapparaat ten behoeve van een goede uitvoering van de politietaak.<sup>74</sup> Slechts in die gevallen waarin aangenomen kan worden dat de gevraagde gegevens in alle redelijkheid en billijkheid niet benodigd, noodzakelijk of onvermijdelijk zijn in verband met de uitoefening van de taak waarvoor deze zijn gevraagd, kan een verstrekking worden geweigerd. In alle andere gevallen wordt ervan uitgegaan dat een verzoek op de juiste gronden wordt gedaan, met inachtneming van het daaromtrent bepaalde in de WPolr en het BPolr. Bij een verstrekking aan het register-MOT is geen sprake van een verstrekking binnen het politieapparaat. Op grond van art. 14 lid 1a BPolr mogen uit een politieregister gegevens worden verstrekt aan het Meldpunt voor zover men deze behoeft voor een goede uitvoering van de taak en de desbetreffende beheerder schriftelijk autorisatie heeft verleend.

#### **Resumerend**

Het gebruik van gegevens uit andere gewone politieregisters dient in overeenstemming te zijn met het doel van die politieregisters. Met het oog op de Wbp is het onwenselijk dat gegevens in een gewoon politieregister voor een ander doel worden verwerkt dan waarvoor zij zijn vastgelegd. Een beheerder dient op grond van art. 14 lid 1 a BPolr schriftelijk toestemming te verlenen voor een verstrekking aan het Meldpunt. Hierbij zal tevens een afweging kunnen worden gemaakt of een verstrekking in overeenstemming is met het doelbindingsbeginsel. Bij een koppeling van het register-MOT met een ander gewoon politieregister dienen de reglementen van de betrokken registers in die mogelijkheid te voorzien. Het reglement van het register-MOT verbindt aan een koppeling de voorwaarde, dat die noodzakelijk dient te zijn voor het register-MOT. Op grond van de WPolr dient de koppeling ook noodzakelijk te zijn voor de politietaak voor zover het de strafrechtelijke handhaving van de rechtsorde betreft. Algemeen geldt dat terughoudendheid is geboden bij de verwerking van gegevens uit andere politieregisters. Het gericht

---

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

74. Schreuders 1995.

zoeken (op bijvoorbeeld een bepaalde naam) door het Meldpunt in de gewone politieregisters of een volledige koppeling met andere registers is onwenselijk. Om gebruik te maken van de gegevens in de gewone politieregisters gaat de voorkeur uit naar het gebruik van verwijssindexen. In de praktijk zal dit het Meldpunt voldoende informatie verschaffen om te bepalen of al dan niet sprake is van een match. Bij het gebruik van verwijssindexen dient duidelijk te zijn welke gegevens daarin zijn opgenomen en of het verstrekkingenregime, dat oorspronkelijk op die gegevens van toepassing is, een verwerking ten behoeve van het register-MOT niet in de weg staat.

#### *8.2.4 Het gebruik van gegevens uit een bijzonder politieregister*

Normaal gesproken mogen zachte gegevens niet in een gewoon politieregister worden vastgelegd. Hoewel het register-MOT een gewoon politieregister is, biedt het register op grond van art. 5a lid 1 onder *b* WPolr de mogelijkheid om er voor langere tijd zachte gegevens in vast te leggen. Met het oog daarop kent het register een beperkt verstrekkingenregime. Volgens de MvT<sup>75</sup> bij de bijzondere politieregisters is de registratie van zachte gegevens voor een ander doel dan de bestrijding van de zware criminaliteit alleen denkbaar in een tijdelijk of een voorlopig politieregister. In het geval van het register-MOT vindt de verwerking van zachte gegevens plaats ter bestrijding van de zware criminaliteit. Het bepaalde in art. 13d lid 3 WPolr staat een verwerking van zachte gegevens door het Meldpunt niet in de weg. Die verwerking vindt namelijk plaats op een moment waarop ten minste sprake dient te zijn van een redelijk vermoeden, maar waarbij nog geen actie kan worden genomen overeenkomstig par. 3a WPolr. Een registratie in het register-MOT is op grond van de Wet MOT al op een eerder tijdstip mogelijk. In hoofdstuk vijf bleek, dat bij het gebruik van gegevens met een verstrekkingenregime dat afwijkt van het verstrekkingenregime van het basisregister de behoefte kan ontstaan aan een afzonderlijke kwalificatie van het datawarehouse. Hoewel het register-MOT geen bijzonder politieregister is, kent het een beperkt verstrekkingenregime. Hierdoor is bij een koppeling met een bijzonder politieregister in beginsel geen sprake van onderling afwijkende verstrekkingenregimes. Bij een koppeling met externe gegevens waarop een beperkt verstrekkingenregime van toepassing is volstaat het register-MOT daarom in de regel als basisregister of datawarehouse. Het register-MOT en het bijbehorende reglement bieden voldoende waarborgen ter bescherming van de persoonlijke levenssfeer van de geregistreerden. Ten behoeve van een verstrekking uit de bijzondere politieregisters aan het register-MOT heeft de wetgever in een aantal aparte wettelijke bepalingen voorzien. In deze sectie wordt onderzocht of en in hoeverre het mogelijk is om in het kader van een ongericht dataminingonderzoek met betrekking tot het register-MOT gebruik te maken van de bijzondere politieregisters: het tijdelijke register, het voorlopige register en het register zware criminaliteit.

---

75. *Kamerstukken II, 1997/198, 25 398, nr. 6, p. 9.*

#### 8.2.4.1 *Het gebruik van een tijdelijk politieregister*

Doordat een tijdelijk politieregister kan worden aangelegd voor ‘de politietaak in een bepaald geval’ heeft het een toepassingsbereik dat zich uitstrekt over zowel een onderzoek naar een aantal fietsendiefstallen tot en met de bestrijding van de zware criminaliteit. Hoewel de onderhavige zaken qua inhoud en ernst zeer ver uiteen kunnen liggen, is op alle gegevens in een tijdelijk politieregister hetzelfde verstrekkingenregime van toepassing. Het gebruik van een tijdelijk politieregister is al gedeeltelijk behandeld in het kader van het MRO-bestand; voor het overige wordt verwezen naar het onderstaande.

#### **Doelbinding**

Op grond van art. 13 lid 2 WPolr is een verstrekking uit een tijdelijk register slechts mogelijk voor het doel waarvoor dat is aangelegd, dan wel ten behoeve van opname in een van de twee andere bijzondere politieregisters. Het register-MOT heeft een specifiek doel en een verstrekking aan dit register dient in beginsel alleen het Meldpunt. Hoewel bij een verstrekking van gegevens uit een tijdelijk politieregister aan het register-MOT zou kunnen worden volstaan met een antwoord op de vraag of een bepaald persoon al dan niet in het tijdelijke politieregister voorkomt, blijkt uit de kamerstukken<sup>76</sup> dat de mogelijkheid daartoe ontbreekt. Deze stringente regeling voorkomt, dat velen voor verschillende doeleinden in die registraties kunnen zien wie daarin is opgenomen. Daarnaast leidt een dergelijke verstrekking niet tot verkrijging van meer informatie over betrokkene (het doel van het register). Op grond van art. 4 lid 2 WPolr dient een registratie van (persoons)gegevens uit een tijdelijk politieregister in het register-MOT (in het kader van een ongericht dataminingonderzoek met betrekking tot laatstgenoemd register) noodzakelijk te zijn voor het doel van het register-MOT. De doelbinding staat een verstrekking aan het register-MOT in de weg. Aangezien ook de uitzonderingen van art. 13d lid 2 WPolr niet van toepassing zijn, lijkt het gebruik van (gegevens uit) een tijdelijk politieregister niet mogelijk.

#### **Koppeling**

Een koppeling met een tijdelijk politieregister dient op grond van art. 4 lid 2 BPolr noodzakelijk te zijn voor het doel waarvoor het tijdelijke register is aangelegd. Het ongerichte dataminingonderzoek, en daarmee de koppeling, vindt plaats ten behoeve van een verbetering van de informatiepositie van het register-MOT, welke niet direct noodzakelijk zal zijn voor (de informatiepositie van) het tijdelijke politieregister. Uit de formulering van art. 4 lid 2 BPolr kan worden opgemaakt dat het initiatief tot een verstrekking ligt bij de beheerder van het tijdelijke politieregister, hetgeen moeilijk te rijmen valt met het feit dat het initiatief voor het gebruik van gegevens uit een tijdelijk politieregister bij het ongerichte dataminingonderzoek bij het register-MOT ligt. Bij een koppeling van twee politieregisters dienen in beginsel de reglementen van beide betrokken politieregis-

---

76. *Kamerstukken II*, 1997/198, 25 398, nr. 6, p. 24.

ters in die mogelijkheid te voorzien. Nu een tijdelijk politieregister van deze verplichting is uitgezonderd behoeft enkel het reglement van het register-MOT te voorzien in de mogelijkheid tot koppeling.

#### **De aard van het ongerichte dataminingonderzoek**

Een verwerking van gegevens uit een bijzonder politieregister ten behoeve van een verbetering van de informatiepositie van het register-MOT impliceert een inbreuk op de persoonlijke levenssfeer. De mogelijkheid om zachte gegevens vast te leggen in het register-MOT berust dan ook op een wettelijke grondslag. Zowel de registratie van zachte gegevens als de verwerking daarvan zullen in een inbreuk op de privacy resulteren en kunnen daarom worden aangemerkt als een ingrijpend middel. Bij het ontbreken van een specifieke, wettelijke grondslag voor het gebruik van een dergelijk ingrijpend middel in het kader van een ongericht dataminingonderzoek, is sprake van een ontoelaatbare inbreuk op de persoonlijke levenssfeer. Hoewel de wetgever voor de andere twee bijzondere politieregisters in een wettelijke verstrekingsgrond heeft voorzien, is dat niet het geval voor het tijdelijke politieregister. Verstrekking uit een tijdelijk politieregister aan het register-MOT in het kader van een ongericht dataminingonderzoek heeft geen wettelijke grondslag en lijkt om die reden uitgesloten.

#### **Resumerend**

Het verstrekkingenregime van een tijdelijk politieregister staat een verstrekking van gegevens uit dit register aan het register-MOT in het kader van een ongericht dataminingonderzoek in beginsel in de weg.

##### *8.2.4.2 Het gebruik van een voorlopig politieregister*

Een voorlopig politieregister heeft, evenals een tijdelijk politieregister, een beperkt verstrekkingenregime. Voor een verstrekking van gegevens uit een voorlopig politieregister ten behoeve van het register-MOT is evenwel voorzien in een aparte wettelijke regeling.

#### **Doelbinding**

Uit een voorlopig politieregister kunnen op grond van art. 13*b* lid 2 WPolr voor identificatie benodigde gegevens worden verstrekt voor het doel waarvoor dat voorlopige register is aangelegd. Voorts wordt verstrekt ten behoeve van de opname in een ander bijzonder politieregister of ten behoeve van het Meldpunt. Uit het artikel wordt niet meteen duidelijk of de doelbinding van art. 13*b* lid 2 WPolr ook van toepassing is op de tweede volzin van lid 2, dat ziet op de verstrekking ten behoeve van een opname in een ander bijzonder politieregister of ten behoeve van het register-MOT. De parlementaire geschiedenis geeft aan dat de verstrekkingen in de tweede volzin van art. 13*b* lid 2 WPolr moeten worden uitgelegd overeenkomstig de bepalingen voor de tijdelijke registers.<sup>77</sup> Uit

---

77. *Kamerstukken II*, 1996/197, 25 398, nr. 3, p. 19.

de toelichting op art. 13 WPolr blijkt dat, behalve voor het doel van het tijdelijke register, ook gegevens worden verstrekt ter opname in het register zware criminaliteit, het voorlopige register of een ander tijdelijk register. Daarvoor is vereist dat de opname van de persoonsgegevens in overeenstemming is met het doel van die registers.<sup>78</sup> Voor een voorlopig politieregister betekent dit, dat een verstrekking op grond van art. 13b lid 2, tweede volzin, WPolr in overeenstemming dient te zijn met het doel van het register waaraan wordt verstrekt. Een verstrekking op grond van art. 13b lid 2 WPolr aan het register-MOT hoeft niet noodzakelijk te zijn voor het voorlopige politieregister, maar enkel in overeenstemming te zijn met het doel van het register-MOT. Met het oog op de wettelijk geregelde mogelijkheid tot verstrekking aan en registratie in het register-MOT lijkt aan deze voorwaarde te zijn voldaan. De registratie van (persoons)gegevens uit een voorlopig politieregister in het register-MOT dient op grond van art. 4 lid 2 WPolr noodzakelijk te zijn voor het doel van het laatstgenoemde register. De regeling van art. 13b lid 2 en 3 WPolr, die uitdrukkelijk de mogelijkheid van het vastleggen van gegevens uit een voorlopig politieregister vast te leggen in het register-MOT open laat, lijkt deze noodzaak te bevestigen. Het doelbindingsbeginsel lijkt een verstrekking uit een voorlopig politieregister aan het register-MOT niet in de weg te staan.

### **Koppeling**

Een verstrekking uit een voorlopig politieregister aan het register-MOT heeft tot doel het verkrijgen van aanvullende informatie omtrent een op voorhand onbepaalde groep van personen. Dit betekent onder meer dat de verstrekking die in het kader van een koppeling plaatsvindt noodzakelijk dient te zijn voor een goede uitvoering van de politietraak. Bovendien moeten de reglementen van beide betrokken registers voorzien in de mogelijkheid van een koppeling.

*Privacyreglement Meldpunt* – Het reglement van het register-MOT bepaalt in art. 13 lid 1 onder *b* van dat een koppeling mogelijk is met het grijze veldregister bij de CRI. Het, sterk verouderde, reglement doelt daarmee op de voorheen als ‘grijze veldregisters’ bekend staande voorlopige politieregisters. Het reglement voorziet daarmee expliciet in de mogelijkheid om die registers te koppelen.

*Modelreglement voorlopig politieregister* – Op grond van art. 14 van het modelreglement van een voorlopig politieregister<sup>79</sup> kan een koppeling plaatsvinden met een ander politieregister of een register als bedoeld in art. 17, aanhef en onder *a* Wpr voor zover deze noodzakelijk is voor het doel van het register, en het andere bijzondere politieregisters betreft. Een verstrekking uit een voorlopig politieregister aan het register-MOT is moge-

---

78. *Kamerstukken II*, 1996/197, 25 398, nr. 3, p. 15.

79. *Stcrt.* 12 oktober 2000, nr. 198, p. 17, 12.

lijk op grond van art. 13*b* lid 2 WPolr. In beginsel voldoet een dergelijke verstrekking niet aan de voorwaarde, dat de koppeling in het kader waarvan de verstrekking plaatsvindt noodzakelijk moet zijn voor het voorlopige politieregister. Een verstrekking op grond van art. 13*b* lid 2, tweede volzin WPolr heeft namelijk alleen noodzakelijk te zijn voor het doel van het register waaraan wordt verstrekt, in dit geval het register-MOT. Uit de toelichting op het modelreglement blijkt dat deze voorwaarde om te mogen koppelen samenhangt met het feit, dat koppeling juridisch gezien verstrekkingen met zich mee brengt. Een koppeling voor een ander doel zou dus in strijd zijn met het doelbindingsbeginsel. Bij het opstellen van het reglement lijkt men echter geen rekening te hebben gehouden met art. 13*b* lid 2 WPolr, waar de wetgever een uitzondering heeft gemaakt voor de verstrekking aan het register-MOT. Dit heeft vergaande gevolgen voor de mogelijkheid tot koppeling van een voorlopig politieregister met dat register. Aangezien het modelreglement van het voorlopige register een koppeling in de weg staat is deze, gezien het bepaalde in art. 6 lid 2 WPolr, uitgesloten.

#### **De aard van het ongerichte dataminingonderzoek**

Aangezien de verwerking van gegevens uit een voorlopig politieregister ten behoeve van een verbetering van de informatiepositie van het register-MOT berust op een wettelijke grondslag, zal die activiteit niet leiden tot een ontoelaatbare inbreuk op de persoonlijke levenssfeer. Desondanks dienen verstrekkingen uit een voorlopig politieregister zo beperkt mogelijk te geschieden. Het streven naar terughoudend gebruik van externe gegevens hangt nauw samen met de aard van een ongericht dataminingonderzoek. Een koppeling met een voorlopig register dient noodzakelijk zijn voor de uitvoering van de taak waarvoor het register-MOT is aangelegd, waarbij de wetgever aangeeft dat slechts die gegevens worden verstrekt die noodzakelijk zijn om te kunnen vaststellen of een persoon in dat voorlopige politieregister is opgenomen.<sup>80</sup> Een verstrekking dient het Meldpunt redelijkerwijs in staat te stellen, met de verkregen gegevens een match te vinden. De verstrekking van alleen een naam zal daarom in veel gevallen volstaan. De verstrekking van aanvullende gegevens is slechts toegestaan voor zover kan worden aangetoond, dat de beschikking daarover voor het Meldpunt noodzakelijk is.

#### **Resumerend**

Op grond van art. 13*b* lid 2, tweede volzin WPolr kunnen gegevens uit een voorlopig politieregister worden verstrekt aan het register-MOT. Daarbij dient het te gaan om een minimale verstrekking die noodzakelijk is voor een goede uitvoering van de taak van het Meldpunt. Het modelreglement van een voorlopig politieregister houdt echter geen rekening met deze uitzonderingsbepaling. Een verstrekking uit een voorlopig politieregister in het kader van een koppeling met het register-MOT is niet direct noodzakelijk

---

80. *Kamerstukken II, 1996/97, 25 398, nr. 3, p. 19.*

voor het eerstgenoemde register, maar wel een noodzakelijke voorwaarde om te mogen koppelen. Aangezien het modelreglement van het voorlopige register een koppeling in de weg staat is deze, gezien het bepaalde in art. 6 lid 2 WPolr, uitgesloten. Teneinde een dergelijke koppeling alsnog te legitimeren kan worden overwogen, de formulering van art. 14 van het modelreglement te herzien; daarmee zal tevens eventuele onduidelijkheid omtrent dit artikel worden weggenomen.

#### 8.2.4.3 *Het register zware criminaliteit*

Ten slotte is onderzocht of in het kader van een ongericht dataminingonderzoek met betrekking tot het register-MOT gebruik kan worden gemaakt van een register zware criminaliteit. Hierbij is wederom het onderscheid tussen de verschillende gegevens in een register zware criminaliteit van belang, met name waar het gaat om:

- 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 beramen of plegen van misdrijven als bedoeld onder *a*;
- c. personen die in een bepaalde relatie staan tot degenen, bedoeld onder *a* en *b*.

#### **Doelbinding**

Het verstrekkingenregime van een register zware criminaliteit stelt in beginsel geen specifieke eisen aan een verwerking van gegevens in een register zware criminaliteit behorende tot de categorieën *a* en *b* ten behoeve van het register-MOT. De gegevens zijn bedoeld voor operationeel gebruik en kunnen daarom worden verstrekt aan het Meldpunt. In sectie 7.3.4.3 onder het kopje *Doelbinding* is uiteengezet dat de criteria van duurzame opslag en operationeel gebruik onvoldoende recht doen aan de bescherming van de persoonlijke levenssfeer bij de vraag naar een verstrekking van gegevens uit een register zware criminaliteit. In dat licht is het wenselijk om een eventuele bepaalde verwerking van gegevens uit een register zware criminaliteit te toetsen aan het doelbindingsbeginsel, teneinde te bezien of die verwerking de inbreuk op de persoonlijke levenssfeer rechtvaardigt. Daarbij dient het doel van de verwerking gerelateerd te zijn aan het doel van een register zware criminaliteit. Ook is van belang op welke wijze die verwerking plaatsvindt. Deze dient overeen te stemmen met het verstrekkingenregime van een register zware criminaliteit.

Gewone politieregisters zijn geschikt voor operationeel gebruik en worden in beginsel aangelegd en bijgehouden voor andere doeleinden dan de bijzondere politieregisters. Een registratie van zachte (categorie *b* en *c*) gegevens uit een bijzonder politieregister in een gewoon politieregister is in beginsel ongewenst. Een verstrekking aan het register-MOT is vanwege het beperkte verstrekkingenregime van dat register echter minder bezwaarlijk dan aan één van de overige gewone politieregisters. Naast een waarborging van het verstrekkingenregime moet een verstrekking in overeenstemming zijn met het doel waar-

voor de gegevens in het register zware criminaliteit zijn verzameld. De wetgever geeft aan dat bij misdrijven die een ernstige inbreuk op de rechtsorde opleveren moet worden gedacht aan de handel in harddrugs, mensenhandel, witwassen of wapenhandel. Deze misdrijven schokken het rechtsgevoel ernstig door hun omvang en hun gevolgen voor de samenleving.<sup>81</sup> Nu het witwassen wordt aangemerkt als een misdrijf waarvoor een register zware criminaliteit kan worden aangelegd, zal een verstrekking aan het register-MOT overeenstemmen met het doel van een register zware criminaliteit.

*Artikel 13d lid 3 WPolr* – Op grond van art. 13d lid 3 WPolr is het vastleggen en gebruiken van persoonsgegevens voor de doeleinden van par. 3a WPolr slechts mogelijk overeenkomstig het bij of krachtens par. 3a WPolr bepaalde. Het doel van het register-MOT rechtvaardigt ook een registratie in een register zware criminaliteit. Met het oog op de formulering van art. 13d lid 3 WPolr lijkt dit te betekenen dat die gegevens niet in het register-MOT, maar in een register zware criminaliteit dienen te worden vastgelegd. Gegevens in het register-MOT kunnen immers worden aangemerkt als persoonsgegevens die worden vastgelegd voor een van de doeleinden als bedoeld in par. 3a WPolr. Toch staat het bepaalde in art. 13d lid 3 WPolr een verwerking in het kader van het register-MOT niet in de weg. Wanneer gegevens in het register-MOT worden vastgelegd is een registratie van die gegevens voor dat doel in een register zware criminaliteit nog niet mogelijk. De gegevens in het register-MOT hebben betrekking op onverdachte personen en art. 13a lid 1 WPolr biedt in beginsel geen ruimte voor registratie van die gegevens in een register zware criminaliteit.<sup>82</sup> Hoewel het doel verwijst naar een register zware criminaliteit, is een registratie voor dat doel enkel nog maar mogelijk in het register-MOT. Om verwarring op dit punt te voorkomen, kan worden overwogen om de art. 13d lid 3 WPolr anders te formuleren. In plaats van:

*‘Persoonsgegevens die worden vastgelegd voor de doeleinden, bedoeld in deze sectie, worden slechts vastgelegd en gebruikt overeenkomstig het bij of krachtens deze sectie bepaalde’*,

kan worden gekozen voor:

*‘Persoonsgegevens die kunnen worden vastgelegd voor de doeleinden, bedoeld in deze sectie, worden slechts vastgelegd en gebruikt overeenkomstig het bij of krachtens deze sectie bepaalde’*.

81. *Kamerstukken II*, 1996/197, 25 398, nr. 3, p. 6.

82. Tenzij in het geval van gegevens als bedoeld in art. 13a lid 1 onder c WPolr.

Met de invoeging van het woord ‘kunnen’ wordt aangegeven, dat de bescherming van art. 13*d* lid 3 WPolr slechts van toepassing is indien het gaat om gegevens die ook daadwerkelijk kunnen worden vastgelegd onder par. 3*a* WPolr.

*Artikel 4 lid 2 WPolr* – Een verstrekking van gegevens uit een register zware criminaliteit aan het register-MOT betekent in beginsel een registratie van die gegevens in het laatstgenoemde register. Uit art. 4 lid 2 WPolr kan worden opgemaakt, dat een verstrekking van (persoons)gegevens<sup>83</sup> noodzakelijk dient te zijn voor het doel van het register-MOT. Met het oog op art. 13*a* lid 4 en 13*b* lid 2 WPolr, waarmee uitdrukkelijk de mogelijkheid is gecreëerd om aan het register-MOT te verstrekken, kan worden geconcludeerd dat van die noodzaak sprake is.

*Doelbinding gegevens categorie c* – Op de gegevens in categorie *c* is op grond van art. 13*a* lid 2 WPolr het verstrekkingenregime van het voorlopige politieregister van toepassing, dat is neergelegd in art. 13*b* lid 2 WPolr. Op grond daarvan<sup>84</sup> dient de registratie van de verstrekte gegevens uit een voorlopig politieregister in overeenstemming te zijn met het doel van het register-MOT waaraan wordt verstrekt.<sup>85</sup> Met het oog op de wettelijke regeling tot verstrekking in art. 13*b* lid 2 WPolr zal hiervan in beginsel sprake zijn. Op grond van art. 13*b* lid 2, eerste volzin WPolr is het toegestaan dat de gegevens worden vastgelegd in het register-MOT. In de situatie waarbij dit resulteert in een structurele opslag van gegevens die betrekking hebben op onverdachte personen in het register-MOT, is voorzien met art. 5*a* lid 1 sub *b* WPolr.

### Koppeling

Een koppeling dient noodzakelijk te zijn voor een goede uitvoering van de politietaak betreffende de strafrechtelijke handhaving van de rechtsorde. Uit de omstandigheid dat de art. 13*a* lid 4 en 13*b* lid 2 WPolr uitdrukkelijk de mogelijkheid bieden tot verstrekking uit een register zware criminaliteit aan het register-MOT, kan worden afgeleid dat een dergelijke noodzaak aanwezig is. Voorts dienen de reglementen van de betrokken politieregisters te voorzien in de mogelijkheid van een koppeling.<sup>86</sup> Het reglement van het register-MOT bepaalt in art. 13 lid 1 onder *a* dat kan worden gekoppeld met het CID-register bij de CRI, oftewel het register zware criminaliteit. Het is de vraag of dit andersom ook het geval is voor het modelreglement van een register zware criminaliteit.

---

83. Ongeacht de categorie.

84. Zie sectie 8.2.4.2 onder het kopje *Doelbinding*.

85. *Kamerstukken II*, 1996/197, 25 398, nr. 3, p. 15.

86. Art. 6 lid 2 WPolr.

*Modelreglement register zware criminaliteit* – In art. 17 lid 1 sub *a* van het modelreglement<sup>87</sup> wordt bepaald, dat een koppeling alleen mogelijk is voorzover noodzakelijk ter voorkoming en opsporing van misdrijven die een ernstige inbreuk op de rechtsorde opleveren. Daartoe kan worden gekoppeld met andere registers zware criminaliteit, voorlopige politieregisters, dan wel gegevensverzamelingen waarvan de doelstelling nauw bij die van het register zware criminaliteit aansluit. Het modelreglement van een register zware criminaliteit stelt indirect het doelbindingsbeginsel als voorwaarde voor een verstreking dan wel een koppeling. Omdat het register-MOT qua doelstelling nauw aansluit bij een register zware criminaliteit (zoals bedoeld in art. 17 lid 1 sub *a* modelreglement) voorziet het modelreglement van een register zware criminaliteit in de mogelijkheid tot koppeling met het register-MOT.

Wanneer niet aan de voorwaarde van art. 17 lid 1 sub *a* wordt voldaan, kan voor een koppeling met andere gegevensverzamelingen<sup>88</sup> een beroep worden gedaan op art. 17 lid 1 sub *b*. Volgens de toelichting bij het modelreglement zware criminaliteit ziet deze bepaling op gevallen, waarin niet op voorhand kan worden aangegeven met welke registers de koppeling zal plaatsvinden. Deze mogelijkheid tot koppeling is gebaseerd op de regeling van art. 6 lid 4 WPolr. Daar wordt bepaald dat de MvJ in bepaalde gevallen, in afwijking van het bepaalde in art. 6 lid 2 en 3 WPolr, toestemming kan geven tot een koppeling indien dat noodzakelijk is voor de opsporing van een misdrijf waardoor de rechtsorde ernstig geschokt is. Een koppeling op grond van art. 17, en daarmee een verstreking in het kader van die koppeling, vindt in beginsel slechts plaats ten behoeve van misdrijven waarvoor een register zware criminaliteit kan worden aangelegd.

#### **Aard ongericht dataminingonderzoek**

Aangezien de WPolr voorziet in een wettelijke grondslag voor een verstreking ten behoeve van de werkzaamheden van het Meldpunt, zal een verwerking van gegevens in dat kader uit een register zware criminaliteit in beginsel niet leiden tot een ontoelaatbare inbreuk op de persoonlijke levenssfeer. Die wettelijke grondslag wordt gevonden in de Wet MOT en, meer specifiek, in de wetgeving inzake de politieregisters. Van een doorkruising van het verstrekkingenregime van een register zware criminaliteit bij het verrichten van het ongerichte dataminingonderzoek blijkt geen sprake te zijn.

Met het oog op de ongerichte aard van het dataminingonderzoek en de bescherming van de persoonlijke levenssfeer dient bij een verstreking aan het Meldpunt terughoudendheid te worden betracht. Er dienen niet meer gegevens te worden verstrekt dan noodzakelijk is voor de uitvoering van de taak waarvoor een register-MOT is aangelegd. Evenals

87. *Stert.* 12 oktober 2000, nr. 198, p. 17.

88. Op grond van art. 17 lid 2 van het modelreglement dient van een dergelijke koppeling melding te worden gedaan aan het CBP.

bij een verstrekking van gegevens uit een voorlopig politieregister aan een register-MOT kan als uitgangspunt worden genomen, dat het Meldpunt met de verkregen gegevens redelijkerwijs in staat dient te zijn een eventuele match te kunnen vinden. In het verlengde daarvan bepaalt art. 13a lid 4 WPolr, dat een verstrekking uit een register zware criminaliteit ten behoeve van het register-MOT slechts verplicht is voor zover het gaat om gegevens die noodzakelijk zijn om vast te kunnen stellen of een persoon in een register zware criminaliteit staat geregistreerd. Daartoe kan een verwijsindex met namen volstaan. Gezien de algemene zorgplicht die de beheerder van een register zware criminaliteit heeft dient hij op grond van art. 13a lid 3 WPolr in beginsel ieder verzoek om een verstrekking van aanvullende gegevens te weigeren. Voor een goede uitvoering van de politietaak blijft de noodzaak aanwezig, dat een inbreuk op de persoonlijke levenssfeer tot een minimum beperkt blijft. Het proportionaliteitsbeginsel vindt aansluiting op een beperkte invulling van de koppeling.

#### **Weigering door de beheerder**

Hoewel een beheerder van een register zware criminaliteit op grond van art. 13a lid 3 WPolr een verstrekking kan weigeren of beperkende voorwaarden kan stellen aan het verdere gebruik van de gegevens, verklaart lid 4 deze mogelijkheid niet van toepassing wanneer het gaat om een verstrekking aan het register-MOT die noodzakelijk is om vast te kunnen stellen of een persoon geregistreerd staat in een register zware criminaliteit.

#### **Resumerend**

Voor de gegevens in een register zware criminaliteit geldt, dat deze in beginsel kunnen worden verwerkt ten behoeve van het register-MOT. De WPolr voorziet in art. 13a lid 4 en 13b lid 2 WPolr in de mogelijkheid (verplichting) van een (beperkte) verstrekking. Dit is niet anders wanneer de verstrekking plaatsvindt in het kader van een koppeling. Ook het modelreglement van een register zware criminaliteit voorziet in een dergelijke mogelijkheid.

#### *8.2.4.4 Conclusie verwerking bijzondere politieregisters*

Het is niet mogelijk om in het kader van een ongericht dataminingonderzoek met betrekking tot het register-MOT gebruik te maken van een tijdelijk politieregister. Hiermee dient ook rekening te worden gehouden wanneer men gebruik maakt van verwijsindexen als het MRO-bestand. Voor een verstrekking aan het register-MOT uit een voorlopig politieregister en een register zware criminaliteit bestaat een wettelijke regeling. Desondanks staat het modelreglement van het voorlopige politieregister een koppeling van dit register met het register-MOT in de weg. Omdat een verstrekking aan het register-MOT niet direct noodzakelijk is voor het doel van een voorlopig politieregister maar berust op een aparte wettelijke grondslag, is niet voldaan aan de voorwaarden om te mogen koppelen. Een verstrekking lijkt daarmee alleen mogelijk uit een register zware criminaliteit. Die dient dan wel beperkt te blijven tot gegevens die noodzakelijk zijn om

vast te kunnen stellen of de in het register-MOT geregistreerde naam ook in een register zware criminaliteit voorkomt. Een verstrekking van meer gegevens dan noodzakelijk is kan worden aangemerkt als een ontoelaatbare inbreuk op de persoonlijke levenssfeer.

### 8.3 Afsluitend

Hierna worden de belangrijkste bevindingen en aanbevelingen die uit dit hoofdstuk naar voren komen kort aangestipt. Afsluitend volgt een overzicht van de mogelijkheden van het ongerichte dataminingonderzoek met betrekking tot een register-MOT.

In feite maakt het Meldpunt reeds gebruik van datamining. Een analysemethode kan ook als datamining worden aangemerkt wanneer bij de aanvang daarvan al bekend is waarnaar wordt gezocht. Bij ieder dataminingonderzoek (in het kader van de opsporing) dient, ten minste in grote lijnen, om twee redenen een doelstelling aanwezig te zijn. Gegevens die in het kader van een dataminingonderzoek worden verwerkt kunnen in beginsel steeds worden aangemerkt als informatie. Zij hebben een bepaalde betekenis voor het onderzoek en zijn op grond daarvan geselecteerd. Een zodanige selectie is slechts mogelijk wanneer tot op zekere hoogte bekend is waarnaar men zoekt. Daarnaast is ook voor een juridische grondslag voor het mogen verwerken van gegevens een duidelijk doel noodzakelijk. Of er sprake is van dataminingonderzoek wordt bepaald door het antwoord op de vraag, of de bewerking die plaatsvindt betrekking heeft op een bepaalde of op een onbepaalde groep van personen. Alleen in het laatste geval is sprake van dataminingonderzoek, aangezien een bewerking in het eerste geval gericht is op een verificatie van gegevens waarover al wordt beschikt.

Opgemerkt zij verder dat registervergelijking en datamining niet als twee los van elkaar staande zaken gezien dienen te worden. Ook een onderzoek waarbij gericht wordt gezocht kan als dataminingonderzoek worden aangemerkt. Registervergelijking staat niet naast (het) datamining(s)proces maar maakt daar als bewerking van de verkregen informatie deel van uit. Ook in die zin kan in het kader van de werkzaamheden van het Meldpunt worden gesproken van de toepassing van dataminingonderzoek.

Bij het opstellen van het van het modelreglement van een voorlopig politieregister lijkt geen rekening te zijn gehouden met art. 13*b* lid 2 WPolr, waar de wetgever een uitzondering heeft gemaakt voor de verstrekking aan het register-MOT. Dit heeft vergaande gevolgen voor de mogelijkheid tot koppeling van een voorlopig politieregister met dat register. Aangezien het modelreglement van het voorlopige register een koppeling in de weg staat is deze, gezien het bepaalde in art. 6 lid 2 WPolr, uitgesloten. Het is de vraag of dit een wenselijke beperking betreft.

Op grond van art. 4 WPolr mogen persoonsgegevens alleen worden verwerkt indien dat noodzakelijk is voor de uitvoering van de politietaak. Dit betekent dat het niet mogelijk

is om gegevens te vergaren over een onbepaalde groep van burgers voor algemene politieke doeleinden, ook niet uit openbare bronnen. Hoewel het Meldpunt gegevens vergaart met het oog op een bepaald doel, ligt aan die vergaring geen verdenking ten grondslag. In dit verband zij gewezen op het belang om aan een ongebruikelijke transactie de kwalificatie van verdenking te koppelen. Daardoor wordt het mogelijk om ook gebruik te maken van openbare bronnen.

Teneinde de gegevens uit een tijdelijk politieregister beschikbaar te maken voor het Meldpunt kan worden overwogen, de status van een MRO-bestand te herzien. In navolging van het register-MOT zou een MRO-bestand kunnen worden gekwalificeerd als een gewoon politieregister met een beperkt verstrekkingenregime. Dit betekent dat de gegevens niet langer beschikbaar zijn voor operationeel gebruik. Met het oog op de toegevoegde waarde van verwijfsindexen voor de opsporingstaak gaat de voorkeur uit naar een oplossing die niet alleen ziet op MRO-bestanden. Door een verwijfsindex als bijzonder politieregister te kwalificeren wordt het probleem van het afwijkende verstrekkingenregime voor alle verwijfsindexen ondervangen. Om ten behoeve van het register-MOT gebruik te maken van gegevens uit een tijdelijk politieregister kan worden overwogen om, overeenkomstig de regeling voor het voorlopige politieregister, te voorzien in een aparte mogelijkheid daartoe.

Op grond van art. 13*d* lid 3 WPolr is het vastleggen en gebruiken van persoonsgegevens voor de doeleinden van par. 3*a* WPolr slechts mogelijk overeenkomstig het bij of krachtens par. 3*a* WPolr bepaalde. Het doel van het register-MOT rechtvaardigt ook een registratie in een register zware criminaliteit. Met het oog op de formulering van art. 13*d* lid 3 WPolr lijkt dit te betekenen dat die gegevens niet in het register-MOT, maar in een register zware criminaliteit dienen te worden vastgelegd. Gegevens in het register-MOT kunnen immers worden aangemerkt als persoonsgegevens die worden vastgelegd voor een van de doeleinden als bedoeld in par. 3*a* WPolr. Toch staat het bepaalde in art. 13*d* lid 3 WPolr een verwerking in het kader van het register-MOT niet in de weg. Wanneer gegevens in het register-MOT worden vastgelegd is een registratie van die gegevens voor dat doel in een register zware criminaliteit nog niet mogelijk. De gegevens in het register-MOT hebben betrekking op onverdachte personen en art. 13*a* lid 1 WPolr biedt in beginsel geen ruimte voor registratie van die gegevens in een register zware criminaliteit<sup>89</sup>. Hoewel het doel verwijst naar een register zware criminaliteit, is een registratie voor dat doel enkel nog maar mogelijk in het register-MOT. Om verwarring op dit punt te voorkomen, kan worden overwogen om art. 13*d* lid 3 WPolr anders te formuleren. Met de toevoeging van het woord 'kunnen' wordt aangegeven, dat de bescherming van

---

89. In dat geval zou het een ingrijpend middel betreffen, wat in dit stadium van het proces van informatiegaring niet is toegestaan.

art. 13d lid3 WPolr slechts van toepassing is indien het gaat om gegevens die ook daadwerkelijk kunnen worden vastgelegd onder par. 3a WPolr.

### *Overzicht en schema*

#### **1. Geen gebruik van externe gegevens**

##### *Algemene voorwaarden*

- Het onderzoek is noodzakelijk voor een goede uitvoering van de politietaak voor zover het de strafrechtelijke handhaving van de rechtsorde betreft.
- Er is voldaan aan het doelbindingsbeginsel.
- Het onderzoek wordt uitgevoerd door, dan wel onder het gezag van, de beheerder van het register-MOT.

##### *Koppeling*

Nee.

##### *Toepassing en specifieke beperkingen*

Naast de algemene voorwaarden bestaan in beginsel geen aanvullende beperkingen.

#### **2. Gebruik van gegevens die niet afkomstig zijn uit een politieregister**

##### *Algemene voorwaarden*

- Het onderzoek is noodzakelijk voor een goede uitvoering van de politietaak voor zover het de strafrechtelijke handhaving van de rechtsorde betreft.
- Er is voldaan aan het doelbindingsbeginsel.
- Het onderzoek wordt uitgevoerd door, dan wel onder het gezag van, de beheerder van het register-MOT.

##### *Koppeling*

Indien sprake is van koppeling<sup>90</sup> gelden aanvullende voorwaarden:

- een koppeling dient noodzakelijk te zijn voor de politietaak voor zover het de strafrechtelijke handhaving van de rechtsorde betreft;
- een eventuele koppeling dient noodzakelijk te zijn voor het doel van het basisregister<sup>91</sup>;

---

90. Er is geen sprake van koppeling indien het gaat om externe gegevens die geen onderdeel uitmaken van een zelfstandig register.

91. Het register waarop het dataminingonderzoek betrekking heeft.

- om te mogen koppelen dient het reglement van het basis(politie)register in die mogelijkheid te voorzien<sup>92</sup>;
- met het gebruik van externe gegevens wordt geen ontoelaatbare inbreuk gemaakt op de privacy;<sup>93</sup>
- het gebruik van (persoons)gegevens uit een openbaar register is in beginsel niet toegestaan.

#### *Toepassing en specifieke beperkingen*

Naast de algemene voorwaarden dient in het geval van een koppeling rekening te worden gehouden met de daarvoor geldende regels.

### **3. Gebruik van gegevens uit een gewoon politieregister**

#### *Algemeen*

- Het onderzoek is noodzakelijk voor een goede uitvoering van de politietaak voor zover het de strafrechtelijke handhaving van de rechtsorde betreft.
- Er is voldaan aan het doelbindingsbeginsel.
- Het onderzoek wordt uitgevoerd door, dan wel onder het gezag van, de beheerder van het register-MOT.

#### *Koppeling*

Bij het gebruik van een ander gewoon politieregister is in beginsel steeds sprake van een koppeling.

- Een koppeling dient noodzakelijk te zijn voor de politietaak voor zover het de strafrechtelijke handhaving van de rechtsorde betreft;
- een eventuele koppeling dient noodzakelijk te zijn voor het doel van het basisregister;
- om te mogen koppelen dienen de reglementen van de betrokken politieregisters in de mogelijkheid daartoe te voorzien;
- met het gebruik van externe gegevens wordt geen ontoelaatbare inbreuk gemaakt op de privacy.

#### *Toepassing en specifieke beperkingen*

Naast de algemene en aanvullende voorwaarden dient rekening te worden gehouden met de beperkende werking van de doelbinding, de politietaak of weigering door de beheerder van een politieregister.

---

92. Tenzij de externe gegevens geen deel uitmaken van enig (politie)register. In dat geval is er geen sprake van een wettelijke koppeling.

93. In dat geval zou het een ingrijpend middel betreffen, wat in dit stadium van het proces van informatiegaring niet is toegestaan.

*Politietaak*

Het gebruik van politieregisters die niet zijn aangelegd in het kader van de politietaak (betreffende de strafrechtelijke handhaving van de rechtsorde) is niet vanzelfsprekend.

- Gebruik openbare orde register: beperkt mogelijk indien een verstrekking past binnen de bevoegdheid van art. 2 Politiewet.
- Gebruik Hulpverleningsregister: in beginsel niet mogelijk (onder meer op grond van het doelbindingsbeginsel).

*Doelbinding*

- Gebruik Hulpverleningsregister: in beginsel is verstrekking slechts mogelijk wanneer aan het doelbindingsbeginsel is voldaan.
- Gebruik gewone politieregisters: mogelijk voor zover dat noodzakelijk is voor het doel waarvoor wordt verstrekt<sup>94</sup>.

*Weigering door beheerder*

De beheerder van een register kan in bepaalde gevallen op grond van art. 11 BPolr een verstrekking weigeren, indien dat noodzakelijk is voor een goede uitvoering van de politietaak.

#### 4. Gebruik van gegevens uit een bijzonder politieregister

*Algemeen*

- Het onderzoek is noodzakelijk voor een goede uitvoering van de politietaak voor zover het de strafrechtelijke handhaving van de rechtsorde betreft.
- Er is voldaan aan het doelbindingsbeginsel.
- Het onderzoek wordt uitgevoerd door, dan wel onder het gezag van, de beheerder van het register-MOT.

*Koppeling*

Bij een verwerking van gegevens uit een bijzonder politieregister in het kader van een ongericht dataminingonderzoek is in beginsel sprake van koppeling.

- Een koppeling dient noodzakelijk te zijn voor de politietaak voor zover het de strafrechtelijke handhaving van de rechtsorde betreft;
- een eventuele koppeling dient noodzakelijk te zijn voor het doel van het basisregister;
- om te mogen koppelen dienen de reglementen van de betrokken politieregisters in de mogelijkheid daartoe te voorzien;

---

94. Art. 4 lid 2 WPolr.

- met het gebruik van externe gegevens wordt geen ontoelaatbare inbreuk gemaakt op de privacy.

*Toepassing en specifieke beperkingen*

Naast de algemene en aanvullende voorwaarden kennen bijzondere politieregisters een verstrekkingenregime dat het gebruik van deze registers beperkt.

- Tijdelijk politieregister: het gebruik van dit register is niet mogelijk.
- Voorlopig politieregister: het gebruik van dit register is niet mogelijk.
- Register zware criminaliteit: het gebruik van dit register is mogelijk.

Bovenstaande uiteenzetting van de vier verschillende vormen van ongericht dataminingonderzoek is onderstaand in schema weergegeven.

Onggericht dataminingonderzoek	Koppeling	Beperkingen	Gebruik
Geen externe gegevens	Nee	Algemeen	Onbeperkt
Externe gegevens*	Ja	Algemeen/koppeling	Beperkt
Gegevens uit een gewoon politieregister	Ja	Algemeen/koppeling/specifiek	Beperkt
Gegevens uit een bijzonder politieregister	Ja	Algemeen/koppeling/specifiek	Beperkt toegestaan voor het register zware criminaliteit

\* Uitgezonderd de gegevens die in de politieregisters liggen opgeslagen.

*Schema 12 Overzicht toepassingsmogelijkheden van een ongericht dataminingonderzoek ter verbetering van de informatiepositie van het register-MOT*

---

## 9 Ongericht dataminingonderzoek en de bijzondere politieregisters

In dit hoofdstuk wordt voor elk van de drie bijzondere politieregisters onderzocht, in hoeverre ongericht dataminingonderzoek kan worden gebruikt ter verbetering van de informatiepositie van die registers. Daaraan voorafgaand wordt ingegaan op de functie en de positie van de criminele inlichtingeneenheden (CIE), gevolgd door een beknopte uiteenzetting van de functies die de bijzondere politieregisters kunnen vervullen.

### 9.1 De criminele inlichtingeneenheden

Deze sectie gaat in op de rol die de criminele inlichtingeneenheden kunnen vervullen bij de toepassing van datamining. Begonnen wordt met een kort overzicht van de wijze waarop de uitwisseling van opsporingsinformatie bij de bestrijding van de zware criminaliteit is georganiseerd en welke instanties daarbij zijn betrokken. Vervolgens wordt ingegaan op de regeling criminele inlichtingeneenheden en de gevolgen van die regeling voor de toepassing van datamining.

#### Organisatiestructuur informatie-uitwisseling

Tot 1998 werden politie en justitie bij de bestrijding van de zware criminaliteit ondersteund door de divisie Centrale Recherche Informatie (CRI). Na opheffing van de CRI werden de meeste taken overgenomen door de Dienst Nationale Recherche Informatie (DNRI)<sup>1</sup>. De DNRI ondersteunt en coördineert opsporingsprocessen van het OM en de regionale politiekorpsen, waarbij de nadruk ligt op de bestrijding van de zware, de georganiseerde en de bovenregionale criminaliteit. De DNRI heeft de volgende taken:

- verzamelen, vastleggen, bewerken, analyseren en verstrekken van gegevens en informatie;
- ontwikkelen, delen, toepassen en evalueren van expertise en kennis ten behoeve van de bestrijding van de zwaardere vormen van criminaliteit, daarbij inbegrepen de coördinatie en de beleidsadvisering over de bestrijding van criminaliteit.

---

1. *Kamerstukken II*, 2002 /03, 28 845, nrs. 1-2, p. 8.

In het kader van de informatie-uitwisseling zijn twee units in het bijzonder van belang, te weten de unit Recherche Informatie Uitwisseling (RIU) en de unit Nationaal Inzicht (NI). De unit RIU vormt de schakel tussen onder meer de CIE's en informatiedesks enerzijds en het Korps Landelijke Politie Diensten (KLPD) anderzijds. Zij is verantwoordelijk voor het doen verstrekken en verzamelen van relevante recherche-informatie. De unit NI is verantwoordelijk voor het proces van het vastleggen, bewerken en analyseren van de aangeleverde recherche-informatie. Voor het ontsluiten van de door de RIU verzamelde informatie wordt deze vastgelegd in gestandaardiseerde applicaties. Het NI heeft een ontwikkelingsrol en beheert de verwijzindexen zoals bijvoorbeeld de VROS, welke bestaat uit de CIE-index en de MRO-index. Op basis van de verzamelde informatie worden operationele misdaadanalyses opgesteld, waaruit voorstellen tot opsporingsonderzoeken kunnen resulteren. Ook de nog te bespreken NCIE is ondergebracht in de unit NI. Hoewel deze uiteenzetting slechts enkele onderdelen van de informatiestructuur belicht, geeft het een beeld van de complexiteit van de wijze waarop informatie uitwisseling plaatsvindt. Er zijn veel instanties, verwijzindexen en systemen die alle op een bepaalde manier met elkaar dienen samen te werken ten behoeve van een goede informatiepositie. De wijze waarop dit gebeurt moet in overeenstemming zijn met de WPolr en het BPolr. Vooral bij de bestrijding van de zware criminaliteit, waarbij vergaande inbreuken op de persoonlijke levenssfeer mogelijk zijn en veelvuldig gebruik wordt gemaakt van verwijzindexen, is een kritische toetsing nodig. In het kader hiervan wordt onderzocht hoe de regeling criminele inlichtingeneenheden zich verhoudt tot de WPolr en het BPolr.

### **De regeling criminele inlichtingeneenheden**

Gegevens die kunnen worden vastgelegd in een voorlopig politieregister of het register zware criminaliteit worden aangemerkt als criminele inlichtingen<sup>2</sup>. De criminele inlichtingeneenheden<sup>3</sup> zijn belast met de informatievoorziening in het kader van de uitvoering van de politietaak voor zover het de zware criminaliteit betreft. Ingegaan wordt op de regeling criminele inlichtingeneenheden (CIE-regeling)<sup>4</sup> en de functie die de CIE kan vervullen bij de toepassing van het dataminingsproces ten behoeve van de registers die zij beheren en de opsporing als geheel. Een voorlopig politieregister wordt evenals een register zware criminaliteit bijgehouden door de CIE. Verder is de CIE verantwoordelijk voor een tijdelijk politieregister wanneer dat wordt aangelegd in het kader van een onderzoek dat raakt aan de zware criminaliteit als bedoeld in art. 1 lid 1 onder *k* WPolr. Dit laat een

---

2. Art. 1 onder *e* CIE-regeling.

3. De eenheid bij de regionale politiekorpsen, bedoeld in art. 5 lid 1 van het Besluit beheer regionale politiekorpsen alsmede de eenheid bij het Korps landelijke politiediensten, bij de bijzondere ambtenaren van politie (rijksrecherche) en bij de Koninklijke Marechaussee, belast met de taak bedoeld in art. 2 van de CIE-regeling.

4. De CIE-regeling is op 1 november 2000 van kracht geworden en vervangt de CID-regeling 1995.

(incidentele) verwerking van bedoelde informatie door andere onderdelen binnen de politieorganisatie overigens onverlet. Deze onderdelen komen ook in aanraking met dit soort informatie en dienen ervoor te zorgen dat deze te bestemder plaatse komt. In de praktijk betekent dit dat, wanneer andere organisatieonderdelen binnen de politie beschikken over informatie die alleen maar in aanmerking kan komen voor registratie in de bijzondere politieregisters, deze hun weg moeten kunnen vinden naar de CIE. Voor gegevens die in aanmerking komen voor registratie in een register zware criminaliteit kan het in bepaalde gevallen wenselijk zijn, een tijdelijk politieregister aan te leggen. Een onderzoek waarbij gebruik wordt gemaakt van een tijdelijk politieregister met betrekking tot een misdrijf als bedoeld in art. 1 lid 1 onder *k* WPolr dient op grond van art. 2 van de CIE-regeling te worden uitgevoerd door de CIE. Een uniforme werkwijze en een goede samenwerking zijn essentieel voor een effectieve invulling van de opsporingstaak. De CIE-regeling bepaalt<sup>5</sup> dat de criminele inlichtingeneenheden alles in het werk dienen te stellen om de hun opgedragen taken zo doeltreffend mogelijk uit te voeren. Een uniforme gegevensverwerking en een onderlinge uitwisseling van gegevens verkleint de kans op gefragmenteerde gegevensregistratie en daarmee op het onopgemerkt blijven van bepaalde informatie.

#### *9.1.1 De toepassing van dataminingonderzoek*

Met het oog op de taakstelling van de CIE als beschreven in art. 4 CIE-regeling, lijkt de CIE de eerst aangewezen instantie voor het doen van dataminingonderzoek. In de CIE-regeling is voor de criminele inlichtingeneenheid een primaire rol weggelegd, wanneer het gaat om het actief inwinnen van gegevens (uit welke bron dan ook) die relevant zijn voor de bestrijding van zware criminaliteit en het actief doorsluizen van dergelijke informatie binnen de overige onderdelen van de politie indien deze geschikt is voor operationeel gebruik of wanneer daarmee op andere gronden de goede uitvoering van de politietaal is gediend. Tot de werkzaamheden van de CIE behoren in ieder geval:

- a. verzamelen en verifiëren van criminele inlichtingen;
- b. registreren van gegevens in een register zware criminaliteit en een voorlopig politieregister overeenkomstig de daartoe vastgestelde modelreglementen;
- c. bevorderen van het gericht inwinnen en aanvullen van criminele inlichtingen en andere gegevens die in het kader van de strafrechtelijke handhaving van de rechtsorde in aanmerking komen voor registratie op grond van de WPolr;
- d. analyseren van criminele inlichtingen en het aan de hand daarvan:
  - signaleren van criminaliteitsontwikkelingen, voorzover het betreft misdrijven als bedoeld in art. 1 lid 1 onder *k* WPolr;
  - periodiek verslag doen ten behoeve van criminaliteitsbeelden;

---

5. Art. 3 en 6 CIE-regeling.

- e. verstrekken van criminele inlichtingen overeenkomstig de daartoe vastgestelde modelreglementen.

Voor de toepassing van het dataminingsproces zijn vooral de onderdelen *a*, *c* en *d* van art. 4 lid 1 interessant, omdat deze zien op de verwerking van criminele inlichtingen. Het bepaalde in art. 4 lid 1 onder *b* en *e* CIE-regeling betreft voornamelijk het gebruik van de bijzondere politieregisters. Met betrekking tot de formulering van art. 4 CIE-regeling kan worden overwogen om het daarin onderscheiden verzamelen, verifiëren en analyseren van gegevens onder te brengen onder de noemer ‘verwerken van criminele inlichtingen’.

Volgens art. 4 lid 1 onder *a* CIE-regeling behoort het verzamelen en verifiëren van criminele inlichtingen tot het takenpakket van de CIE. Daartoe worden gegevens opgevraagd uit open bronnen, politieregisters en andere registraties en kunnen tips, meldingen, etc. die op een andere wijze bij de CIE zijn terechtgekomen, nauwkeurig tegen het licht worden gehouden. Op grond van art. 4 lid 1 onder *c* CIE-regeling dient de CIE het gericht inwinnen en aanvullen van criminele inlichtingen en andere gegevens die in het kader van de strafrechtelijke handhaving van de rechtsorde in aanmerking komen voor registratie op grond van de WPolr te bevorderen. Volgens de toelichting op de CIE-regeling ziet deze bepaling echter uitsluitend op het runnen van informanten. In art. 4 lid 1 onder *d* CIE-regeling is bepaald dat de CIE ook verantwoordelijk is voor het analyseren van criminele inlichtingen. Die analyse dient niet alleen het signaleren van criminaliteitsontwikkelingen en de periodieke verslaglegging ten behoeve van criminaliteitsbeelden, maar betreft ook een daarvan losstaande werkzaamheid die bijvoorbeeld tot verrijking van geregistreeerde informatie kan leiden of kan uitmonden in gegevens die zich direct lenen voor operationeel gebruik. De Raad van Advies voor de CIE heeft geadviseerd het ‘analyseren van criminele inlichtingen’ in onderdeel *d*, te wijzigen in ‘het doen analyseren’. Hiermee zou tot uitdrukking worden gebracht dat de analysefunctie ook buiten de CIE kan worden ingevuld. Dit advies is niet overgenomen, omdat art. 14 van het modelreglement van het register zware criminaliteit zich niet verzet tegen autorisatie van ambtenaren die niet werkzaam zijn bij de CIE. Hiermee wordt de mogelijkheid opengelaten om een ongericht dataminingsonderzoek met betrekking tot een voorlopig politieregister of een register zware criminaliteit door een ander dan de beheerders van deze bijzondere politieregisters zelf te laten uitvoeren. Met het oog op de bescherming van de persoonlijke levenssfeer is het echter de vraag of dit wenselijk is. Een verwerking door een ander dan de beheerder van het register mag er niet toe leiden dat de normaliter van toepassing zijnde waarborgen komen te vervallen. Op grond van art. 4 lid 2 CIE-regeling dient de CIE onder meer gebruik te maken van de door de Ministers aangewezen geautomatiseerde verwijzingsindex. Op deze wijze kan snel worden nagegaan of bepaalde personen reeds bekend zijn bij andere criminele inlichtingeneenheden en blijft de inbreuk op de persoonlijke levenssfeer zoveel mogelijk beperkt. In het kader van een ongericht dataminingsonderzoek lijkt vooral de analyse van criminele inlichtingen aan-

knopingspunten te bieden voor het doen van dataminingonderzoek met betrekking tot gegevens in een voorlopig politieregister of een register zware criminaliteit.

De CIE-regeling maakt onderscheid tussen de criminele inlichtingeneenheid en de nationale criminele inlichtingeneenheid. In het hierna volgende wordt voor beide eenheden gekeken op welke wijze een verbetering van de informatiepositie kan worden nagestreefd middels datamining.

### *9.1.2 Datamining door de CIE*

Op grond van art. 6 lid 2 CIE-regeling wisselen de CIE's onderling, gevraagd en ongevraagd, criminele inlichtingen uit indien dit van belang kan zijn voor de uitvoering van de politietaak. Het betreft gegevens uit zowel de voorlopige politieregisters als de registers zware criminaliteit waarbij gebruik wordt gemaakt van een modelformulier.

Bepaalde ambtenaren van iedere CIE hebben rechtstreeks toegang tot de registers zware criminaliteit die gevoerd worden bij overige CIE's. Dit maakt een snelle en effectieve aanvulling en verificatie van mogelijk relevante gegevens mogelijk. Een dergelijke toegangsregeling ontbreekt voor de voorlopige politieregisters. Nu er geen nadere beperkingen worden gesteld aan de aard van de gegevens die kunnen worden uitgewisseld, is het op grond van art. 6 CIE-regeling mogelijk om met behulp van dataminingonderzoek de informatiepositie van de registers zware criminaliteit (die door de CIE's worden beheerd) op landelijk niveau te verbeteren.

#### **Grondslag datamining en nadelen**

Het bepaalde in art. 6 CIE-regeling biedt de mogelijkheid om de informatiepositie ten behoeve van de bestrijding van de zware criminaliteit te verbeteren. Het eerste lid van art. 6 regelt dat de verschillende registers zware criminaliteit en de verschillende voorlopige politieregisters toegang tot elkaar hebben, waardoor een verbetering van de informatiepositie van een register zware criminaliteit of een voorlopig politieregister mogelijk wordt gemaakt. Door gefragmenteerde gegevens te verenigen krijgen deze een grotere waarde en kunnen verbanden worden aangetoond die daarvoor niet zichtbaar waren.

Toch vormt deze regeling niet de meest ideale grondslag voor een dataminingonderzoek. Ten eerste is de verplichting tot het onderling uitwisselen van gegevens min of meer vrijblijvend geformuleerd. Ook kost het gebruik van modelformulieren meer tijd dan een situatie waarbij sprake is van rechtstreekse toegang. De efficiëntie van deze regeling kan voorts in twijfel worden getrokken vanwege het feit, dat voor elk register afzonderlijk wordt gestreefd naar een verbetering van de informatiepositie. Op grond van art. 6 lid 2 en 3 kunnen registers zware criminaliteit rechtstreeks onderling worden geraadpleegd, hetgeen een efficiënte aanvulling en verificatie van gegevens mogelijk maakt. Een verbetering van de informatiepositie van een register zware criminaliteit op grond van art. 6 lid 2 en 3 CIE-regeling heeft als voordeel (ten opzichte van art. 6 lid 1) dat er sprake is

van een directe toegang. Nadeel is dat een dergelijke verbetering alleen met betrekking tot registers zware criminaliteit kan worden nagestreefd; bovendien is een centrale regeling niet mogelijk, doch dient elk register afzonderlijk te worden verbeterd. Gezien genoemde nadelen lijkt art. 6 CIE-regeling niet geschikt om als grondslag te dienen voor een dataminingonderzoek ter verbetering van de informatiepositie van een voorlopig politieregister of een register zware criminaliteit.

### 9.1.3 Datamining door de NCIE

Op grond van art. 8 van de CIE-regeling voert de NCIE een nationaal register zware criminaliteit en een nationaal voorlopige politieregister, waarin criminele inlichtingen van nationale en internationale betekenis kunnen worden opgeslagen. Voorts<sup>6</sup> zorgt deze eenheid ervoor dat de personalia of bedrijfsgegevens van alle personen die op grond van art. 13a lid 1 onder *a* en *b* WPolr geregistreerd zijn, worden opgenomen in een verwijsindex die voor elke CIE toegankelijk is<sup>7</sup>. Daarnaast worden de codes betreffende informantgegevens bijgehouden als bedoeld in art. 5 CIE-regeling. Ten slotte registreert de NCIE de overige informatie die van belang kan zijn voor de landelijke en internationale coördinatie en ondersteuning door de NCIE. De verschillende CIE's zijn verplicht zijn tot een structurele verstrekking van gegevens aan de NCIE. De NCIE analyseert de gegevens die aanwezig zijn in het nationaal register zware criminaliteit en het nationaal voorlopige politieregister. De nationale registers en de verwijsindex met de personalia of bedrijfsgegevens van alle personen die op grond van art. 13a lid 1 onder *a* en *b* WPolr geregistreerd zijn, staan ter beschikking aan hen die daar bij of krachtens de WPolr aanspraak op kunnen maken. Opgemerkt zij dat gegevens omtrent onverdachte personen als bedoeld in art. 13a lid 1 onder *c* WPolr niet aan de NCIE lijken te worden verstrekt waardoor zij geen deel uitmaken van eventuele analyses. Hoewel de uitwisseling van die gegevens wellicht zou kunnen plaatsvinden op grond van art. 7 lid 1 onder *a* of *d* CIE-regeling, lijkt art. 7 lid 1 onder *b* CIE-regeling deze mogelijkheid te willen uitsluiten door enkel voor de gegevens in 13a lid 1 onder *a* en *b* WPolr te bepalen dat zij worden verstrekt. Ook in art. 8 lid 1 onder *b* CIE-regeling wordt alleen verwezen naar de gegevens als bedoeld in art. 13a lid 1 onder *a* en *b* WPolr.

### Grondslag datamining en nadelen

In het nationaal register zware criminaliteit en het nationaal voorlopige politieregister bevinden zich de gegevens uit de verschillende registers zware criminaliteit en de voorlopige politieregisters die van nationale of internationale betekenis worden geacht. Het is de vraag wanneer gegevens precies aan dit 'betekeniscriterium' voldoen en op welke wijze

---

6. Zie art. 7 CIE-regeling.

7. De CIE's zijn verplicht om de desbetreffende gegevens via de aangewezen geautomatiseerde verwijsindex aan de NCIE te verstrekken.

dat wordt vastgesteld. Het middels het dataminingsproces zichtbaar maken van bepaalde nationale dan wel internationale verbanden tussen gegevens kan ondersteuning bieden bij de afweging of gegevens al of niet in aanmerking komen voor verwerking door de NCIE. In art. 8 lid 2 van de CIE-regeling is bepaald dat de NCIE de gegevens in het nationale register zware criminaliteit en het nationale voorlopige politieregister analyseert. Deze bepaling kan als grondslag dienen voor het verrichten van dataminingonderzoek. De NCIE lijkt de eerst aangewezen instantie om dataminingonderzoek te verrichten ter verbetering van de algemene informatiepositie ter bestrijding van de zware criminaliteit. Volstaan kan worden met een centraal dataminingonderzoek; de afzonderlijke bijzondere politieregisters hebben immers toegang tot de nationale politieregisters en de verwijfsindex.

Ook aan art. 8 CIE-regeling kleven enkele nadelen. Met betrekking tot de nationale registers is het niet geheel duidelijk welke gegevens daar precies in worden opgenomen. Kunnen bijvoorbeeld gegevens als bedoeld in art. 13a lid 1 onder *c* WPolr ook deel uitmaken van de verwijfsindex bedoeld in art. 8 lid 1 onder *b* CIE-regeling? Ook is niet helder hoe het bepaalde in art. 8 lid 1 onder *a* CIE-regeling zich verhoudt tot art. 8 lid 1 onder *b* CIE-regeling. Op grond van art. 8 lid 1 onder *b* CIE-regeling houdt de NCIE een geautomatiseerde verwijfsindex bij van de personen en bedrijven als bedoeld in art. 13a lid 1 onder *a* en *b* WPolr. Dit zou betekenen dat geen landelijke verwijfsindex wordt bijgehouden van de gegevens genoemd in art. 13a lid 1 onder *c* WPolr. De toelichting op de CIE-regeling<sup>8</sup> geeft echter aan dat de NCIE zorgt voor opname van de personalia of bedrijfsgegevens van *alle* personen die op grond van art. 13a lid 1 WPolr geregistreerd zijn in een verwijfsindex die voor elke CIE toegankelijk is. Naar de letter genomen betekent dit, dat ook de personen als bedoeld in art. 13a lid 1 onder *c* WPolr in de verwijfsindex worden opgenomen. Voorts kan de vraag worden gesteld of de gegevens in de verwijfsindex als bedoeld in art. 8 lid 1 onder *b* CIE-regeling ook worden opgenomen in het nationale register zware criminaliteit. De gegevens die op grond van art. 8 lid 1 onder *b* van de CIE-regeling worden vastgelegd, kunnen namelijk ook voldoen aan het criterium van art. 8 lid 1 onder *a* van de CIE-regeling. Duidelijkheid hieromtrent is van belang om een invulling te kunnen geven aan de analyse die plaatsvindt op grond van art. 8 lid 2 CIE-regeling.

### Resumerend

De CIE is bij uitstek geëquipeerd voor het verrichten van dataminingonderzoek, waarbij het in eerste instantie gaat om de door die instantie beheerde voorlopige politieregisters en registers zware criminaliteit. Ook is de CIE verantwoordelijk voor een tijdelijk politieregister dat is aangelegd in het kader van de uitvoering van de politietaak voor zover

---

8. *Stert.* 12 oktober 2000, nr. 198, p. 14.

betrekking hebbende op de misdrijven als bedoeld in art. 1 lid 1 onder *k* WPolr. Op grond van art. 6 CIE-regeling kan een beheerder van een voorlopig politieregister of een register zware criminaliteit een dataminingonderzoek verrichten ter verbetering van de informatiepositie van zijn register. Het is in beginsel echter efficiënter wanneer dergelijk onderzoek niet op lokaal, maar op nationaal niveau plaatsvindt. Hiervoor lijkt de NCIE de aangewezen instantie. In dat geval is het wenselijk dat de wijze waarop de CIE-regeling middels art. 8 in een nationaal gegevensbeheer voorziet, op enkele punten wordt herzien. Of met de NCIE-analyse de gegevens in de betrokken bijzondere politieregisters daadwerkelijk ten volle worden benut hangt onder meer af van de juiste keuze of een bepaald gegeven al dan niet van nationaal of internationaal belang is. Voorts lijkt de verwijzindex die wordt aangelegd geen overzicht te verschaffen van de personen die op grond van art. 13*a* lid 1 onder *c* WPolr worden geregistreerd.

In het streven naar een zo efficiënt mogelijk gebruik van de voorhanden zijnde criminele inlichtingen kan worden overwogen te kiezen voor afschaffing van het onderscheid tussen de afzonderlijke lokale voorlopige politieregisters en registers zware criminaliteit en hun nationale equivalenten, en de afzonderlijke lokale registers te vervangen door twee nationale registers. Het is onduidelijk wat de toegevoegde waarde is van het hanteren van afzonderlijke registers naast de overkoepelende nationale registers<sup>9</sup>. In plaats van gegevens voortdurend over en weer te sturen en dubbel te registreren kan worden geopteerd voor één nationaal systeem waartoe eenieder, al dan niet beperkt, toegang heeft. CIE's blijven daarbij verantwoordelijk voor de inhoud c.q. juistheid van de nationale registers, terwijl de beheerstaak en vooral de analyserende taak bij de NCIE ligt. Informatie is niet meer gefragmenteerd aanwezig en er hoeft niet meer te worden doorverstrekt en geanalyseerd op regionaal niveau, hetgeen tijd- en geldbesparend werkt. Een analyse kan plaatsvinden op nationaal niveau met betrekking tot alle voorhanden zijnde gegevens. Het resultaat van een dergelijke analyse komt steeds ten goede aan alle gebruikers van dat register die hierop bij of krachtens de WPolr aanspraak kunnen maken.

## 9.2 Functieverdeling bijzondere politieregisters

In deze sectie wordt stilgestaan bij de manier waarop de functies van de bijzondere politieregisters zich verhouden tot de mogelijkheid tot het verrichten van dataminingonderzoek. In het kader van de bestrijding van de zware criminaliteit bestaat grote behoefte aan vergaande analysemogelijkheden. Vanwege de ernst van deze vorm van criminaliteit en het belang van efficiënte bestrijding daarvan bestaat (in theorie) grote bereidwilligheid om in die behoefte te voorzien. Het is echter de vraag in hoeverre dit mogelijk is,

---

9. Ook vanuit technisch oogpunt lijkt het hanteren van twee afzonderlijke registers overbodig, indien nodig kan een onderscheid tussen lokale en nationale gegevens softwarematig binnen een nationaal register worden gerealiseerd.

gezien de functieverdeling van de bijzondere politieregisters. Na de IRT-affaire is een forse afname van het aantal registraties in deze bijzondere registers beoogd en zijn in het kader van de bescherming van de persoonlijke levenssfeer nadere voorwaarden gesteld aan de opslag en het gebruik van persoonsgegevens.

Een tijdelijk politieregister dient een specifiek doel in het kader waarvan actief gegevens worden verzameld en vastgelegd. Bij het vastleggen van gegevens in dit register gaan de functies van registratie en analyse hand in hand. Een registratie in het kader van een tijdelijk politieregister dient op grond van art. 13 WPolr plaats te vinden met het oog op het doel van het tijdelijk register. Omdat dit register een beperkt verstrekkingenregime kent kunnen er in het kader van een analyse allerhande gegevens in worden vastgelegd, zolang deze bijdragen aan het doel van het register. Een verwerking met betrekking tot een tijdelijk politieregister vindt in beginsel plaats in het kader een verkennend onderzoek of opsporingsonderzoek.

Bij een voorlopig politieregister is een duidelijker onderscheid aanwezig tussen registratie en analyse. Een verwerking in het kader van dit register is mogelijk om vast te kunnen stellen of geregistreerde personen in samenhang met andere gegevens kunnen worden opgenomen in een register zware criminaliteit. Wanneer gegevens worden verzameld in het kader van een ongericht dataminingonderzoek of een analyse met betrekking tot een voorlopig politieregister, komen deze in beginsel niet in aanmerking voor een zelfstandige registratie in dat register. Zij kunnen echter wel worden vastgelegd in het voorlopige politieregister met het oog op het doel van dat register. Het beperkte verstrekkingenregime van het voorlopige politieregister rechtvaardigt hier de ruime mogelijkheid tot registratie van gegevens in het kader van een analyse. Een verwerking van gegevens in het voorlopige politieregister vindt in beginsel plaats in het kader van het eerste stadium van het proces van informatiegaring: het opbouwen en in stand houden van een zekere informatiepositie.

Een register zware criminaliteit biedt een uitgelezen platform voor een analyse op het gebied van de bestrijding van de zware criminaliteit. Dit register is, in tegenstelling tot de overige bijzondere politieregisters, gericht op de bestrijding van de zware criminaliteit als geheel. Het doel van het register is een algemene verbetering van de informatiepositie voor zover het de zware criminaliteit betreft<sup>10</sup>. Hoewel het register de mogelijkheid biedt om op ruime schaal gegevens vast te leggen, geldt daarvoor een beperking door de voorwaarden die art. 13a WPolr stelt aan het gebruik van persoonsgegevens. Dit leidt ertoe dat alle gegevens die in het kader van een register zware criminaliteit worden verwerkt, in aanmerking dienen te komen om als zelfstandig subject in dit register te worden vastge-

---

10. *Kamerstukken II*, 1996/97, 25 403, nr. 3, p. 8.

legd. Een verwerking in het kader van een register zware criminaliteit kan in beginsel worden gerekend tot het eerste stadium van het proces van informatiegaring (het opbouwen en in stand houden van een zekere informatiepositie).

### *9.2.1 Analyse register zware criminaliteit en voorlopig politieregister*

Het register zware criminaliteit en het voorlopige politieregister vallen onder de verantwoordelijkheid van de CIE. In de CIE-regeling is aangegeven op welke wijze de gegevens in een register zware criminaliteit en een voorlopig politieregister kunnen worden verwerkt<sup>11</sup>. Verzamelde gegevens worden geverifieerd en het gericht inwinnen en aanvullen van criminele inlichtingen en andere gegevens die in het kader van de strafrechtelijke handhaving van de rechtsorde in aanmerking komen voor registratie op grond van de WPolr dient te worden bevorderd. Verder vindt een analyse van de gegevens plaats, waarbij onderscheid moet worden gemaakt tussen de gegevens die als zelfstandig subject voor registratie in deze registers in aanmerking komen en de gegevens die kunnen worden geregistreerd in het kader van een analyse. Het verzamelen en verifiëren van criminele inlichtingen ziet, volgens de toelichting op de CIE-regeling, op gegevens die in aanmerking komen voor registratie in een voorlopig politieregister of een register zware criminaliteit. Daarbij wordt gesteld dat op het moment van het verzamelen en (zo mogelijk) verifiëren nog geen zekerheid behoeft te bestaan omtrent de mogelijkheid tot registratie van de gegevens in één van de bijzondere politieregisters. De reden hiervoor is dat elders beschikbare en op te vragen gegevens in combinatie met de in eerste instantie ingewonnen gegevens pas tot de conclusie kunnen leiden, dat registratie gerechtvaardigd is. Hiermee wordt de mogelijkheid van analyse opengelaten. Volgens de toelichting op de CIE-regeling kan gebruik worden gemaakt van gegevens uit open bronnen, politieregisters en andere registraties. Verder kan het gaan om nauwkeurig tegen het licht gehouden tips, meldingen etc., die op een andere wijze bij de CIE terecht zijn gekomen. Externe gegevens die in het kader van een analyse van de al aanwezige gegevens in een register zware criminaliteit of een voorlopig politieregister worden verwerkt, zullen op enig moment worden vastgelegd om een bewerking mogelijk te maken. Hoewel het voor de hand ligt dat dit gebeurt in het register waarop de analyse betrekking heeft<sup>12</sup>, blijkt kortstondige registratie van zachte gegevens in een gewoon politieregister eveneens mogelijk.

### **Datawarehouse en artikel 5a WPolr**

Met betrekking tot het analyseren van gegevens laat de wetgever de mogelijkheid open om naar aanleiding van tips of meldingen persoonsgegevens kortstondig vast te leggen in de registers voor die doeleinden, zoals het BPS. De opslagcriteria voor het register zware criminaliteit of het voorlopige politieregister zijn hierop niet van toepassing, maar tips,

---

11. Art. 4 CIE-regeling.

12. Zie ook art. 13d lid 3 WPolr.

meldingen en constatering die niet worden bevestigd door aanvullende gegevens dienen na verloop van korte tijd te worden geëvalueerd<sup>13</sup>. Dit standpunt is uitgewerkt in art. 5a lid 1 onder *b* WPolr, op grond waarvan zachte gegevens voor een maximumtermijn van vier maanden kunnen worden vastgelegd in een gewoon politieregister<sup>14</sup>. De bevoegdheid van art. 5a WPolr is gericht op een doelmatige taakuitvoering van de politie<sup>15</sup>. De wetgever spreekt hierbij over tips en meldingen. In de toelichting op de CIE-regeling wordt echter ook gesproken over gegevens uit open bronnen, politieregisters en andere registraties. De analyse die in de toelichting op de CIE-regeling wordt beschreven betreft die in de zin van dataminingonderzoek<sup>16</sup>.

In het geval van tips en meldingen gaat het om de mogelijkheid om nieuw binnengekomen gegevens op een verantwoorde manier op te slaan, teneinde deze te kunnen analyseren. Hoewel art. 5a WPolr een mogelijkheid biedt om zachte gegevens vast te leggen in een gewoon politieregister is het niet aannemelijk, dat ook het analyseren van de gegevens steeds binnen dat register plaatsvindt. Een register in de zin van art. 5a lid 1 WPolr is namelijk niet geschikt om als datawarehouse te dienen; bij een analyse van de gegevens in dit register dient ook gebruik te kunnen worden gemaakt van gegevens uit andere (bijzondere) politieregisters. Het kan echter niet de bedoeling zijn dat gegevens die al in een (bijzonder) politieregister zijn vastgelegd, vervolgens op grond van art. 5a WPolr worden overgeheveld naar een register als het BPS. In dat geval komen zij namelijk in aanmerking voor operationeel gebruik, hetgeen strijdig is met het beperkte verstrekkingenregime van de bijzondere politieregisters. Een interpretatie van art. 5a WPolr, waarbij zachte gegevens (waarop normaal gesproken een beperkt verstrekkingenregime van toepassing is) te pas en te onpas in een gewoon politieregister kunnen worden opgenomen, is onwenselijk.

Concluderend biedt art. 5a lid 1 onder *b* WPolr een mogelijkheid tot registratie van gegevens teneinde deze te kunnen analyseren, maar kan het register daarbij in beginsel niet zelf als datawarehouse dienen. Het ligt daarom voor de hand dat de gegevens die in het kader van een analyse worden verwerkt (datawarehouse) worden vastgelegd in het register zware criminaliteit of het voorlopige politieregister zelf (basisregister).

### Het register zware criminaliteit en het voorlopige politieregister als datawarehouse

In de praktijk wordt de mogelijkheid van het verrichten van een dataminingonderzoek met betrekking tot een register zware criminaliteit beperkt door de registratiefunctie in

13. *Kamerstukken II*, 1996/97, 25 398, nr. 3, p. 8.

14. Zie sectie 5.2.2.2.

15. *Kamerstukken I*, 1998/99, 25 398, nr. 63b, p. 4.

16. Ten aanzien van de analysewerkzaamheden wordt in de toelichting op de CIE-regeling opgemerkt dat het analyseren van criminele inlichtingen ook als een losstaande werkzaamheid geldt die bijvoorbeeld tot verrijking van geregistreerde informatie kan leiden of kan uitmonden in gegevens die zich direct lenen voor operationeel gebruik.

samenhang met de (erg ruime) raadpleegfunctie van dat register. De mogelijkheid om persoonsgegevens te registreren in een register zware criminaliteit wordt met het oog op de bescherming van de persoonlijke levenssfeer beperkt door art. 13a lid 1 WPolr. Daar wordt precies aangegeven welke persoonsgegevens in dit register mogen worden vastgelegd. Het artikel spreekt over ‘opneming van persoonsgegevens (...) omtrent;’ Met ‘omtrent’ wordt duidelijk dat het niet alleen gaat om de namen van de categorieën van personen die art. 13a in lid 1 WPolr opsomt, maar ook om gegevens omtrent deze personen. Het is ongewenst dat persoonsgegevens die niet voor zelfstandige registratie in een register zware criminaliteit in aanmerking komen, langdurig worden vastgelegd. De gegevens in een register zware criminaliteit zijn grotendeels bestemd voor operationeel gebruik. Dit beperkt de mogelijkheid om gegevens waarop een afwijkend verstrekkingenregime van toepassing is en gegevens die niet voor registratie in een register zware criminaliteit in aanmerking komen in het kader van een analyse vast te leggen in het register zware criminaliteit. Dat zou tevens inhouden dat de gegevens in ‘het datawarehouse’ voor andere doeleinden kunnen worden gebruikt dan het dataminingonderzoek alleen. Met het oog op de beperkte registratiefunctie is het niet mogelijk om, naar aanleiding van tips of meldingen, persoonsgegevens over onverdachte personen vast te leggen in dit register met het oog op verwerking daarvan. Bij deze gegevens gaat het in beginsel noch om de categorieën van personen die mogen worden vastgelegd in een register zware criminaliteit, noch om gegevens waarvan op voorhand duidelijk is dat zij daarmee verband houden. Tips of meldingen worden juist vastgelegd om zodanige mogelijke verbanden aan te tonen middels een analyse. Dat is in beginsel slechts mogelijk in een voorlopig politieregister.

Een voorlopig politieregister kent geen specifieke beperking aangaande de registratie van persoonsgegevens. Opname van persoonsgegevens in dit register is mogelijk met het oog op het doel van het register. Deze ruimere registratiemogelijkheid wordt gerechtvaardigd door het beperkte verstrekkingenregime van dit register. ‘De waarborgen ter bescherming van de persoonlijke levenssfeer worden in dit geval niet zozeer gevonden in de criteria die de opslag van gegevens betreffen (het doel van het register biedt daarvoor onvoldoende houvast), maar vinden uitwerking in het zeer beperkte verstrekkingenregime dat voor het vaststellingsregister geldt<sup>17</sup>.’

### **9.3 Ongericht dataminingonderzoek en het tijdelijke politieregister**

Teneinde vast te stellen of het mogelijk is de informatiepositie van een tijdelijk politieregister te verbeteren met behulp van een ongericht dataminingonderzoek, zal dit bijzondere politieregister worden getoetst aan de voor deze dataminingsvariant kenmerkende eigenschappen.

---

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

### Doel

Een tijdelijk politieregister kan voor zeer uiteenlopende doeleinden worden gehanteerd. In tegenstelling tot de overige bijzondere politieregisters heeft het niet per definitie betrekking op de bestrijding van de zware criminaliteit<sup>18</sup>. Na aanleg van een tijdelijk register zal logischerwijs alles in het werk worden gesteld om het doel van dat register te bereiken, namelijk een specifieke verbetering van de informatiepositie. Dit in tegenstelling tot een ongericht dataminingonderzoek met betrekking tot het register-MOT, in het kader waarvan weliswaar gericht wordt gezocht maar waarbij het register betrekking heeft op meerdere zaken. Bij een tijdelijk politieregister zal ook een dataminingonderzoek ter verbetering van de informatiepositie van dat register een gericht karakter hebben<sup>19</sup>. Een ongericht dataminingonderzoek ligt dan ook niet in de rede.

Een tijdelijk politieregister dat wordt aangelegd in het kader van een verkennend onderzoek van art. 126gg Sv lijkt te neigen in de richting van de ongerichte dataminingsvariant. Hoewel een opsporingsonderzoek gestart zou kunnen worden kan het noodzakelijk zijn, eerst onderzoek te doen naar de gehele sector teneinde vast te kunnen stellen, op welke wijze de criminaliteit zich daarin genesteld heeft. In dat geval wordt niet alleen een verdachte of een 'betrokkene' bij de georganiseerde criminaliteit onderzocht, maar een veel grotere en lossere verzameling van personen<sup>20</sup>. Er wordt als het ware een stap terug gedaan in het proces van informatiegaring, namelijk van het opsporingsonderzoek naar het verkennend onderzoek<sup>21</sup>. Maar in beide gevallen is sprake van gericht dataminingonderzoek. Dit blijkt onder meer uit het feit dat de wetgever enerzijds spreekt over het maken van een misdaadanalyse op basis van de informatiepositie en anderzijds aangeeft, dat als vervolg hierop een verkennend onderzoek kan worden gedaan. Daarbij gaat het om een gericht onderzoek dat voortkomt uit een ongericht onderzoek. Ook spreekt art. 126gg Sv over verzamelingen van personen<sup>22</sup>. In het kader van een verkennend onderzoek dient deze groep zo nauwkeurig mogelijk te worden beschreven, daarmee een aanwijzing vormende dat sprake is van gericht dataminingonderzoek. Daarnaast kan in het kader van een gericht dataminingonderzoek zeer wel gebruik worden gemaakt van een tijdelijk politieregister (als datawarehouse). Met het oog hierop ligt het verrichten van ongericht dataminingonderzoek met betrekking tot een tijdelijk politieregister niet voor de hand; dat zou immers betekenen dat voor de uitvoering van een gericht dataminingonderzoek (in het kader waarvan het tijdelijk politieregister kan worden aangelegd) gebruik wordt gemaakt van een ongericht dataminingonderzoek.

---

18. *Kamerstukken II*, 1997/198, 25 398, nr. 6, p. 3-4.

19. In dit onderzoek blijkt een tijdelijk register in de regel te worden aangelegd in het kader van een gericht dataminingonderzoek.

20. *Kamerstukken II*, 1996/197, 25 403, nr. 3, p. 49.

21. Zie model IV.

22. *Kamerstukken II*, 1996/197, 25 403, nr. 3, p. 8.

**Inbreuk privacy**

Gegevensvergaring in het kader van een ongericht dataminingonderzoek is slechts mogelijk voor zover daarmee geen ontoelaatbare inbreuk op de privacy wordt gemaakt. In beginsel is nog geen sprake van een verdenking van een strafbaar feit, noch een vermoeden van het beramen of plegen van ernstige misdrijven (in georganiseerd verband). In het kader van een tijdelijk politieregister staat de verwerking van externe gegevens centraal, waarbij het in beginsel ook gaat om inbreukmakende gegevens<sup>23</sup>. Het doel van een tijdelijk politieregister is grotendeels bepalend voor de mate van de inbreuk op de privacy. Dit verklaart het beperkte verstrekkingenregime dat op een tijdelijk register van toepassing is. Dit gaat niet goed samen met de aard van een ongericht dataminingonderzoek waarbij in beginsel juist geen (ontoelaatbare) inbreuken op de persoonlijke levenssfeer plaatsvinden. Een inbreuk op de persoonlijke levenssfeer wordt minder bezwaarlijk naarmate het proces van informatiegaring vordert. Een ongericht dataminingonderzoek betreft vooral het eerste stadium van dit proces, dat ziet op het opbouwen en in stand houden van een zekere informatiepositie. Bij een onderzoek met betrekking tot een tijdelijk politieregister gaat het veeleer om een verkennend onderzoek dan om een opsporingsonderzoek en is een gericht dataminingonderzoek dan ook de meest logische keuze.

**Tijdelijk of permanent karakter**

Een ongericht dataminingonderzoek is in beginsel permanent van aard. De behoefte waarin het dataminingonderzoek voorziet, de verbetering van de algemene informatiepositie, zal steeds aanwezig zijn. Dit gaat niet samen met het temporele karakter van een tijdelijk politieregister. Een dataminingonderzoek met betrekking tot een tijdelijk politieregister ziet op een specifieke verbetering van de informatiepositie. Wanneer het doel van het tijdelijk register is bereikt, vervalt ook het bestaansrecht van dat register. Aangezien het doel van het dataminingonderzoek overeenkomt met dat van het tijdelijk politieregister is het dataminingonderzoek, evenals het tijdelijk politieregister, tijdelijk van aard.

**Gebruik van externe gegevens**

Een ongericht dataminingonderzoek kenmerkt zich in beginsel door een terughoudende opstelling wanneer het gaat om het (actief) verwerken van (externe) gegevens. Bij het streven naar een algemene verbetering van de informatiepositie van een politieregister bestaan over het algemeen onvoldoende bezwaren om gerichte politieke activiteiten te rechtvaardigen. De nadruk ligt op de gegevens die al in het register aanwezig zijn. Bij een tijdelijk politieregister staat het actief verwerken van (externe) gegevens juist voorop. Voor elk afzonderlijk onderzoek wordt – indien het zich daartoe leent – in beginsel een nieuw tijdelijk register in het leven geroepen. De nadruk ligt in eerste instantie niet op

---

23. Nu gericht wordt gezocht gaat het in beginsel steeds om persoonsgegevens.

gegevens die al in het register aanwezig zijn, aangezien het gaat om een nieuw onderzoek waarbij vaak in het geheel nog geen gegevens voorhanden zijn. Pas gaandeweg het onderzoek zal het zwaartepunt zich verleggen. Wanneer voldoende informatie is verzameld, zal aan de hand daarvan worden getracht het doel van het tijdelijk register te bereiken. Op dat moment concentreert het onderzoek zich meer op de tot dan toe verzamelde gegevens en is de noodzaak om nieuwe gegevens te verzamelen minder prominent aanwezig.

### Resumerend

Gelet op het voorgaande is het in beginsel niet mogelijk om met behulp van een ongericht dataminingonderzoek een verbetering van de informatiepositie van een tijdelijk politieregister na te streven. Het karakter van een tijdelijk politieregister is op een aantal essentiële punten onverenigbaar met de eigenschappen van de ongerichte dataminingsvariant:

- een tijdelijk politieregister heeft steeds een unieke en gerichte doelstelling;
- het register kent een beperkt verstrekkingsregime;
- het register is tijdelijk van aard;
- het betreffende dataminingonderzoek kan ingrijpend van aard zijn;
- in eerste instantie staat de verwerking van externe gegevens voorop.

### 9.4 Onggericht dataminingonderzoek en het voorlopige politieregister

In deze sectie wordt de mogelijkheid onderzocht om met behulp van een ongericht dataminingonderzoek een verbetering van de informatiepositie van een voorlopig politieregister na te streven. Ook hier vindt een toetsing plaats van het voorlopige politieregister aan de kenmerken van deze dataminingsvariant.

#### Doel

Een voorlopig politieregister wordt aangelegd ten dienste van een deelgebied van de justitiële politietaak, te weten de voorkoming en opsporing van de misdrijven als omschreven in art. 1 sub *k* WPolr<sup>24</sup>. Als voorportaal van het register zware criminaliteit heeft een voorlopig politieregister een beperkte doelstelling. Het bevat informatie over individuele personen ten aanzien van wie gegevens zijn verkregen die niet uitsluiten dat deze personen, indien aanvullende gegevens zouden binnenkomen, op basis van de samenhang tussen de oorspronkelijke en de aanvullende gegevens geregistreerd kunnen worden in een

---

24. *Kamerstukken II*, 1997/98, 25 398, nr. 6, p. 20, *Kamerstukken II*, 1996/97, 25 398, nr. 3, p. 14, *Kamerstukken I*, 1998/99, 25 398, nr. 63a, p. 2-3. Bij de omschrijving van het begrip 'voorlopig politieregister' wordt de uitvoering van de politietaak gerelateerd aan de misdrijven behorend tot de zware criminaliteit. Het register wordt bijgehouden met het oog op de uitvoering van de politietaak, voorzover het betreft de vaststelling of de geregistreerde, in samenhang met andere, gegevens kunnen worden opgenomen in een register zware criminaliteit.

register zware criminaliteit<sup>25</sup>. Opname van persoonsgegevens in een voorlopig register vindt alleen plaats met het oog op dit doel<sup>26</sup>. De registratie van gegevens omtrent personen, ten aanzien van wie (nog) geen redelijk vermoeden van betrokkenheid bij zware criminaliteit bestaat, kan plaatsvinden in een tijdelijk of voorlopige politieregister<sup>27</sup>. Bij een voorlopig politieregister gaat het, net als bij het register-MOT, om meer dan één geval. Hoewel het doel van een voorlopig register gericht is, kan een dataminingonderzoek ter verbetering van de informatiepositie van dit register ongericht van aard zijn. Het dataminingonderzoek ziet, evenals het voorlopig register zelf, niet op de politietaak in een bepaald geval (zoals bij een gericht dataminingonderzoek), maar op een verbetering van de informatiepositie van het voorlopige politieregister als geheel.

### Inbreuk privacy

De gegevens in een voorlopig politieregister<sup>28</sup> bestaan voornamelijk uit tips en meldingen die nog niet door andere bronnen worden bevestigd. Niet alle tips kunnen worden vastgelegd. Er moet een relatie bestaan met het opslagcriterium voor het register zware criminaliteit<sup>29</sup>. Met een voorlopig register is ervoor gezorgd dat deze gegevens op een verantwoorde wijze kunnen worden opgeslagen. Uit een voorlopig politieregister worden geen gegevens voor operationeel gebruik verstrekt, aangezien deze nog niet voldoen aan het criterium voor registratie in een register zware criminaliteit. Het gaat om gegevens waaraan minder eisen worden gesteld voor wat betreft de aard, de betrouwbaarheid en de verifieerbaarheid, zoals tips van onbekende bronnen of van bronnen waarbij vraagtekens inzake de betrouwbaarheid kunnen worden geplaatst. Er worden slechts gegevens (die benodigd zijn ter identificatie) verstrekt met het oog op het specifieke doel waarvoor het voorlopig register is aangelegd ter verrijking van al opgeslagen informatie<sup>30</sup>. Ter verkrijging van aanvullende gegevens is het niet noodzakelijk om op ruimere schaal eigen gegevens te verstrekken<sup>31</sup>. Een verstrekking buiten het doel van een voorlopig register om is mogelijk ten behoeve van opname in een ander bijzonder politieregister of ten behoeve van het register-MOT.

Bij een voorlopig politieregister is sprake van een noodzaak tot registratie van gegevens die mogelijk betrekking hebben op onschuldige burgers. Het gaat om informatie die nog niet voldoet aan het opslagcriterium voor het register zware criminaliteit, maar achteraf

---

25. *Kamerstukken II*, 1996/97, 25 398, nr. 3, p. 18, *Kamerstukken II*, 1997/98, 25 398, nr. 6, p. 3 en *Kamerstukken I*, 1998/99, 25 398, nr. 63b, p. 2.

26. Art. 13b lid 1 WPolr.

27. *Kamerstukken II*, 1997/98, 25 398, nr. 6, p. 9.

28. In de *Kamerstukken* wordt nog gesproken over het vaststellingsregister in plaats van het voorlopige politieregister, zoals het vaststellingsregister thans heet.

29. *Handelingen II*, 1998/99, nr. 17, p. 1017-1032.

30. *Kamerstukken II*, 1997/98, 25 398, nr. 6, p. 3.

31. *Kamerstukken II*, 1996/97, 25 398, nr. 3, p. 19.

gezien wel belangwekkend kan zijn en mogelijk zelfs het enige aanknopingspunt vormt voor de opsporing van zware criminaliteit. Het voorlopig register biedt de mogelijkheid om aan de hand van een passieve registratie van tips, in afwachting van aanvullende informatie, binnen een bepaalde termijn te beoordelen of de verkregen informatie voldoende is om de betrokkene in het register zware criminaliteit te kunnen opnemen<sup>32</sup>. Het passieve karakter van de registratie lijkt het gebruik van een gericht dataminingonderzoek uit te sluiten. Een verwerking van gegevens in een voorlopig register, waarbij wordt vastgesteld of de gegevens in aanmerking komen voor opname in een register zware criminaliteit, wordt in de MvT<sup>33</sup> aangeduid als misdaadanalyse. Het betreft hier in beginsel de klassieke misdaadanalyse, waarbij sprake dient te zijn van een niet-ingrijpend middel. Met het oog hierop ligt het gebruik van een ongericht dataminingonderzoek voor de hand. Terwijl het in het kader van de bestrijding van de zware criminaliteit mogelijk lijkt een misdaadanalyse te doen waarbij een vergelijking met andere bijzondere politieregisters plaatsvindt, is iedere andere verwerking waarbij gegevens in een voorlopig politieregister (omtrent onverdachte personen) worden gekoppeld in beginsel uitgesloten<sup>34</sup>.

#### Tijdelijk of permanent karakter

De duur van de opslag van gegevens in een voorlopig politieregister is naar tijd beperkt. Het betreft hier de wettelijk vastgelegde termijn voor de registratie van gegevens in een voorlopig politieregister, waardoor de samenstelling van de gegevens in een voorlopig politieregister voortdurend aan verandering onderhevig is<sup>35</sup>. Het voorlopig register zelf is, evenals een dataminingonderzoek met betrekking tot dit politieregister, permanent van aard<sup>36</sup>. Nu de behoefte waarin dit bijzondere politieregister voorziet voortdurend

32. *Handelingen II*, 1998/199, nr. 17, p. 17-1018.

33. *Kamerstukken II*, 1996/197, 25 398, nr. 3, p. 19-20.

34. *Kamerstukken II*, 1997/198, 25 880, nrs. 1-2, p. 83.

35. De procedure inzake de opslag van gegevens in het voorlopige register schrijft voor, dat tips en meldingen voor een termijn van zes maanden in dit register kunnen worden opgeslagen. Wanneer deze niet worden aangevuld met andere gegevens dient onherroepelijk verwijdering en vernietiging te volgen. In het geval binnen de termijn van zes maanden relevante nadere informatie in aanvulling op de tip binnenkomt, vindt in beginsel 'promotie' naar het register zware criminaliteit plaats. Wanneer de verkregen gegevens echter niet van dien aard blijken te zijn dat kan worden gesproken van een redelijk vermoeden van betrokkenheid bij het plegen of beramen van misdrijven waarvoor het register zware criminaliteit kan worden aangelegd, volgt eveneens verwijdering en vernietiging van de gegevens. De noodzaak tot registratie kan ook eerder dan na zes maanden komen te vervallen. Dit is bijvoorbeeld het geval wanneer er duidelijke aanwijzingen zijn dat de gegeven tip zijn achtergrond vindt in gevoelens van wraak en bovendien in strijd is met de waarheid. Na zes maanden kan met zekerheid worden gesteld dat alle oorspronkelijke gegevens zijn verdwenen en vervangen door nieuwe. Dit resulteert in een complete vernieuwing van het register, hetgeen een verwerking in het kader van een voorlopig politieregister een zeker tijdelijk karakter geeft.

36. *Kamerstukken II*, 1997/198, 25 398, nr. 6, p. 6.

aanwezig is, vormt de levensduur van een voorlopig register geen obstakel voor het gebruik van een ongericht dataminingonderzoek.

### **Gebruik van externe gegevens**

De opslag van gegevens in een voorlopig politieregister vindt plaats vanuit de verwachting, dat naar aanleiding van toekomstige gegevens een basis ontstaat om die gegevens over te hevelen naar een register zware criminaliteit. Hierdoor speelt de verwerking van externe gegevens een belangrijke rol, waarbij terughoudend te werk moet worden gegaan. Vanwege de onbetrouwbare aard van de gegevens in een voorlopig register is er geen plaats voor gericht politieel politieoptreden. Dit betekent dat het niet is toegestaan om actief informatie te verzamelen die (nog) niet in enig politieregister aanwezig is. Eventuele gegevensvergaring door middel van niet-ingrijpende middelen is slechts mogelijk voor zover daarmee geen ontoelaatbare inbreuk op de privacy wordt gemaakt. In dit geval is de term ‘vergaring’ wellicht misleidend, nu de mogelijkheden daartoe beperkt lijken te zijn tot het openhouden van ogen en oren. Andere vormen van gegevensvergaring zullen al snel een gericht karakter kunnen hebben, hetgeen moeilijk samengaat met de aard van de gegevens in een voorlopig politieregister.

### **Resumerend**

Gelet op het voorgaande kan, ter verbetering van de informatiepositie van een voorlopig politieregister, gebruik worden gemaakt van een ongericht dataminingonderzoek. Deze dataminingsvariant ziet op een verbetering van de informatiepositie door middel van niet-ingrijpende middelen en concentreert zich in eerste instantie op de gegevens die al in het voorlopige politieregister aanwezig zijn.

## **9.5 Vier verschillende onderzoeksmogelijkheden**

Hierna worden de mogelijkheden onderzocht om de informatiepositie van een voorlopig register te verbeteren met behulp van ongericht dataminingonderzoek. Daarbij gaat het achtereenvolgens om dataminingonderzoek waarbij:

- geen gebruik wordt gemaakt van externe gegevens;
- gebruik wordt gemaakt van externe gegevens die niet afkomstig zijn uit een politieregister;
- gebruik wordt gemaakt van externe gegevens afkomstig uit een gewoon politieregister;
- gebruik wordt gemaakt van externe gegevens afkomstig uit een bijzonder politieregister.

### *9.5.1 Geen gebruik van externe gegevens*

Met betrekking tot een voorlopig politieregister kan in theorie ongericht dataminingonderzoek worden verricht zonder daarbij gebruik te maken van externe gegevens. Dit is bijvoorbeeld van belang wanneer er verschillende tips binnenkomen die betrekking hebben op één en dezelfde persoon. Door de gegevens in een voorlopig register onderling te

vergelijken kan een dergelijke match worden aangetoond, die aanleiding kan zijn om de betreffende gegevens naar een register zware criminaliteit over te hevelen. In de praktijk lijkt deze situatie zich niet snel voor te zullen doen, nu een zodanige vergelijking al kan plaatsvinden wanneer de ‘aanvullende’ gegevens in het BPS worden opgeslagen. Het systeem van de bijzondere politieregisters laat de mogelijkheid open van een kortstondige registratie van persoonsgegevens naar aanleiding van tips of meldingen in het BPS<sup>37</sup>. Deze registratie gaat in beginsel vooraf aan de opslag van het desbetreffende gegeven in een bijzonder politieregister. Het ligt daarom voor de hand dat van een eventuele match al blijkt wanneer wordt getoetst aan het BPS en niet op een later tijdstip binnen het voorlopige politieregister (na een verstrekking uit het BPS).

#### **De politietaak, het doelbindingsbeginsel en de uitvoering**

Bij een ongericht dataminingonderzoek met betrekking tot een bijzonder politieregister dienen wederom de algemene voorwaarden die daarvoor gelden in acht te worden genomen<sup>38</sup>. Zo dient het onderzoek noodzakelijk te zijn voor een goede uitvoering van de politietaak, dient rekening te worden gehouden met het doelbindingsbeginsel en is het wenselijk dat het dataminingonderzoek uitgevoerd wordt door, dan wel onder het gezag van, de beheerder van het voorlopige politieregister. Voor deze vorm van ongericht dataminingonderzoek gelden geen aanvullende voorwaarden.

#### *9.5.2 Het gebruik van niet uit een politieregister afkomstige gegevens*

Op grond van art. 2 Politiewet 1993 is een verwerking van gegevens, niet zijnde persoonsgegevens, mogelijk indien dat noodzakelijk is voor het voorlopige politieregister. Het noodzakelijkheids criterium en het doelbindingsbeginsel beperken de verwerking van externe persoonsgegevens. In beginsel is een zodanige verwerking alleen noodzakelijk bij de bestrijding van misdrijven. Omdat een voorlopig politieregister wordt bijgehouden in het kader van de bestrijding van de zware criminaliteit kunnen in het kader daarvan dus persoonsgegevens worden verwerkt. Deze kunnen slechts in een voorlopig register worden vastgelegd met het oog op het doel van dat register. Het gebruik van externe gegevens kan verder worden beperkt door de aard van het ongericht dataminingonderzoek, de koppelingsregeling en de aard van de externe gegevens.

##### *9.5.2.1 De aard van ongericht dataminingonderzoek*

Wanneer gegevens worden vergeleken van en kennis wordt vergaard over personen ten aanzien waarvan geen feiten of omstandigheden bekend zijn dat zij zich bezig houden met strafbare feiten, is er sprake van een ingrijpende bevoegdheid<sup>39</sup>. Of het gebruik van

---

37. *Kamerstukken II*, 1997/198, 25 398, nr. 6, p. 7.

38. Zie hoofdstuk 7.

39. *Kamerstukken II*, 1997/198, 25 880, nrs. 1-2, p. 83.

externe gegevens in het kader van een ongericht dataminingonderzoek met betrekking tot een voorlopig politieregister tot een ontoelaatbare inbreuk op de privacy leidt hangt onder meer af van de vraag, of die verwerking op een wettelijke grondslag berust. Burgers zijn gevrijwaard van politieke activiteit indien hun persoon geen aanleiding geeft tot politieke bemoeienis. Dit betekent dat er geen sprake mag zijn van activiteiten die gericht zijn op de strafrechtelijke handhaving van de rechtsorde en die verricht worden door de politie. Indien de betrokkene daartoe geen aanleiding geeft, kunnen noch zwaardere opsporingsbevoegdheden, noch lichtere, waarvoor de grondslag in de politietoelatingen ligt, worden toegepast<sup>40</sup>. In bepaalde situaties kan er reden zijn om ook over onverdachte burgers bepaalde aspecten van hun gedrag te volgen om vast te stellen of zij zich niet schuldig maken (of hebben gemaakt) aan strafbare feiten. Dit volgen van het gedrag van burgers is veeleer een vorm van toezicht, aangezien er nog geen sprake is van enig strafbaar feit. De desbetreffende bestanden zijn daarom afgescheiden van de overige politieregisters, zoals bij een voorlopig politieregister het geval is<sup>41</sup>. In een voorlopig register kan informatie worden vastgelegd die mogelijk betrekking heeft op onschuldige burgers en nog niet voldoet aan het opslagcriterium voor het register zware criminaliteit. Hoewel het kan gaan om onverdachte personen bestaan er, al dan niet buiten hun toedoen om, bezwaren tegen hen op grond waarvan een registratie in een voorlopig politieregister plaatsvindt. Nu het bezwaren betreft die zijn gerelateerd aan de bestrijding van de zware criminaliteit zal het overheidsbelang bij de opsporing, dan wel de voorkoming daarvan, zwaarder wegen dan het belang dat een geregistreerde heeft bij de waarborging van zijn privacy. Een inbreuk is dan onder bepaalde voorwaarden toegestaan. In de kamerstukken<sup>42</sup> wordt hierover opgemerkt:

*'Het is immers zeer wel mogelijk dat personen – naar eerst achteraf kan worden vastgesteld – volstrekt ten onrechte in dit bestand zijn opgenomen, bijvoorbeeld omdat anonieme tips door vijandig gezinde medeburgers zijn binnengekomen. Deze mogen geen basis vormen voor een gericht politie-optreden buiten de sfeer van misdaadanalyse. Wordt een tip dus niet later door andere tips bevestigd, dan dient verwijdering plaats te vinden en dient ook zeker te zijn dat, indien die tip verstrekt is aan een vaststellingsregister<sup>43</sup> van een andere politieregio, verwijdering aldaar eveneens plaatsvindt. Het ligt gelet op artikel 7, tweede lid, van de wet in de rede dat bij de geautomatiseerde verwerking van de gegevens zodanige programmatuur wordt gebruikt dat automatisch na verloop van de termijn de gegevens worden gewist wanneer deze niet op enigerlei wijze tijdens de duur van de opslag worden bevestigd.'*

---

40. Kamerstukken II, 1997/98, 25 403, nr. 7, p. 18.

41. Kamerstukken II, 1997/98, 25 880, nrs. 1-2, p. 84.

42. Kamerstukken II, 1996/97, 25 398, nr. 3, p. 19-20.

43. De voorlopige politieregisters.

Omdat de gegevens in een voorlopig politieregister in eerste instantie betrekking hebben op onverdachte personen, dient een verwerking op een wettelijke grondslag te berusten. Met art. 13*b* WPolr wordt slechts summier voorzien in de verwerking van de gegevens in een voorlopig register. Het artikel biedt vooral een bevoegdheid tot een passieve registratie van tips<sup>44</sup>. Omdat de gegevens in een voorlopig politieregister nog niet voldoen aan het criterium voor registratie in een register zware criminaliteit, dient een verwerking ervan beperkt te blijven tot misdaadanalyse. In dat geval betreft het een niet-ingrijpend middel, waarbij men in beginsel is beperkt tot het gebruik van gegevens die al bij de opsporingsinstanties aanwezig zijn. Uit de MvT<sup>45</sup> bij de bijzondere politieregisters blijkt dat gegevens in een voorlopig politieregister kunnen worden gebruikt in een misdaadanalyse, opdat kan worden vastgesteld of deze in samenhang met andere gegevens als zelfstandig subject in het register zware criminaliteit kunnen worden opgenomen. In het kader hiervan kunnen gegevens in een voorlopig politieregister worden vergeleken met gegevens uit andere bijzondere politieregisters.

Het is zeer de vraag of ook een vergelijking kan plaatsvinden met andere externe gegevens. Een zodanige koppeling kan in beginsel niet meer worden aangemerkt als een niet-ingrijpend middel. Het passieve karakter van een voorlopig politieregister beperkt het gebruik van externe gegevens die afkomstig zijn van buiten de politieke sfeer. Over het gebruik van het voorlopig register wordt gesteld dat, indien een tip later niet door andere tips wordt bevestigd, verwijdering dient plaats te vinden. Met het oog hierop lijkt een overheveling naar een register zware criminaliteit (en daarmee de verwerking van de gegevens in een voorlopig politieregister), slechts mogelijk naar aanleiding van een andere tip. Dit zou enige actieve inbreng van opsporingsdiensten in deze grotendeels uitsluiten. Als regel kan worden aangehouden dat externe gegevens in beginsel onafhankelijk van het voorlopige politieregister dienen te worden verkregen. Dit betekent dat zij niet het resultaat mogen vormen van een gericht zoeken met (de gegevens in) het voorlopige politieregister als uitgangspunt waarbij gebruik wordt gemaakt van opsporingsbevoegdheden. Bij het gebruik van externe gegevens zal het vooral gaan om eigen kennis of informatie die wordt verkregen door het openhouden van ogen en oren (waarbij geen ontoelaatbare inbreuk op de persoonlijke levenssfeer mag worden gemaakt), andere tips en meldingen en een eventuele vergelijking met andere bijzondere politieregisters.

#### *9.5.2.2 Koppeling*

Bij een verwerking van externe gegevens is niet steeds sprake van een koppeling, aangezien de externe gegevens waar het hier in beginsel om kan (en mag) gaan vaak niet tot een zelfstandige gegevensverzameling zullen behoren. Koppeling is alleen mogelijk met een ander politieregister of met een persoonsregistratie van het Rijk, provincies, gemeenten en andere

---

44. *Handelingen II*, 1998/99, nr. 17, p. 1017-1018.

45. *Kamerstukken II*, 1996/97, 25 398, nr. 3, p. 19-20.

openbare lichamen met inbegrip van de daaronder ressorterende diensten, instellingen en bedrijven<sup>46</sup>. Een koppeling van een voorlopig politieregister met (een) externe gegevens(verzameling) leidt in beginsel tot een registratie van die externe gegevens in een voorlopig politieregister. Op grond van art. 4 lid 2 WPolr dient een zodanige registratie van externe (persoons)gegevens noodzakelijk te zijn voor het doel van het voorlopige politieregister. Bovendien dient een koppeling noodzakelijk te zijn voor de politietaak. Hoewel de verwerking plaatsvindt in het kader van de bestrijding van de zware criminaliteit is het de vraag, in hoeverre sprake is van een noodzaak om bepaalde externe gegevens te verwerken. Op grond van art. 6 lid 2 WPolr dient het modelreglement van het voorlopige politieregister in een mogelijkheid tot koppeling te voorzien. Een koppeling is op grond van art. 14 van dit modelreglement mogelijk wanneer deze noodzakelijk is voor het doel van het voorlopig register<sup>47</sup>. Nu deze koppeling in beginsel plaatsvindt in het kader van een misdaadanalyse<sup>48</sup> behoeft daarvan geen proces-verbaal te worden opgemaakt<sup>49</sup>.

#### 9.5.2.3 *Vrijwillige verstrekking*

Aangezien de wetgever in het kader van het voorlopige register meermalen spreekt over ‘tips’ of ‘gegevens die vrijwillig worden verstrekt’, is het gebruik van vrijwillig verstrekte gegevens in beginsel mogelijk. Daarbij is het van belang dat niet aan derden om die gegevens wordt verzocht, maar dat de verstrekking vrijwillig en op eigen initiatief door hen plaatsvindt. In de regel kan de beheerder van een voorlopig register deze vrijwillig verstrekte gegevens verwerken, indien hij daarmee niet in strijd handelt met een wettelijke regeling en voldoet aan de voorwaarden die voor een dergelijke verwerking gelden<sup>50</sup>. Verzoeken om informatie aan derden staat op gespannen voet met het uitgangspunt dat een verwerking van persoonsgegevens slechts mogelijk is op grond van een wettelijke regeling<sup>51</sup>. Dit geldt met name wanneer dit verzoek plaatsvindt voor een ander doel dan waarvoor de gegevens zijn vastgelegd.

#### 9.5.2.4 *Het gebruik van gegevens uit openbare registers*

Buiten een verkennend onderzoek, een verdenking of een andere uitvoering van de politietaak in een bepaald geval is het niet mogelijk om ten behoeve van de opsporing gebruik te maken van gegevens uit openbare registers<sup>52</sup>. Naast het feit dat een koppeling

46. Als bedoeld in art. 17, aanhef en onder *a* Wpr.

47. *Stcr.* 12 oktober 2000, nr. 198/p. 17, p. 8. “Koppeling van het register met een ander politieregister of een register als bedoeld in artikel 17, aanhef en onder *a*, van de Wet persoonsregistraties (*Stb.* 1988, 665), kan plaatsvinden voor zover deze koppeling noodzakelijk is voor het doel van het register, en het andere bijzondere politieregisters betreft.”

48. Zie sectie 9.4.2.1.

49. Art. 14 lid 3 Modelreglement voorlopig politieregister.

50. Zo zullen de gegevens dienen te voldoen aan het bepaalde in art. 13*b* lid 1 WPolr.

51. Zie sectie 4.2.

52. *Kamerstukken II*, 1998/99, 26 410, nr. 3.

met niet-politierregisters slechts beperkt is toegestaan, zal de inbreuk die met het gebruik van deze registers gepaard gaat in beginsel onverenigbaar zijn met de aard van een ongericht dataminingonderzoek. Persoonsgegevens mogen slechts worden verwerkt indien dat noodzakelijk is voor de uitvoering van de politietaak. Dit brengt met zich mee dat de politietaak niet kan rechtvaardigen dat in het kader van een ongericht dataminingonderzoek met betrekking tot een voorlopig politieregister over een onbepaalde groep van burgers gegevens worden vergaard voor algemene politieke doeleinden<sup>53</sup>.

### Resumerend

Er kan slechts op beperkte schaal gebruik worden gemaakt van externe gegevens van buiten de politieke sfeer. Een voorlopig politieregister betreft vooral een passieve registratie van gegevens. Met betrekking tot de personen in een voorlopig register bestaan in beginsel nog onvoldoende bezwaren om een actief en gericht zoeken naar aanvullende gegevens te kunnen rechtvaardigen. Bij het gebruik van externe gegevens zal het vooral gaan om tips en andere gegevens die kunnen worden verkregen door middel van niet-ingrijpende middelen.

#### *9.5.3 Het gebruik van gegevens uit een gewoon politieregister*

Indien in het kader van een ongericht dataminingonderzoek met betrekking tot een voorlopig politieregister gebruik wordt gemaakt van gegevens uit een gewoon politieregister zal het in beginsel gaan om gegevens die pas bekend zijn geworden, nadat het dataminingonderzoek een aanvang heeft genomen. Wanneer in één van de (gewone) politieregisters namelijk al belastende informatie<sup>54</sup> over een geregistreerde in een voorlopig politieregister aanwezig zou zijn geweest, dan zou de betreffende persoon waarschijnlijk niet eerst in het voorlopig register, maar direct in het register zware criminaliteit zijn geregistreerd.

##### *9.5.3.1 Beperkingen aan het gebruik van gewone politieregisters*

De 'free flow' van informatie binnen het opsporingsapparaat met betrekking tot de gegevens in gewone politieregisters kan door verschillende factoren worden beperkt. In deze sectie wordt onderzocht in hoeverre die factoren een rol spelen bij het gebruik van gewone politieregisters ten behoeve van een ongericht dataminingonderzoek met betrekking tot een voorlopig politieregister.

---

53. *Kamerstukken II*, 1998/99, 26 410, nr. 3, p. 11.

54. Op grond waarvan overheveling naar het register zware criminaliteit zou kunnen plaatsvinden.

### De doelbinding

Wanneer gegevens uit een gewoon politieregister in het kader van een ongericht dataminingonderzoek worden vastgelegd in een voorlopig politieregister dient dat noodzakelijk te zijn voor het doel van dat voorlopige register. Dit vloeit voort uit art. 4 lid 2 en art. 13*b* lid 1 WPolr, waarmee indirect sprake is van doelbinding. Overigens wordt het doelbindingsbeginsel minder strikt toegepast wanneer de koppeling plaatsvindt in het kader van de opsporing van ernstige delicten<sup>55</sup>. Met betrekking tot de verwerking van de gegevens in een hulpverleningsregister en het register-MOT is voorzien in een directe doelbinding<sup>56</sup>.

*Het hulpverleningsregister en het register-MOT* – Voor het hulpverleningsregister is de doelbinding geregeld in art. 12 lid 1 sub *a* BPolr. Uit dit register mag slechts worden verstrekt voor de doeleinden waarvoor het is aangelegd, tenzij een geregistreerde zelf uitdrukkelijk instemt met het gebruik van zijn of haar gegevens. Het passieve karakter van een ongericht dataminingonderzoek past echter niet bij een actief en gericht politieel optreden dat gepaard gaat met het verkrijgen van deze expliciete instemming. Het gebruik van een hulpverleningsregister lijkt uitgesloten nu het een geheel ander doel dient dan een voorlopig register.

In art. 12 lid 1 sub *b* BPolr wordt voor het register-MOT bepaald dat een verstrekking uit dit register slechts mogelijk is voor het doel waarvoor het is aangelegd. Op deze regel is een uitzondering gemaakt wanneer de verstrekking plaatsvindt ten behoeve van de opname in een register zware criminaliteit of een voorlopig politieregister. Het is de vraag of het op grond hiervan mogelijk is om een koppeling te bewerkstelligen tussen een voorlopig politieregister en het register-MOT. Daartoe dient te worden vastgesteld wat precies moet worden verstaan onder een verstrekking die plaatsvindt ‘ten behoeve van de opname in een register zware criminaliteit of een voorlopig register’. De WPolr noch het BPolr gaan nader in op de aard van deze verstrekking aan een voorlopig politieregister of een register zware criminaliteit. Het is echter onwaarschijnlijk dat op grond van art. 12 lid 1*b* onder 1 BPolr de gegevens in het register-MOT kunnen worden gebruikt ten behoeve van een ongericht dataminingonderzoek met betrekking tot een voorlopig register. De gegevens in het register-MOT hebben namelijk betrekking op onverdachte personen die in beginsel geen enkele aanleiding hebben gegeven voor enige politieke bemoeienis ten aanzien van hun persoon. Volgens de wetgever rechtvaardigt het doel van het register-MOT de verwerking van gegevens over onverdachte personen in het kader van dit register. Dit betekent niet dat het gebruik van de gegevens in het register-MOT ook is (en blijft) gerechtvaardigd, wanneer zij worden gebruikt voor een ander doel dan waarvan sprake is bij een verstrekking aan een voorlopig politieregister.

---

55. *Kamerstukken II*, 1988 /89, 19 589, nr. 11, p. 13-14.

56. Art. 12 BPolr.

*‘Ten behoeve van’ versus ‘ten behoeve van de opname in’* – Art. 12 lid 1b onder 1 BPolr spreekt over een verstrekking *ten behoeve van de opname in* een voorlopig politieregister en niet over een verstrekking *ten behoeve van* een voorlopig politieregister. Het betreft een klein maar essentieel verschil. Een verstrekking uit een register-MOT ten behoeve van de opname in een register zware criminaliteit of een voorlopig register is mogelijk, wanneer wordt voldaan aan de voorwaarden die par. 3a WPolr daaraan stelt. Van deze mogelijkheid is bijvoorbeeld sprake wanneer met betrekking tot bepaalde gegevens in het register-MOT de verwachting bestaat dat zij mettertijd, door het verkrijgen van meer informatie, kunnen worden overgeheveld naar het register zware criminaliteit<sup>57</sup>. De betreffende gegevens kunnen dan worden opgenomen in een voorlopig politieregister op grond van art. 12 lid 1b onder 1 BPolr. Dit geldt ook voor een verstrekking aan een register zware criminaliteit wanneer de gegevens in het register-MOT voldoen aan de voorwaarden die art. 13a WPolr stelt aan een registratie. Doorslaggevend is dat de gegevens als zelfstandig subject in aanmerking komen voor een registratie in één van deze bijzondere politieregisters. Opvallend is dat in art. 12 BPolr niet wordt gesproken over de mogelijkheid tot een verstrekking van gegevens voor opname in een tijdelijk politieregister. Dit kan worden verklaard door het feit dat een tijdelijk politieregister geen permanent karakter heeft. Gegevens in het register-MOT worden niet zozeer verstrekt aan een (bestaand) tijdelijk register, maar kunnen wel aanleiding geven tot de aanleg van een (nieuw) tijdelijk politieregister.

Bij een verstrekking *ten behoeve van* een ander register is het voor een verstrekking niet noodzakelijk dat de verstrekte gegevens als zelfstandig subject voor een registratie in dat register in aanmerking komen. De verstrekking grond ‘ten behoeve van’ pleegt te voorzien in de mogelijkheid om de verstrekte gegevens te verwerken ten behoeve van het register waaraan wordt verstrekt. De primaire reden tot verstrekking is in dat geval niet de opname van de verstrekte gegevens in het andere register. In dat geval kunnen de verstrekte gegevens ook niet als zelfstandig subject worden geraadpleegd door de gebruikers van het register waaraan de verstrekking heeft plaatsgevonden. Om dit in de praktijk te realiseren is het van belang, dat de gegevens in een datawarehouse uitsluitend worden gebruikt voor het doel waarvoor zij in dat datawarehouse zijn geregistreerd, namelijk het dataminingonderzoek. De mogelijkheid om te verstrekken ten behoeve van een ander register kan een wettelijke grondslag vormen voor een verstrekking in het kader van een (on)gericht dataminingonderzoek. Dit is niet het geval wanneer wordt gesproken van een verstrekking *ten behoeve van een opname in* een ander register, nu daarmee slechts een bevoegdheid wordt gecreëerd om gegevens te verstrekken die als zelfstandig subject in aanmerking komen voor registratie in het register waaraan wordt verstrekt.

Gelet op het voorgaande lijkt een verstrekking uit het register-MOT aan een voorlopig politieregister voor een ander doel dan waarvoor de gegevens zijn verzameld alleen

---

57. *Kamerstukken II*, 1997/198, 25 398, nr. 6, p. 9.

gerechtvaardigd, wanneer die gegevens als zelfstandig subject in aanmerking komen voor een registratie in een voorlopig politieregister. Nu art. 12 lid 1*b* onder 1 BPolr niet spreekt over 'een verstrekking ten behoeve van een voorlopig politieregister' zal een verstrekking in alle andere gevallen in strijd zijn met het doelbindingsbeginsel van het register-MOT. Gegevens in het register-MOT, die normaal gesproken geenszins in aanmerking komen voor een registratie in een register zware criminaliteit of een voorlopig politieregister, kunnen ook in dit geval niet in een voorlopig register worden vastgelegd. Voorts zou een verstrekking uit het register-MOT aan het voorlopige politieregister betekenen dat de taak van het Meldpunt deels wordt overgenomen door de beheerder van het voorlopige politieregister. Art. 13*b* lid 2 WPolr voorziet namelijk expliciet in de mogelijkheid om gegevens uit een voorlopig politieregister te verstrekken aan het register-MOT. Deze mogelijkheid stelt het Meldpunt in staat te toetsen of een persoon in beide registers is geregistreerd. Wanneer de beheerder van een voorlopig politieregister door middel van een koppeling van zijn register met het register-MOT deze toets zelf (ook) uitvoert, doorkruist hij daarmee de werkzaamheden van het Meldpunt.

#### **De aard van de politietaak**

De gewone politieregisters staan in beginsel volledig ter beschikking van alle bij de wet aangewezen bevoegde opsporingsambtenaren. Van politieregisters die niet worden aangelegd in het kader van de politietaak met betrekking tot de strafrechtelijke handhaving van de rechtsorde is het gebruik minder vanzelfsprekend, en voor politieregisters die in het geheel niet zijn aangelegd in het kader van de politietaak als omschreven in art. 2 Politiewet 1993 geldt ten slotte dat er geen sprake is van een vrij verkeer van gegevens. Die gegevens kunnen slechts worden gebruikt onder de voorwaarden die gelden voor het gebruik van externe gegevens afkomstig van buiten de politieke sfeer.

*De handhaving van de openbare orde* – Het OOH-register is niet aangelegd in het kader van de politietaak voor zover het de strafrechtelijke handhaving van de rechtsorde betreft. Een verwerking van gegevens die in het kader van een andere politietaak zijn vergaard, wordt beperkt door de doelbinding. De gegevens vallen weliswaar onder de 'free flow' van informatie, maar zijn vastgelegd voor een doel dat sterk afwijkt van dat van een voorlopig politieregister. In het eerste geval gaat het om de handhaving van de openbare orde en in het tweede geval om de bestrijding van de zware criminaliteit. Voor een verwerking van gegevens die zijn vastgelegd in het kader van de handhaving van de openbare orde ten behoeve van een ongericht dataminingonderzoek dient een aantoonbare noodzaak te bestaan. Nu de doelstellingen van beide politieregisters zo sterk uiteenlopen, lijkt de toegevoegde waarde van de gegevens in een OOH-register onvoldoende om een verwerking daarvan ten behoeve van een voorlopig politieregister te kunnen rechtvaardigen.

*De hulpverleningstaak* – Naast de doelbinding staat ook de aard van de politietaak in de weg aan het gebruik van het hulpverleningsregister ten behoeve van een voorlopig politieregister. Op grond van art. 12 lid 1 sub *a* BPoI mogen in beginsel geen gegevens uit dit register worden verstrekt voor een ander doel dan waarvoor het hulpverleningsregister is aangelegd, tenzij met uitdrukkelijke instemming van de geregistreerde. Nu de verstrekking van gegevens in dit geval niet plaatsvindt voor het doel van het hulpverleningsregister en het verkrijgen van uitdrukkelijke toestemming voor het verwerken van de gegevens niet samengaat met de aard van een ongericht dataminingonderzoek, is het gebruik van dit register in beginsel niet mogelijk.

### **Koppeling**

In het geval van een koppeling met een gewoon politieregister gelden aanvullende voorwaarden. Zo dient deze op grond van art. 6 lid 1 WPoI noodzakelijk te zijn voor een goede uitvoering van de politietaak voor zover het de strafrechtelijke handhaving van de rechtsorde betreft. Dit beperkt de mogelijkheid om gebruik te maken van registers die niet in het kader van deze politietaak zijn aangelegd. Voorts is de koppeling slechts toegestaan wanneer en voor zover de reglementen van de betrokken politieregisters in deze mogelijkheid voorzien.

*Modelreglement voorlopig politieregister* – Het modelreglement van een voorlopig politieregister bepaalt, dat een koppeling met een ander register slechts mogelijk is voor zover dit overeenstemt met het stringente verstrekkingenregime dat van toepassing is op het voorlopige register. Ook dient de koppeling noodzakelijk te zijn voor het doel van het voorlopige register. In sectie 8.2.4.2 (onder het kopje *Koppeling*) bleek uit de toelichting op art. 14 van het modelreglement dat wordt uitgegaan van het standpunt, dat een koppeling een verstrekking van gegevens uit het voorlopige politieregister impliceert. Dit is bij een koppeling in het kader van een ongericht dataminingonderzoek met betrekking tot een voorlopig politieregister echter niet het geval, zodat het beperkte verstrekkingenregime van een voorlopig politieregister gewoon gehandhaafd blijft. Een koppeling met een gewoon politieregister is daarom mogelijk, wanneer dat noodzakelijk is voor het doel van het voorlopige politieregister. Die voorwaarde hangt samen met het uitgangspunt dat een koppeling een verstrekking met zich meebrengt. Een koppeling voor een ander doel zou in strijd zijn met de algemene regel, dat uit het register slechts gegevens mogen worden verstrekt ten behoeve van het doel van het register. Deze uitleg zoekt aansluiting op het bepaalde in art. 13b lid 2 WPoI. Hiermee lijkt uitvoering te zijn gegeven aan het standpunt van de wetgever in deze kwestie<sup>58</sup> die stelt, dat een koppeling met andere dan de bijzondere politieregisters niet mogelijk is omdat daaraan voorafgaande niet duidelijk

---

58. *Kamerstukken I*, 1998/99, 25 398, nr. 63b, p. 8.

is dat meer informatie over de geregistreerde personen kan worden verkregen om vast te stellen of deze kunnen worden opgenomen in het register zware criminaliteit.

Omdat bij een ongericht dataminingonderzoek met betrekking tot een voorlopig politieregister in beginsel geen sprake is van een verstrekking uit het voorlopige politieregister is een koppeling met een gewoon politieregister op grond van art. 14 van het modelreglement mogelijk indien dat noodzakelijk is voor het doel van het voorlopige politieregister. Hoewel op grond van art. 5 BPolr van een koppeling proces-verbaal dient te worden opgemaakt, geldt dit niet voor de koppeling van een voorlopig politieregister met een ander register in het kader van een ongericht dataminingonderzoek. Het modelreglement van een voorlopig politieregister bepaalt in art. 14 lid 3 namelijk, dat deze verplichting niet geldt voor een koppeling die plaatsvindt in het kader van een misdaadanalyse. Hierbij zal het gaan om de klassieke misdaadanalyse die sterke overeenkomsten vertoont met het ongericht dataminingonderzoek.

#### **De aard van het ongerichte dataminingonderzoek**

De aard van zowel de gegevens in een voorlopig politieregister als die van een ongericht dataminingonderzoek beperkt de mogelijkheden van verwerking van de gegevens in een voorlopig politieregister. Een voorlopig register biedt de mogelijkheid tot een passieve registratie van gegevens omtrent onverdachte personen. Het is de vraag hoe dit uitgangspunt zich verhoudt tot een actieve koppeling van een voorlopig politieregister met andere politieregisters. In de kamerstukken<sup>59</sup> wordt aangegeven dat de gegevens in een voorlopig politieregister kunnen worden vergeleken met gegevens uit andere bijzondere politieregisters. De mogelijkheid van een vergelijking met gegevens uit gewone politieregisters wordt als zodanig echter niet genoemd. Indien een dergelijke koppeling toch mogelijk en wenselijk wordt geacht, dient de inbreuk die hiermee gepaard gaat tot een minimum beperkt te blijven. Daarbij heeft het de voorkeur om een verwijzindex te gebruiken waarin geen, dan wel zeer beperkte, gegevens uit andere bestanden zijn opgenomen.

#### **Het BPS**

Voor het doel van een voorlopig politieregister lijkt het niet noodzakelijk om gebruik te maken van gewone politieregisters, aangezien deze in beginsel geen informatie bevatten betreffende zware criminaliteit. De registratie (voor langere tijd) van dergelijke gegevens is voorbehouden aan de bijzondere politieregisters. De gewone politieregisters, waarin naar aanleiding van tips of meldingen kortstondig (zachte) gegevens worden opgeslagen vormen hierop een uitzondering. Alle mutaties met mogelijke opsporingsrelevante informatie kunnen nu eenmaal niet meteen worden getoetst aan de criteria voor de bijzondere politieregisters; dergelijke informatie wordt kort na registratie in het BPS vaak operatio-

---

59. *Kamerstukken II, 1996/97, 25 398, nr. 3, p. 19-20.*

neel gecheckt, waarbij wordt nagegaan of er echt iets aan de hand is. Wanneer het gaat om de bestrijding van de zware criminaliteit ligt het voor de hand dat deze analyse wordt uitgevoerd door de CIE (en niet door bijvoorbeeld de beheerder van het BPS). De CIE kan beschikken over bijzondere politieregisters en is mede daarom bij uitstek geëquipeerd om structureel gevoelige gegevens over ernstige criminaliteit te verwerken. Met het oog hierop is voor de CIE een primaire rol weggelegd voor enerzijds het actief inwinnen van gegevens die relevant zijn voor de bestrijding van zware criminaliteit en anderzijds het actief doorsluizen van dergelijke informatie binnen de overige onderdelen van de politie wanneer deze geschikt is voor operationeel gebruik of wanneer daarmee op andere gronden de goede uitvoering van de politietaak is gediend<sup>60</sup>.

Tips waarvan blijkt dat die direct voor registratie in bijzondere politieregisters in aanmerking komen, bijvoorbeeld ten behoeve van het afschermen van de identiteit van de tipgever, worden uiteraard geregistreerd. De tipgever zal in dat geval om afscherming vragen. Die kan niet door de registerbeheerder van het BPS worden geboden, tenzij gebruik wordt gemaakt van een voorziening op grond van het BPolr. In de regel zal betrokkene met zijn tip dan ook worden verwezen naar de registerbeheerder van de bijzondere politieregisters<sup>61</sup>. Voor de (tijdelijke) opslag in een BPS van gegevens die eigenlijk in een bijzonder politieregister thuishoren, bestaan geen juridische belemmeringen. In de MvT<sup>62</sup> wordt gesteld dat het mogelijk is om persoonsgegevens die voldoen aan de opslagcriteria voor het register zware criminaliteit of het voorlopige politieregister kortstondig te registreren in bijvoorbeeld het BPS. Het bestaan van die mogelijkheid betekent niet automatisch dat er sprake is van een dubbele registratie van gegevens. De MvT spreekt over gegevens die *kunnen* worden opgeslagen in de bijzondere politieregisters, en niet over gegevens waarbij dat al daadwerkelijk het geval is.

#### **Koppeling voorlopige politieregister met BPS**

De mogelijkheid om zachte gegevens kortstondig in het BPS te registreren maakt het koppelen van dit register met een voorlopig politieregister interessant. Het BPS kan, als voorportaal van de overige politieregisters, gegevens bevatten die van belang zijn voor een voorlopig politieregister. Het biedt de mogelijkheid nieuw binnengekomen gegevens te registreren om te bepalen of, en zo ja, op welke wijze, die gegevens binnen het politie-apparaat verwerkt dienen te worden. De zachte aard van de gegevens in een BPS zorgt ervoor, dat de doelbinding minder snel in de weg staat aan het gebruik van die gegevens in het kader van een ongericht dataminingonderzoek met betrekking tot een voorlopig politieregister. Nu gegevens in het BPS ook betrekking kunnen hebben op de zware cri-

---

60. *Stert*. 12 oktober 2000, nr. 198, p. 14.

61. *Handelingen II*, 1998/99, nr. 17, p. 1017-1019.

62. *Kamerstukken II*, 1996/97, 25 398, nr. 3, p. 8.

minaliteit kan worden overwogen, dit gewone politieregister te koppelen met een voorlopig politieregister. Voordeel hiervan is een efficiënte verwerking van de gegevens in zowel het BPS als het voorlopige register, waarbij tips die binnenkomen en worden vastgelegd in het BPS eenvoudig en snel in verband kunnen worden gebracht met mogelijk daaraan gerelateerde gegevens in een voorlopig register. Een ongericht dataminingonderzoek met betrekking tot een voorlopig politieregister waarbij wordt gekoppeld met het BPS maakt een zorgvuldige afweging mogelijk ten aanzien van de gegevens in het BPS. In dat geval beschikt degene die de afweging maakt (de beheerder van het voorlopige politieregister) in beginsel over alle benodigde gegevens. Ter rechtvaardiging van een rechtstreekse koppeling dient het voorlopige politieregister in samenhang te worden gezien met het criterium voor de opslag van gegevens in het register zware criminaliteit<sup>63</sup>. Voor een ongericht dataminingonderzoek met betrekking tot een voorlopig politieregister kan worden gesteld, dat het belang dat een voorlopig politieregister dient een koppeling met het BPS rechtvaardigt. Naast zachte gegevens bevat het BPS gegevens die in de gewone politieregisters thuishoren. Hier zal de beperkende werking van de doelbinding een rol spelen. In de praktijk hoeft dit geen probleem te vormen omdat een BPS, hoewel dit één geautomatiseerd systeem is, wordt gevormd door de integratie van verschillende modules<sup>64</sup>. Een bevraging van het BPS ten behoeve van een voorlopig politieregister lijkt wenselijk en mogelijk. Met het oog op de aard van een ongericht dataminingonderzoek en de gegevens in het BPS behoort een volledige koppeling met het BPS in beginsel niet tot de mogelijkheden.

### Resumerend

Als gevolg van het doelbindingsbeginsel kan in het kader van een ongericht dataminingonderzoek met betrekking tot een voorlopig politieregister in beginsel geen gebruik worden gemaakt van gegevens uit een gewoon politieregister: een gewoon politieregister wordt voor een ander doel aangelegd dan een voorlopig register. Er dient steeds te worden nagegaan of een koppeling noodzakelijk is voor een goede uitvoering van de politietoon en voor het doel van het voorlopige politieregister. Voorts dient op grond van de doelbinding te worden getoetst of de gegevens voor het doel van een voorlopig politieregister mogen worden verwerkt. Daarbij wordt niet geredeneerd vanuit het standpunt van het voorlopige politieregister, maar uit dat van het register waaruit aan het voorlopige register wordt verstrekt. In dat geval is bijvoorbeeld een verstrekking uit het register-MOT aan een voorlopig politieregister onwenselijk. Bij een koppeling van een voorlopig politieregister met een gewoon politieregister kan in beginsel niet meer van passief onderzoek worden gesproken. Een koppeling met de gegevens in een voorlopig politieregister als uitgangspunt kan al worden aangemerkt als een actief en gericht zoeken, het-

---

63. *Kamerstukken II*, 1996/197, 25 398, nr. 3, p. 9.

64. Zie ook Schreuders 2001, p. 26.

geen op gespannen voet staat met het gebruik van de ongerichte dataminingsvariant en de aard van de gegevens in een voorlopig register. Wanneer het belang van de bestrijding van de zware criminaliteit als motivatie voor een koppeling ten grondslag ligt dan ligt een vergelijking met een ander bijzonder politieregister eerder voor de hand dan een vergelijking met een gewoon politieregister. Koppeling met het BPS vormt hierop een uitzondering. Vanwege de functie van het BPS als voorportaalregister en de mogelijkheid hierin ook zachte gegevens vast te leggen is het wenselijk, om met dit politieregister te kunnen koppelen. Een zodanige koppeling kan als noodzakelijk voor een voorlopig politieregister worden aangemerkt. In dit verband zij wederom gewezen op de mogelijkheid om verwijzindexen, waarin zachte gegevens kunnen worden vastgelegd, als bijzondere politieregisters aan te merken, dan wel middels een wettelijke regeling in een beperkt verstrekkingenregime voor deze registers te voorzien. Daarmee zou een eventuele koppeling van het BPS met een voorlopig politieregister in overeenstemming worden gebracht met het uitgangspunt van de wetgever op dit punt<sup>65</sup>.

#### *9.5.4 Het gebruik van gegevens uit een bijzonder politieregister*

In het hierna volgende is voor elk van de bijzondere politieregisters onderzocht, of de gegevens in deze registers kunnen worden gebruikt in het kader van een ongericht dataminingonderzoek met betrekking tot een voorlopig politieregister.

##### *9.5.4.1 Het gebruik van een tijdelijk politieregister*

Het feit dat een tijdelijk politieregister voor allerlei doeleinden kan worden aangelegd in combinatie met de mogelijkheid tot de registratie van zachte gegevens, maakt het gebruik van dit bijzondere politieregister interessant. Of dit ook mogelijk is in het kader van een ongericht dataminingonderzoek hangt af van een aantal factoren, welke hieronder worden behandeld.

#### **Doelbinding**

Een registratie van gegevens uit een tijdelijk politieregister in een voorlopig politieregister dient op grond van art. 4 lid 2 WPolr noodzakelijk te zijn voor het doel van het laatstgenoemde register. Omdat een tijdelijk politieregister zeer uiteenlopende doelstellingen kan hebben, dient per geval te worden afgewogen of hiervan sprake is. Daaraan voorafgaande dient te worden onderzocht of een verstrekking uit een tijdelijk register mogelijk is. Uit een tijdelijk politieregister worden slechts gegevens verstrekt voor het doel waarvoor het is aangelegd, tenzij de verstrekking plaatsvindt ten behoeve van de opname in een register zware criminaliteit of een voorlopig register. Met het oog op het doel van een tijdelijk register is een verstrekking mogelijk ter verrijking van de al in het

---

65. Als uiteengezet in sectie 9.5.3.1 onder het kopje *De aard van het ongerichte dataminingonderzoek*.

register opgeslagen gegevens via misdaadanalyse<sup>66</sup>. In het geval van een verstrekking ten behoeve van een ongericht dataminingonderzoek met betrekking tot een voorlopig politieregister kan het dataminingonderzoek mogelijk als misdaadanalyse worden aangemerkt. Deze misdaadanalyse dient in beginsel ter verrijking van het voorlopige politieregister, en niet van het tijdelijk politieregister. Een verstrekking van gegevens uit een tijdelijk politieregister aan een voorlopig register lijkt daarom niet te beantwoorden aan het doel waarvoor het tijdelijk register is aangelegd. Dit geldt vooral wanneer dat doel een ander is dan de bestrijding van de zware criminaliteit.

De mogelijkheid bestaat echter om buiten het doel van een tijdelijk politieregister gegevens te verstrekken aan een voorlopig politieregister, namelijk wanneer gegevens in een tijdelijk politieregister als zelfstandig subject in aanmerking komen voor registratie in een voorlopig register<sup>67</sup>. Deze situatie dient te worden onderscheiden van die waarbij de behoefte om gegevens uit een tijdelijk politieregister te registreren in een voorlopig politieregister niet voortkomt uit de gegevens zelf, maar uit de behoefte om die gegevens te gebruiken voor een ongericht dataminingonderzoek (analyse). De gegevens die op grond van art. 13 lid 2 WPolr kunnen worden verstrekt zijn die, waarvan de opname in een ander bijzonder politieregister overeenkomt met het doel van dat andere register<sup>68</sup>. In alle andere gevallen is een verstrekking in strijd met het beperkte verstrekkingenregime van een tijdelijk politieregister. De gegevens uit een tijdelijk register die niet voor operationeel gebruik zijn bestemd kunnen door een verstrekking aan een register zware criminaliteit daarvoor alsnog beschikbaar komen. Samenvattend is een verstrekking uit een tijdelijk politieregister aan een voorlopig register in beginsel niet mogelijk. Indien de wetgever een koppeling tussen deze registers wenselijk had geacht zou art. 13 lid 2 WPolr spreken van een verstrekking ten behoeve van een *voorlopig politieregister* en niet van een verstrekking ten behoeve van een *opname*.

### Koppeling

Uit sectie 4.3.2.4 blijkt de mogelijkheid van onderlinge koppeling van bijzondere politieregisters. Het is evenwel de vraag, wanneer een koppeling van een tijdelijk politieregister met een voorlopig politieregister noodzakelijk is voor een goede uitvoering van de politietaak zoals art. 6 lid 1 WPolr stelt. Dit zal het geval zijn wanneer het betreffende tijdelijke politieregister is aangelegd in het kader van een onderzoek dat is gelieerd aan de zware criminaliteit en het mogelijk gegevens bevat die van belang zijn voor de informatiepositie van een voorlopig politieregister. Uit de formulering van art. 4 lid 2 BPolr kan worden opgemaakt dat het initiatief tot een koppeling (en daarmee een gegevensverstrekk-

---

66. *Kamerstukken II*, 1996/97, 25 398, nr. 3, p. 4.

67. Zie sectie 9.4.3.1.1.

68. *Kamerstukken II*, 1996/97, 25 398, nr. 3, p. 4.

king) uitgaat van de beheerder van het tijdelijk politieregister, waarbij koppeling noodzakelijk dient te zijn vanuit het oogpunt van het tijdelijk register. Het ongericht dataminingonderzoek in het kader waarvan de koppeling plaatsvindt, heeft hier echter betrekking op het voorlopige politieregister. Ook zal, teneinde een koppeling mogelijk te maken, het begrip ‘noodzakelijk’ in art. 4 lid 2 BPoI erg ruim geïnterpreteerd dienen te worden. Zo is het denkbaar dat een koppeling noodzakelijk wordt geacht omdat daarmee mogelijk indirect informatie wordt verkregen die van nut is voor het onderzoek, waarvoor het tijdelijk register is aangelegd. In het kader van de doelbinding eerder in dit onderzoek<sup>69</sup> bleek een dergelijke situatie echter niet aannemelijk. Een zodanige ruime uitleg van art. 4 lid 2 BPoI draagt voorts niet bij aan het streven naar duidelijke wet- en regelgeving voor de gegevensverwerking in het kader van de opsporing.

#### **Reglement tijdelijk politieregister en modelreglement voorlopige politieregister**

Omdat er sprake is van een koppeling van twee (bijzondere) politieregisters, dienen de reglementen van beide registers in beginsel te voorzien in de mogelijkheid daartoe. Het tijdelijk politieregister vormt hierop (in eerste instantie) een uitzondering<sup>70</sup>, waardoor enkel het reglement van het voorlopige politieregister in een koppeling dient te voorzien. Op grond van art. 14 van het modelreglement van een voorlopig register is een koppeling met een ander bijzonder politieregister mogelijk voor zover dat noodzakelijk is voor het doel van het voorlopige politieregister. Wanneer een tijdelijk politieregister is aangelegd in het kader van de bestrijding van de zware criminaliteit zal in beginsel aan deze voorwaarde (welke overeenkomt met art. 4 lid 2 WPoI) zijn voldaan.

#### **De aard van het ongerichte dataminingonderzoek**

De MvT<sup>71</sup> lijkt ruimte te bieden aan een vergelijking van een voorlopig politieregister met een tijdelijk politieregister. De WPoI en het BPoI lijken momenteel echter een vergelijking van reeds aanwezige gegevens in het kader van een ongericht dataminingonderzoek in de weg te staan. Art. 13 lid 2 WPoI staat een vergelijking van een voorlopig register met gegevens uit een tijdelijk register alleen toe voor zover de gegevens uit een tijdelijk register als zelfstandig subject in aanmerking komen voor een registratie in een voorlopig politieregister. Aangezien een vergelijking met een tijdelijk politieregister niet plaatsvindt voor het doel van dat politieregister, maar voor het doel van het voorlopige register is een vergelijking zoals de wetgever die voorstaat in beginsel in de praktijk niet mogelijk. Wanneer – teneinde bijzondere politieregisters toch onderling te kunnen vergelijken – het verstrekkingenregime zou worden aangepast, blijft terughoudendheid geboden. Uit een tijdelijk politieregister dienen niet méér gegevens te worden verstrekt

---

69. Sectie 9.4.4.1.1.

70. Art. 13 lid 3 WPoI.

71. *Kamerstukken II*, 1996/97, 25 398, nr. 3, p. 19-20.

dan strikt noodzakelijk is voor het doel waarvoor die verstrekking plaatsvindt. Daarbij kan gebruik worden gemaakt van verwijzindexen. In het geval van een koppeling met een tijdelijk politieregister kan wellicht gebruik worden gemaakt van een MRO-bestand waarmee een overzicht wordt verschafte van alle rechercheonderzoeken als bedoeld in de art. 126<sup>gg</sup> en 132<sup>a</sup> Sv en dat tevens bijdraagt aan de informatievoorziening in het kader van de uitvoering van art. 2 Politiewet 1993.

De mogelijkheid om gegevens uit een tijdelijk politieregister op te nemen in een ander bijzonder politieregister mag niet worden uitgelegd als een bevoegdheid, om onbeperkt gegevens uit te wisselen met andere bijzondere politieregisters. Met par. 3<sup>a</sup> WPolr heeft de wetgever beoogd om het gebruik, de opslag en de verstrekking van zachte opsporingsinformatie nader te normeren. Daartoe is in de WPolr precies aangegeven voor welke doeleinden dergelijke gegevens binnen de uitvoering van de politietaak mogen worden geregistreerd en wanneer verstrekking is toegestaan<sup>72</sup>. Een verstrekking van gegevens uit een tijdelijk aan een voorlopig politieregister in het kader van een koppeling kan leiden tot omzeiling van de waarborgen van het tijdelijke politieregister. Dit gebeurt wanneer de verstrekte gegevens niet in aanmerking komen om als zelfstandig subject te worden geregistreerd in een voorlopig register. In tegenstelling tot het tijdelijk politieregister laat het verstrekkingenregime van een voorlopig politieregister namelijk de mogelijkheid open tot verstrekking aan het register-MOT. Terwijl een rechtstreekse verstrekking van gegevens uit een tijdelijk politieregister aan het register-MOT is uitgesloten, wordt dit als gevolg van voornoemde koppeling alsnog mogelijk. Hiermee dient temeer rekening te worden gehouden nu de WPolr met betrekking tot de gegevens die uit een tijdelijk politieregister worden verstrekt niet bepaalt, dat deze niet in enig ander register mogen worden opgeslagen<sup>73</sup>. Dit wekt bevreemding, aangezien in een tijdelijk politieregister ook gegevens kunnen worden opgeslagen over onverdachte personen. Waar voor een verstrekking van dergelijke gegevens uit een register zware criminaliteit en een voorlopig politieregister is bepaald dat deze niet in enig ander register mogen worden opgeslagen, kent het tijdelijk politieregister deze beperking niet. Gezien het feit dat een verstrekking uit een tijdelijk politieregister in beginsel slechts plaatsvindt ter verrijking van dat register, lijkt het noodzakelijk noch wenselijk dat de verstrekte informatie daartoe in een ander politieregister wordt opgeslagen. Met het oog op art. 13<sup>b</sup> lid 1 en art. 13<sup>d</sup> lid 3 WPolr is een zodanige registratie alleen mogelijk, wanneer de verstrekte gegevens als zelfstandig subject in aanmerking komen voor de registratie in het (bijzondere) politieregister waaraan wordt verstrekt.

---

72. *Kamerstukken II*, 1997/98, 25 398, nr. 6, p. 2.

73. Op grond van art. 13<sup>b</sup> lid 3 WPolr is dit wel het geval voor een verstrekking uit een voorlopig politieregister.

### Resumerend

Een vergelijking van een voorlopig politieregister met een ander bijzonder politieregister kan als een niet-ingrijpend middel worden aangemerkt en worden toegepast in het kader van een ongericht dataminingonderzoek. Het modelreglement van een voorlopig politieregister laat de mogelijkheid open om te koppelen met een tijdelijk politieregister. Met het oog op art. 4 lid 2 BPolr lijkt een koppeling van een tijdelijk politieregister alleen mogelijk wanneer het initiatief daartoe uitgaat van de beheerder van het tijdelijk politieregister. Bij een verstrekking in het kader van een ongericht dataminingonderzoek met betrekking tot een voorlopig politieregister ligt het initiatief echter bij de beheerder van het voorlopige politieregister. Voorts staat het beperkte verstrekkingenregime van een tijdelijk politieregister een verstrekking aan een voorlopig register in het kader van een koppeling in de weg.

#### *9.5.5 Het gebruik van een ander voorlopige politieregister*

Omdat de voorlopige politieregisters qua doelstelling, verstrekkingenregime en reglement identiek zijn, bestaan in beginsel geen juridische bezwaren tegen het onderling uitwisselen van gegevens tussen deze politieregisters. Ten behoeve van een verbetering van de informatiepositie van één voorlopig politieregister kan zeer wel gebruik worden gemaakt van gegevens uit andere voorlopige politieregisters. Met het oog op de CIE-regeling lijkt de in sectie 9.1.2.2 besproken NCIE hiervoor de aangewezen instantie.

#### *9.5.6 Het gebruik van het register zware criminaliteit*

In deze sectie wordt onderzocht of gegevens in een register zware criminaliteit in aanmerking komen voor gebruik ten behoeve van de informatiepositie van een voorlopig politieregister. Hierbij wordt wederom het onderscheid gehanteerd dat art. 13a WPolr maakt naar:

- 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 beramen of plegen van misdrijven als bedoeld onder *a*;
- c. personen die in een bepaalde relatie staan tot degenen, bedoeld onder *a* en *b*.

##### *9.5.6.1 De doelbinding*

Het doelbindingsbeginsel wordt in beginsel minder strikt uitgelegd wanneer het gaat om de opsporing van ernstige delicten<sup>74</sup>. Hoewel een register zware criminaliteit is bedoeld voor operationeel gebruik, dient een verwerking van gegevens in dit register zoveel mogelijk in overeenstemming te zijn met het doel waarvoor de gegevens zijn geregistreerd<sup>75</sup>. Aangezien de doelomschrijving van een voorlopig politieregister is gerelateerd

---

74. *Kamerstukken II*, 1988 /89, 19 589, nr. 11, p. 13-14.

75. Zie sectie 7.3.4.3 onder het kopje *Doelbinding*.

aan het opslagcriterium van het register zware criminaliteit<sup>76</sup> is een koppeling tussen deze registers in beginsel in overeenstemming met het doel van een register zware criminaliteit<sup>77</sup>. Voorts resulteert een verstrekking aan een voorlopig politieregister niet in een verwerking die in strijd is met het verstrekkingenregime van een register zware criminaliteit. Aangezien een voorlopig politieregister een strenger verstrekkingenregime kent dan een register zware criminaliteit, blijft de bescherming van de persoonlijke levenssfeer zelfs bij een verstrekking gewaarborgd.

#### **Art. 4 lid 2 WPolr**

Wanneer gegevens uit een register zware criminaliteit in het kader van een koppeling worden vastgelegd in een voorlopig politieregister dient die registratie op grond van art. 4 lid 2 WPolr noodzakelijk te zijn voor het doel van het voorlopige politieregister. Op het eerste gezicht lijkt het voor de vaststelling, of een bepaald persoon in samenhang met andere gegevens in aanmerking komt voor registratie in een register zware criminaliteit, niet direct noodzakelijk om gebruik te maken van gegevens uit datzelfde register zware criminaliteit. Het ligt voor de hand dat een vergelijking met gegevens in een register zware criminaliteit al plaatsvindt wanneer de politie de beschikking krijgt over de gegevens. Daartoe wordt de mogelijkheid geboden door de registratie van de betreffende gegevens in het BPS die vooraf gaat aan de registratie in een voorlopig politieregister. Aangezien naderhand echter ook nieuwe gegevens in een register zware criminaliteit worden opgenomen die mogelijk van belang zijn voor de informatiepositie van een voorlopig politieregister, dient de mogelijkheid van een vergelijking met een register zware criminaliteit niet geheel te worden uitgesloten. Daarbij kan er toch sprake zijn van een noodzaak om in het kader van een ongericht dataminingonderzoek gegevens uit een register zware criminaliteit te registreren in een voorlopig politieregister.

#### **Doelbinding gegevens categorie C**

Met betrekking tot de gegevens in een register zware criminaliteit die behoren tot categorie c) verklaart art. 13a lid 2 WPolr het verstrekkingenregime van een voorlopig politieregister van toepassing. Op grond daarvan (art. 13b lid 2 WPolr) dient de registratie van de verstrekte gegevens uit een register zware criminaliteit in overeenstemming te zijn met het doel van het voorlopige politieregister waaraan wordt verstrekt<sup>78</sup>. Hiervan kan sprake zijn wanneer de gedragingen van een contactpersoon aanleiding geven tot nadere politieke aandacht. Volgens de MvT<sup>79</sup> bij de bijzondere politieregisters kunnen diens gegevens in dat geval worden gebruikt in een misdaadanalyse, opdat kan worden vastgesteld

---

76. *Kamerstukken II, 1996/197, 25 398, nr. 3, p. 18.*

77. Dit geldt in het bijzonder voor de gegevens in een register zware criminaliteit die behoren tot de categorieën *a* en *b*.

78. *Kamerstukken II, 1996/197, 25 398, nr. 3, p. 15.*

79. *Kamerstukken II, 1996/197, 25 398, nr. 3, p. 19.*

of hij in samenhang met andere gegevens als zelfstandig subject in het register zware criminaliteit kan worden opgenomen. Daarmee lijkt te worden bevestigd dat een verstrekking van deze gegevens ten behoeve van een opname in een ander bijzonder politieregister, in dit geval een voorlopig politieregister, op grond van art. 13*b* lid 2 WPolr alleen mogelijk is wanneer die gegevens als zelfstandig subject in dat andere bijzondere politieregister kunnen worden geregistreerd.

#### 9.5.6.2 *Koppeling*

Ook in het geval van een koppeling van een register zware criminaliteit met een voorlopig politieregister dient de daaruit voortvloeiende bijdrage noodzakelijk te zijn voor het doel van het laatstgenoemde register. Voor een koppeling van twee politieregisters is het verder noodzakelijk dat de modelreglementen van beide registers in de mogelijkheid van een koppeling voorzien<sup>80</sup>.

#### **Modelreglementen register zware criminaliteit en voorlopige politieregister**

Het modelreglement van een register zware criminaliteit<sup>81</sup> bepaalt in art. 17 lid 1 sub *a* dat een koppeling mogelijk is voorzover deze noodzakelijk is ter voorkoming en opsporing van misdrijven die een ernstige inbreuk op de rechtsorde opleveren. Nu het daarbij dient te gaan om andere registers zware criminaliteit, voorlopige registers, dan wel gegevensverzamelingen waarvan de doelstelling nauw bij die van het register zware criminaliteit aansluit, is een koppeling met een voorlopig politieregister mogelijk. Het modelreglement van het voorlopige politieregister bepaalt in art. 14 dat een koppeling is toegestaan voor zover noodzakelijk voor het doel van het voorlopige politieregister, en het andere bijzondere politieregisters betreft. Daarmee verschaft ook dit reglement de mogelijkheid van een koppeling.

#### 9.5.6.3 *De aard van het ongerichte dataminingonderzoek*

In de MvT<sup>82</sup> bij de bijzondere politieregisters wordt een vergelijking van een voorlopig politieregister met andere bijzondere politieregisters aangemerkt als misdaadanalyse. Een dergelijke vergelijking in het kader van een ongericht dataminingonderzoek is in beginsel slechts mogelijk voor zover het de gegevens in een register zware criminaliteit betreft die behoren tot de categorieën *a* en *b*<sup>83</sup>. De gegevens in categorie *c* in een register zware criminaliteit hebben betrekking op personen die in een bepaalde relatie staan tot degenen die voldoen aan het opslagcriterium voor dit register. Zij zijn weliswaar geregistreerd in een register zware criminaliteit, maar voldoen noch aan het criterium om als zelfstandig subject in het register zware criminaliteit te worden opgenomen, noch aan het crite-

80. Art. 6 lid 2 WPolr.

81. *Stcr.* 12 oktober 2000, nr. 198, p. 17.

82. *Kamerstukken II*, 1996/97, 25 398, nr. 3, p. 19-20.

83. Zie sectie 9.5.6.

rium om te kunnen worden opgenomen in een voorlopig politieregister. Dit beperkt de mogelijkheid om deze gegevens te verwerken. In beginsel worden zij niet verstrekt (aan een voorlopig politieregister) of verwerkt indien de geregistreerde geen aanleiding geeft tot nader onderzoek. Een verwerking met betrekking tot deze categorie gegevens kan worden aangemerkt als een ingrijpend middel waarvoor een specifieke wettelijke grondslag aanwezig dient te zijn. Daarmee heeft de registratie van deze gegevens in een register zware criminaliteit een nog passiever karakter dan een registratie van gegevens in een voorlopig register. Ook met het oog op de Nota WES<sup>84</sup> lijkt een verwerking van deze gegevens in het kader van een ongericht dataminingonderzoek met betrekking tot een voorlopig register niet mogelijk. De gegevens kunnen weliswaar op bepaalde individuele personen worden bevraagd, maar er mag niet mee worden gekoppeld.

#### *9.5.6.4 Weigering door de beheerder*

De beheerder van een register zware criminaliteit kan een verstrekking (uit elk van de drie categorieën gegevens) weigeren of beperkende voorwaarden stellen aan het gebruik van verstrekte gegevens, indien dat noodzakelijk is voor een goede uitvoering van de politietaak<sup>85</sup>. Deze bevoegdheid dient te worden geplaatst in de context van het verplichte verstrekkingenregime binnen het politieveld. Het uitgangspunt blijft daarom de verplichting tot verstrekking binnen de politie, voor zover dat nodig is voor de uitvoering van de politietaak<sup>86</sup>.

#### **Resumerend**

In het kader van een ongericht dataminingonderzoek ten behoeve van een voorlopig politieregister kan gebruik worden gemaakt van de gegevens in een register zware criminaliteit die behoren tot de categorieën *a* en *b*. Omdat de betrokken registers qua doelstelling nauw verwant zijn, zal een verstrekking niet in strijd komen met het doelbindingsbeginsel. De wetgever geeft aan dat ten behoeve van een voorlopig politieregister een vergelijking kan worden gemaakt met andere bijzondere politieregisters<sup>87</sup>. Deze verwerking is ook in overeenstemming met het uitgangspunt dat een register zware criminaliteit is bestemd voor operationeel gebruik. Ten slotte is een koppeling tussen deze bijzondere politieregisters mogelijk op grond van de betreffende modelreglementen. Dankzij het verstrekkingenregime van een voorlopig politieregister blijft de bescherming van de persoonlijke levenssfeer hierbij voldoende gewaarborgd. Gegevens in een register zware criminaliteit die behoren tot categorie *c* kunnen niet worden gebruikt ten behoeve van het ongerichte dataminingonderzoek. Deze gegevens kennen een stringenter verstrekkingenregime, op grond waarvan een verstrekking aan een voorlopig politieregister in het kader

---

84. *Kamerstukken II*, 1997/98, 25 880, nrs. 1-2, p. 83.

85. Art. 13a lid onder 3 WPolr.

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

87. In het kader van een misdaadanalyse.

van een koppeling enkel mogelijk is wanneer zij als zelfstandig subject voor registratie in dat politieregister in aanmerking komen. De gegevens in categorie *c* hebben betrekking op onverdachte personen. Nu een wettelijke grondslag hiervoor ontbreekt, impliceert een verdere verwerking van deze gegevens in het kader van een ongericht dataminingonderzoek een ontoelaatbare inbreuk op de persoonlijke levenssfeer.

#### *9.5.7 De mogelijkheden ter verbetering van de informatiepositie van een voorlopig politieregister*

Deze sectie behelst een overzicht van de onderzochte mogelijkheden ter verbetering van de informatiepositie van een voorlopig politieregister met behulp van ongericht dataminingonderzoek.

##### **Geen gebruik van externe gegevens**

Wanneer in het kader van een ongericht dataminingonderzoek met betrekking tot een voorlopig politieregister geen gebruik wordt gemaakt van externe gegevens bestaan er – behalve de aan elk dataminingonderzoek inherente algemene voorwaarden – geen nadere beperkingen.

##### **Gebruik van gegevens die niet afkomstig zijn uit een politieregister**

Voor het gebruik van externe gegevens van buiten de politieke sfeer gelden beperkingen. Een gericht en actief speuren naar externe gegevens staat op gespannen voet met het uitgangspunt dat personen, die daartoe geen enkele aanleiding hebben gegeven, niet het onderwerp mogen vormen van politieke bemoeienis. Het verwerken van gegevens over onverdachte personen kan worden aangemerkt als een ingrijpend middel. Daarvoor dient een wettelijke grondslag aanwezig te zijn. Wanneer sprake is van een koppeling gelden nadere beperkingen. Zo is een koppeling slechts mogelijk met een ander politieregister of met een persoonsregistratie van het Rijk, provincies, gemeenten en andere openbare lichamen, met inbegrip van de daaronder ressorterende diensten, instellingen en bedrijven.

##### **Gebruik van gegevens uit een gewoon politieregister**

Wanneer in het kader van een ongericht dataminingonderzoek gebruik wordt gemaakt van gegevens uit een gewoon politieregister is er sprake van koppeling en dient, naast de algemene voorwaarden, rekening te worden gehouden met aanvullende voorwaarden. Zo moeten de reglementen van beide betrokken registers in een koppeling voorzien en gelden specifieke beperkingen op grond van de politietoek en het doelbindingsbeginsel. Waar het gebruik van gegevens uit een OOH-register mogelijk is indien een verstrekking past binnen de bevoegdheid van art. 2 Politiewet 1993, is – mede vanwege het doelbindingsbeginsel – een verstrekking uit het hulpverleningsregister in het geheel niet mogelijk. Ook uit het register-MOT vindt op grond van dit beginsel geen verstrekking plaats

aan een voorlopig register. Het gebruik van de overige gewone politieregisters is slechts mogelijk voor zover dat noodzakelijk is voor het doel van het voorlopige politieregister<sup>88</sup>.

### Gebruik van gegevens uit een bijzonder politieregister

De mogelijkheid om ten behoeve van een verbetering van de informatiepositie van een voorlopig politieregister te koppelen met andere bijzondere politieregisters, wordt beperkt door het verstrekkingenregime van de bijzondere politieregisters. Een zodanige koppeling is alleen mogelijk met andere voorlopige politieregisters en gegevens in een register zware criminaliteit die behoren tot de categorieën *a* en *b*. Uit de voorgaande bevindingen kan onderstaand schema worden afgeleid.

Ongericht dataminingonderzoek	Koppeling	Beperkingen	Gebruik
Geen gebruik externe gegevens	Nee	Algemeen	Onbeperkt
Gebruik externe gegevens*	Ja**	Algemeen/koppeling	Beperkt
Gegevens uit een gewoon politieregister	Ja	Algemeen/koppeling/specifiek	Beperkt
Gegevens uit een bijzonder politieregister	Ja	Algemeen/koppeling/specifiek	Voorlopig politieregister en in beperkte mate het register zware criminaliteit

\* Uitgezonderd de gegevens die in de politieregisters liggen opgeslagen.

\*\* Tenzij de externe gegevens niet tot enig zelfstandig register behoren.

*Schema 13 Toepassing ongericht dataminingonderzoek ter verbetering van de informatiepositie van een voorlopig politieregister*

### 9.6 Ongericht dataminingonderzoek en het register zware criminaliteit

Het register zware criminaliteit is het derde bijzondere politieregister waarvoor wordt onderzocht of met behulp van een ongericht dataminingonderzoek een verbetering van de informatiepositie ervan kan worden nagestreefd. Hiertoe wordt dit register eerst getoetst aan de kenmerken van de ongerichte dataminingsvariant.

88. Art. 4 lid 2 WPolr.

### Doel

Het doel van een register zware criminaliteit is algemener van aard dan dat van een tijdelijk of voorlopig politieregister. Uit art. 1 lid 1 onder *k* WPolr blijkt, dat het register ziet op de bestrijding van de zware criminaliteit in al haar facetten<sup>89</sup>. Om zicht te krijgen op de aard en de omvang van de (georganiseerde) zware criminaliteit is het noodzakelijk dat allerlei, vooral zachte, gegevens over personen worden opgeslagen. Het gedrag van deze personen wordt duurzaam gevolgd door middel van het registreren van onder meer gegevens over levenswijze en contacten. Registratie kan al geschieden bij een vermoeden van betrokkenheid bij het beramen of plegen van misdrijven, waarbij onder meer tips, gedragspatronen, gebruikte auto's en communicatieapparatuur in kaart kunnen worden gebracht<sup>90</sup>. Bij het analyseren van dergelijke hoeveelheden informatie kan een ongericht dataminingonderzoek een belangrijke rol vervullen.

Om te bepalen van welke variant van het dataminingsproces in een bepaald geval sprake is, kan onder meer worden gekeken naar het stadium van het proces van informatiegaring dat van toepassing is. Volgens de wetgever<sup>91</sup> kunnen bepaalde vormen van criminaliteit alleen, dan wel op veel effectievere wijze, worden aangepakt wanneer de politie een informatiepositie van een zeker niveau heeft. Dat is eveneens de ratio achter het register zware criminaliteit. Het opbouwen en in stand houden van een zekere informatiepositie (aangaande personen die in dit register geregistreerd staan) is ook typerend voor de ongerichte dataminingsvariant.

Uit art 13*a* lid 1 WPolr blijkt dat de voorwaarden voor een registratie in een register zware criminaliteit overeenkomen met de kenmerken van het opsporingsonderzoek van art. 132*a* Sv. Uit model IV kan worden afgeleid dat het opsporingsonderzoek in beginsel steeds samengaat met de gerichte dataminingsvariant. Dit doet de vraag rijzen of een dataminingonderzoek met betrekking tot een register zware criminaliteit wellicht kan worden gerekend tot het opsporingsonderzoek en mogelijk gericht van aard kan zijn. Bij een opsporingsonderzoek is sprake van opsporing, terwijl het register zware criminaliteit – en daarmee ook een dataminingonderzoek met betrekking tot dit register – primair ziet op de verbetering van de informatiepositie betreffende de zware criminaliteit. Daarmee is het dataminingonderzoek niet direct gericht op een strafvorderlijke afdoening.

---

89. Opgemerkt zij dat in een register zware criminaliteit gegevens kunnen worden opgeslagen betreffende te plegen misdrijven waarop naar de wettelijke omschrijving een gevangenisstraf van acht jaar of meer is gesteld. Ten aanzien van het beramen van dergelijke misdrijven mogen echter geen bijzondere opsporingsbevoegdheden worden toegepast. Dit betekent dat verschil bestaat tussen de voor opslag in het register zware criminaliteit en de voor de toepassing van bijzondere opsporingsbevoegdheden geldende criteria.

90. *Kamerstukken II*, 1996/97, 25 398, nr. 3, p. 5-7.

91. *Kamerstukken II*, 1996/97, 25 403, nr. 3, p. 8.

Het register ziet niet op een enkele zaak, maar op de bestrijding van de zware criminaliteit als geheel; daarbij wordt overigens niet uitgesloten dat, in het kader van de algemene informatiepositie ter bestrijding van de zware criminaliteit, naar aanleiding van een bepaald opsporingsonderzoek ook gegevens worden opgeslagen in dit register. Ter verbetering van deze informatiepositie kan vervolgens ongericht dataminingonderzoek worden verricht. De verwerking van de gegevens in een register zware criminaliteit betreft dus geen opsporingsonderzoek. Wanneer behoefte bestaat aan het inwinnen van nadere informatie in het kader van een opsporingsonderzoek kan de verwerking die daartoe plaatsvindt wel worden aangemerkt als een gericht dataminingonderzoek. Er kunnen omstandigheden zijn waardoor een meer ingekaderde en op het specifieke geval gerichte registratie te prefereren is. Er kan dan een tijdelijk politieregister worden aangelegd voor de duur van het onderzoek naar dat, naar tijd en ruimte omgrensde, geval. In dat register worden alleen die gegevens opgenomen die van betekenis kunnen zijn voor de oplossing van dat bepaalde ernstige misdrijf. Wanneer het daarmee verband houdende opsporingsonderzoek tot een einde is gekomen, kan het register vervolgens worden beëindigd<sup>92</sup>.

#### **Inbreuk privacy**

Het register zware criminaliteit biedt de (uitputtende) mogelijkheid om zachte gegevens langdurig voor operationeel gebruik vast te leggen. De schaal waarop dit gebeurt impliceert een vergaande inmenging van de overheid in het privéleven van personen op grond van veelal nog niet verifieerbare informatie. De hiermee gepaard gaande inbreuk op de persoonlijke levenssfeer wordt gerechtvaardigd door het feit dat, los van de verdenking van een concreet strafbaar feit, een zodanige registratie noodzakelijk is om de zware criminaliteit effectief te bestrijden. Tegenover de mogelijkheid om de gegevens in dit register operationeel te gebruiken, staat een beperking van de registratiemogelijkheden<sup>93</sup>. Bij het uitvoeren van een ongericht dataminingonderzoek dient daarmee rekening te worden gehouden. Een verwerking die in strijd is met de regels die par. 3a WPolr daaraan stelt leidt tot een ontoelaatbare inbreuk op de persoonlijke levenssfeer.

#### **Tijdelijk of permanent**

Een dataminingonderzoek met betrekking tot een register zware criminaliteit is in beginsel permanent van aard. De behoefte aan een goede informatiepositie bij de bestrijding van de zware criminaliteit zal voortdurend aanwezig zijn.

---

92. *Kamerstukken II*, 1997/98, 25 398, nr. 6, p. 10.

93. Met het wettelijke criterium voor de opslag van gegevens in het register zware criminaliteit is uitvoering gegeven aan het uitgangspunt om ten aanzien van de opslag van persoonsgegevens een criterium te hanteren dat een juiste balans treft tussen enerzijds de bescherming van de persoonlijke levenssfeer en anderzijds de belangen van de opsporing en vervolging van ernstige strafbare feiten. *Kamerstukken II*, 1996/97, 25 398, nr. 3, p. 7-8.

### **Gebruik van externe gegevens**

Het belang van de mogelijkheid van gebruik van externe gegevens op zo groot mogelijke schaal geldt met name voor een register zware criminaliteit. In de toelichting op de CIE-regeling wordt in dat verband opgemerkt dat gegevens kunnen worden opgevraagd uit open bronnen, politieregisters en andere registraties<sup>94</sup>. Hoewel de noodzaak voor terughoudendheid bij het gebruik van externe gegevens, gezien het doel van een register zware criminaliteit, niet prominent aanwezig is, vormt het feit dat een dergelijk register beschikbaar is voor operationeel gebruik aanleiding tot een beperking van de verwerking van externe gegevens.

### **Resumerend**

Een register zware criminaliteit dient te voorzien in een goede informatiepositie. Binnen het proces van informatiegaring gaat het daarbij om het opbouwen en in stand houden van een zekere informatiepositie met gebruik van ongericht dataminingonderzoek. Hierna zal voor elk van de vier toepassingsmogelijkheden van deze dataminingsvariant worden onderzocht, op welke wijze daarmee kan worden bijgedragen aan de informatiepositie van een register zware criminaliteit.

### **9.7 Vier verschillende onderzoeksmogelijkheden**

Een ongericht dataminingonderzoek met betrekking tot een register zware criminaliteit kan op de volgende wijzen worden toegepast:

- er wordt geen gebruik gemaakt van externe gegevens;
- er wordt gebruik gemaakt van externe gegevens die niet afkomstig zijn uit een politieregister;
- er wordt gebruik gemaakt van externe gegevens afkomstig uit een gewoon politieregister;
- er wordt gebruik gemaakt van externe gegevens afkomstig uit een bijzonder politieregister.

In het onderhavige verband zij wederom gewezen op het onderscheid tussen de gegevens in dit register met betrekking tot:

- 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 beramen of plegen van misdrijven als bedoeld onder *a* en;
- c. personen die in een bepaalde relatie staan tot degenen, bedoeld onder *a* en *b*.

---

94. *Stert.* 12 oktober 2000, nr. 198, p. 14.

**Verwerking gegevens in de categorieën a en b**

De gegevens die behoren tot de categorieën *a* en *b* voldoen aan de voorwaarden voor het instellen van een opsporingsonderzoek. Het betreft verdachten van zware criminaliteit en personen ten aanzien van wie een redelijk vermoeden bestaat dat zij betrokken zijn bij het beramen dan wel plegen van zware misdrijven. Deze mate van verdenking, in combinatie met het feit dat het de bestrijding van de zware criminaliteit betreft, rechtvaardigt een verwerking van deze gegevens.

**Verwerking gegevens in categorie c**

Met betrekking tot de gegevens in een register zware criminaliteit die behoren tot categorie *c* is het onduidelijk in hoeverre zij mogen worden verwerkt. De registratie ervan wordt noodzakelijk geacht voor het doel waarvoor een dergelijk register wordt aangelegd<sup>95</sup>. De mogelijkheid om deze gegevens daarin vast te leggen komt vooral voort uit het belang van een verantwoorde opslag. De gegevens hebben betrekking op onverdachte personen die in een bepaalde relatie staan tot personen die voldoen aan het opslagcriterium voor het register zware criminaliteit waarbij het gaat om contacten, getuigen, informanten, aangevers en slachtoffers. Omdat deze personen nog niet voldoen aan het criterium op grond waarvan een gericht politieoptreden gerechtvaardigd is, mogen de gegevens niet operationeel worden gebruikt. Vanwege de aard van de gegevens is het ook onwaarschijnlijk dat zij kunnen worden verwerkt in het kader van een misdaadanalyse. Op grond van wat in de MvT<sup>96</sup> bij de bijzondere politieregisters wordt opgemerkt over de gegevens in een register zware criminaliteit als bedoeld in art. 13*a* lid 1 onder *c* WPolr, lijkt een verwerking pas mogelijk wanneer een geregistreerde zelf aanleiding geeft tot nadere politieke aandacht. Het enkele feit dat men in een register zware criminaliteit is geregistreerd is daarvoor onvoldoende.

Registers waarin gegevens worden bijgehouden over burgers die niet als verdachte of als CIE-subject kunnen worden aangemerkt dienen te worden afgeschermd van andere registers. Het adagium 'if there is no crime, there is no investigation' impliceert, dat koppelingen van registers waarin onverdachte burgers zijn geregistreerd voor de politie niet zijn toegelaten. Dit leidt tot een compartimentering van registers voor zover het gaat om registraties van onverdachte burgers. De wetgeving voorziet niet in bevoegdheden om deze compartimentering door een algemene registervergelijking te doorbreken. Hoewel het mogelijk dient te zijn deze gegevens op bepaalde individuele personen te bevragen, is het ongewenst dat bestanden waarin onverdachte burgers zijn opgenomen worden gekoppeld teneinde strafbare feiten boven water te halen waarvan op voorhand geen enkel vermoeden bestaat. In beginsel zullen deze gegevensbestanden geen onderdeel

---

95. *Kamerstukken II*, 1997/98, 25 398, nr. 6, p. 33-34.

96. *Kamerstukken II*, 1996/97, 25 398, nr. 3, p. 19-20.

mogen uitmaken van een dataminingonderzoek<sup>97</sup>. De wetgever tekent hierbij aan dat de mogelijkheid moet openblijven om in zeer ernstige zaken (bijvoorbeeld de georganiseerde criminaliteit) volgens passende procedures omvangrijke bestanden te bevragen en te koppelen, ook wanneer deze zijn aangelegd voor geheel andere doeleinden. Het is essentieel dat de gegevens die daarbij worden verwerkt goed worden afgeschermd, vervolgens niet voor andere onderzoeken kunnen worden gebruikt en zodra mogelijk worden vernietigd. Vooralsnog lijkt een wettelijke regeling die hierin voorziet te ontbreken. Indien gegevens worden vergeleken van en kennis wordt vergaard over personen ten aanzien van wie geen feiten of omstandigheden bekend zijn dat zij zich bezig houden met strafbare feiten, is er sprake van een ingrijpende bevoegdheid<sup>98</sup>. Art. 13a WPolr biedt in beginsel alleen een mogelijkheid tot registratie. Met art. 13b lid 2 WPolr is een wettelijke regeling getroffen voor de verstrekking van deze categorie gegevens, onder meer aan het Meldpunt ongebruikelijke transacties<sup>99</sup>. Voor een verwerking van de gegevens binnen het register zware criminaliteit zelf lijkt geen plaats. Zowel in het kader van de bestrijding van de zware criminaliteit als de bescherming van de persoonlijke levenssfeer is het van belang dat duidelijkheid bestaat over de verwerking van de gegevens in een register zware criminaliteit als bedoeld in art. 13a lid 1 onder c WPolr. Daarbij gaat het vooral om het doel waarvoor de gegevens worden opgeslagen en de wijze waarop zij vervolgens kunnen worden verwerkt.

#### 9.7.1 *Geen gebruik van externe gegevens*

Het is mogelijk om dataminingonderzoek te doen met betrekking tot een register zware criminaliteit zonder daarbij gebruik te maken van externe gegevens. Met het oog op de enorme omvang en diversiteit van de gegevens die in het kader van de bestrijding van de zware criminaliteit kunnen worden vastgelegd moeten de in het register aanwezige gegevens kunnen worden geanalyseerd. Daardoor kunnen verbanden of complexe netwerken tussen personen onderling worden blootgelegd en in kaart gebracht. De bescherming van de persoonlijke levenssfeer wordt gewaarborgd door het verstrekkingenregime dat van toepassing is op het register zware criminaliteit. De strenge voorwaarden die gelden voor een registratie in dit bijzondere politieregister dienen een al te lichtvaardige registratie en verwerking van persoonsgegevens te voorkomen. Rekening dient te worden gehouden met de algemene voorwaarden die samenhangen met de politietaak en het doelbindings-

---

97. *Kamerstukken II*, 1997/98, 25 880, nrs. 1-2, p. 83.

98. *Kamerstukken II*, 1997/98, 25 880, nrs. 1-2, p. 83.

99. Zie ook art. 13d lid 2 WPolr.

beginsel welke in de voorgaande hoofdstukken zijn besproken. Ook is het wenselijk dat het dataminingonderzoek wordt uitgevoerd door, dan wel onder het gezag van de CIE<sup>100</sup>.

### 9.7.2 *Het gebruik van niet uit een politieregister afkomstige gegevens*

Voor het verkrijgen en behouden van een goede informatiepositie bij de bestrijding van de zware criminaliteit is het essentieel dat gebruik wordt gemaakt van externe gegevens. Daarbij kan het gaan om gegevens uit open bronnen, registraties<sup>101</sup> en de toepassing van niet-ingrijpende middelen zoals het openhouden van ogen en oren<sup>102</sup>. Bij een verwerking van deze externe gegevens dient rekening te worden gehouden met het noodzakelijkheidsvereiste en het doelbindingsbeginsel. Omdat de verwerking van externe gegevens hier plaatsvindt in het kader van de bestrijding van de zware criminaliteit is daarmee in beginsel sprake van een noodzaak om persoonsgegevens te verwerken<sup>103</sup>. Het gebruik van externe gegevens dient voorts in overeenstemming te zijn met het doelbindingsbeginsel<sup>104</sup>. Dit sluit aan op de constatering in de toelichting op de CIE-regeling, dat de CIE verantwoordelijk is voor het actief inwinnen van gegevens (uit welke bron dan ook) die relevant zijn voor de bestrijding van zware criminaliteit. Het actief verwerken van externe gegevens is slechts mogelijk voor zover (duidelijk is dat) die gegevens noodzakelijk zijn voor de bestrijding van de zware criminaliteit. Wanneer het gaat om externe persoonsgegevens die voor een ander doel zijn vergaard, dient een verwerking daarvan in beginsel steeds te berusten op een wettelijke grondslag. Met het oog op de persoonlijke levensfeer kan het gebruik van externe gegevens ook worden beperkt door de aard van het ongericht dataminingonderzoek, de koppelingsregeling en de aard van de te verwerken externe gegevens.

#### 9.7.2.1 *De aard van ongericht dataminingonderzoek*

De verwerking van externe gegevens door de CIE is slechts mogelijk voor zover deze gegevens verband houden met de bestrijding van de zware criminaliteit. In het kader van een ongericht dataminingonderzoek met betrekking tot een register zware criminaliteit kunnen gegevens, zijnde geen persoonsgegevens, in beginsel worden verwerkt ter verbetering van de informatiepositie van het register zware criminaliteit<sup>105</sup>. Dit gebruik van

100. “De Raad van Advies voor de CID heeft geadviseerd het ‘analyseren van criminele inlichtingen’ in het eerste lid aanhef, onder *d*, te wijzigen in ‘het doen analyseren’. Hiermee zou tot uitdrukking worden gebracht dat de analysefunctie ook buiten de CIE kan worden ingevuld. Dit advies is niet overgenomen, aangezien artikel 14 van het modelreglement van het register zware criminaliteit zich niet verzet tegen autorisatie van ambtenaren die niet werkzaam zijn bij de CIE.” (*Stcr.* 12 oktober 2000, nr. 198, p. 14).

101. *Stcr.* 12 oktober 2000, nr. 198, p. 14.

102. *Kamerstukken II*, 1996/97, 25 403, nr. 3, p. 8.

103. Zie sectie 7.3.1 en *Kamerstukken II*, 2001/02, 28 059, nr. 5, p. 10.

104. *Kamerstukken II*, 1996/97, 25 398, nr. 3, p. 7.

105. Art. 1 lid 1 onder *k* WPolr.

externe gegevens door middel van niet-ingrijpende middelen dient te passen binnen de politietaak met betrekking tot de strafrechtelijke handhaving van de rechtsorde<sup>106</sup>.

Voor een verwerking van externe persoonsgegevens gelden nadere beperkingen. Wanneer gegevens worden vergeleken en kennis wordt vergaard over personen ten aanzien van wie geen feiten of omstandigheden bekend zijn dat zij zich bezig houden met strafbare feiten, is er sprake van een ingrijpende bevoegdheid<sup>107</sup>. Hiervoor dient in beginsel een wettelijke grondslag aanwezig te zijn. Dat zal het geval zijn wanneer een verwerking van externe gegevens samenhangt met personen die al in een register zware criminaliteit zijn vastgelegd. Met betrekking tot die personen bestaan vaak zodanige bezwaren, dat is voorzien in een wettelijke bevoegdheid tot het vergaren van gegevens over hen. Het gebruik van externe persoonsgegevens wordt voorts beperkt door de functies van een register zware criminaliteit.

#### **Functies register zware criminaliteit**

In sectie 9.2.1 is uiteengezet dat de regels die de WPolr en het BPolr stellen aan een registratie in een register zware criminaliteit de mogelijkheden beperken van een verbetering van de informatiepositie van dat register. Wanneer in het kader van een ongericht dataminingonderzoek met betrekking tot een dergelijk register externe persoonsgegevens worden verwerkt, dienen deze op enigerlei wijze te worden vastgelegd. Het register zware criminaliteit biedt daartoe slechts een beperkte mogelijkheid. De reden hiervoor hangt samen met het streven van de wetgever om het aantal CIE-subjecten terug te dringen en te beperken tot hetgeen ten behoeve van de aanpak van de zware criminaliteit noodzakelijk is<sup>108</sup>. Met het oog hierop kunnen slechts persoonsgegevens worden vastgelegd over de personen die art. 13a lid 1 WPolr noemt. Dit gaat niet samen met het in de toelichting op de CIE-regeling beschreven standpunt, dat bij een analyse met betrekking tot de bestrijding van de zware criminaliteit gegevens kunnen worden verwerkt die nog niet voor een zelfstandige registratie in dit register in aanmerking komen. Omdat die gegevens op grond van art. 13a lid 1 WPolr (nog) niet kunnen worden vastgelegd in een register zware criminaliteit, kunnen zij niet in een analyse worden betrokken. Voor een verwerking van externe persoonsgegevens dient het te gaan om personen die mogen worden vastgelegd in een register zware criminaliteit of om gegevens waarvan het op voorhand duidelijk is dat zij daarmee direct verband houden. Het is daarom niet mogelijk om naar aanleiding van tips of meldingen persoonsgegevens over onverdachte personen vast te leggen in een register zware criminaliteit teneinde deze te verwerken. Deze gege-

---

106. *Kamerstukken II*, 1996/197, 25 403, nr. 3, p. 8.

107. *Kamerstukken II*, 1997/198, 25 880, nrs. 1-2, p. 83.

108. *Kamerstukken II*, 1996/197, 25 398, nr. 3, p. 5-6.

vens worden immers juist vastgelegd om middels analyse mogelijke verbanden met andere gegevens aan te tonen<sup>109</sup>.

In art. 18 van het modelreglement van het register zware criminaliteit wordt met betrekking tot het bestaan van verbanden met andere gegevensverzamelingen aangegeven, dat de gegevens in dit register afkomstig kunnen zijn uit andere registers zware criminaliteit of een voorlopig register. Bij opname in het zware criminaliteitsregister dient te zijn voldaan aan het in de wet geformuleerde opslagcriterium. Het lijkt niet de bedoeling om met het bepaalde in art. 18 van het modelreglement het gebruik van gegevens van buiten de politieke sfeer volledig uit te sluiten. Wel lijkt het standpunt te worden bevestigd dat een dataminingonderzoek waarbij gebruik wordt gemaakt van persoonsgegevens uit andere politieregisters of open bronnen in beginsel niet kan plaatsvinden wanneer het register zware criminaliteit als basisregister (datawarehouse) fungeert. Het gebruik van externe persoonsgegevens van buiten de politieke sfeer lijkt slechts mogelijk wanneer op voorhand duidelijk is dat die gegevens betrekking hebben op de categorieën van personen die art. 13a lid 1 WPolr noemt. Nu het ongerichte dataminingonderzoek juist is gericht op het aantonen van dergelijke verbanden tussen gegevens in een register zware criminaliteit en andere gegevens, is de ruimte die het register zware criminaliteit biedt voor het doen van ongericht dataminingonderzoek beperkt.

#### *9.7.2.2 Koppeling*

Er is sprake van een koppeling wanneer gebruik wordt gemaakt van externe gegevens die deel uitmaken van een zelfstandige verzameling van persoonsgegevens. Een register zware criminaliteit kan op grond van art. 4 lid 1 BPolr slechts worden gekoppeld met een ander politieregister of met een persoonsregistratie van het Rijk, provincies, gemeenten en andere openbare lichamen met inbegrip van de daaronder ressorterende diensten, instellingen en bedrijven<sup>110</sup>. Voorts gelden de overige voorwaarden die bij een koppeling in acht dienen te worden genomen. Eén daarvan is dat het modelreglement van een register zware criminaliteit in een zodanige koppeling dient te voorzien.

#### **Modelreglement register zware criminaliteit**

Het modelreglement van een register zware criminaliteit bepaalt in art. 17 dat kan worden gekoppeld met een ander politieregister of een register als bedoeld in art. 17, aanhef en onder *a* Wpr, voor zover dat noodzakelijk is voor het voorkomen en opsporen van misdrijven die een ernstige inbreuk op de rechtsorde opleveren en het betreft: (a) andere registers zware criminaliteit, voorlopige registers, dan wel gegevensverzamelingen waarvan de doelstelling nauw bij die van het register zware criminaliteit aansluit; (b) andere

---

109. Een zodanige analyse kan mogelijk plaatsvinden in een voorlopig politieregister.

110. Als bedoeld in art. 17, aanhef en onder *a* Wpr.

gegevensverzamelingen. Hiermee bevestigt het modelreglement het bepaalde in art. 4 lid 1 BPolr. In art. 17 lid 1*b* van het modelreglement wordt gesproken over ‘andere gegevensverzamelingen’. Deze bepaling ziet op situaties waarin niet op voorhand kan worden aangegeven met welke registers de koppeling zal plaatsvinden. Zowel bij de gegevensverzamelingen waarvan de doelstellingen nauw aansluiten bij die van het register zware criminaliteit, alsook bij de andere gegevensverzamelingen die art. 17 noemt, dient het te gaan om een politieregister of een register als bedoeld in art. 17, aanhef en onder *a* Wpr. Dit betekent dat een register zware criminaliteit bijvoorbeeld niet kan worden gekoppeld met een klantenbestand van een internetprovider.

#### *9.7.2.3 Vrijwillige verstrekking*

Ook een verwerking van gegevens die vrijwillig door derden aan het register zware criminaliteit worden verstrekt is gebonden aan de beperkingen die samenhangen met de functies van dit bijzondere politieregister. Persoonsgegevens die nog niet in aanmerking komen voor zelfstandige registratie in een register zware criminaliteit kunnen in beginsel alleen worden vastgelegd en bewerkt in het BPS of een voorlopig politieregister. Een directe toetsing van het register zware criminaliteit aan de betreffende gegevens is in beginsel uitgesloten.

#### *9.7.2.4 Gebruik van gegevens uit openbare registers*

Persoonsgegevens mogen slechts worden verwerkt indien dat noodzakelijk is voor de uitvoering van de politietaak. Uit art. 4 WPolr vloeit voort dat de politietaak niet kan rechtvaardigen dat over een onbepaalde groep van burgers gegevens worden vergaard voor algemene politieke doeleinden, ook niet uit openbare bronnen. Het gebruik van deze gegevens is beperkt tot een ‘bepaald geval’ in de zin van art. 13 WPolr, ofwel bij een verdenking of een CIE-subject. Het ruimste gebruik zou zijn bij een verkennend onderzoek<sup>111</sup>. Hoewel ook bij een verwerking met betrekking tot een register zware criminaliteit sprake is van CIE-subjecten is het de vraag of, ter verbetering van de algemene informatiepositie van dit register, inderdaad kan worden gekoppeld met openbare registers. In zeer ernstige zaken (georganiseerde criminaliteit) dient het mogelijk te zijn om, volgens passende procedures, omvangrijke bestanden te bevragen en te koppelen, ook wanneer deze zijn aangelegd voor geheel andere doeleinden<sup>112</sup>. Het ligt echter niet voor de hand deze mogelijk te verbinden aan een ongericht dataminingonderzoek ter verbetering van de algemene informatiepositie van een register zware criminaliteit. Wanneer er omstandigheden zijn waardoor een meer ingekaderde en op het specifieke geval gerichte registratie is te prefereren, kan namelijk ook een tijdelijk register worden aangelegd. Met

---

111. *Kamerstukken II*, 1998/99, 26 410, nr. 3, p. 10-11.

112. *Kamerstukken II*, 1997/98, 25 880, nrs. 1-2, p. 83.

betrekking tot een CIE-subject wordt dan een gericht dataminingonderzoek verricht<sup>113</sup>, waarbij kan worden gekoppeld met openbare registers.

### Resumerend

Het gebruik van externe gegevens van buiten de politieke sfeer is beperkt mogelijk. Voor het gebruik van externe persoonsgegevens gelden aanvullende voorwaarden, die als grondslag dienen voor een verwerking en vastlegging als zelfstandig subject in een register zware criminaliteit. Ondanks het grote belang van dataminingonderzoek met betrekking tot dit bijzondere politieregister, worden de mogelijkheden daartoe beperkt door de functies van een register zware criminaliteit en het daarmee samenhangende verstrekkingenregime. Met het oog op het doel van een register zware criminaliteit, de taken van de CIE en het bepaalde in art. 1 lid 1 onder *k* en art. 13*d* lid 3 WPolr, komt dat register het beste in aanmerking om als datawarehouse te dienen bij een verbetering van de informatiepositie daarvan. De mogelijkheden daartoe zijn op grond van art. 13*a* lid 1 WPolr evenwel slechts beperkt.

#### *9.7.3 Het gebruik van gegevens uit een gewoon politieregister*

In deze sectie wordt nagegaan of ten behoeve van de informatiepositie van een register zware criminaliteit gebruik kan worden gemaakt van gegevens uit gewone politieregisters. Daarbij wordt de invloed van factoren als de doelbinding, de aard van de politietoon, de koppeling en de aard van het dataminingonderzoek op het gebruik van deze registers onderzocht.

##### *9.7.3.1 De doelbinding*

Hoewel ten aanzien van de gewone politieregisters een vrij verkeer van gegevens binnen het politieapparaat bestaat, is onbeperkt gebruik van die gegevens ten behoeve van de informatiepositie van een register zware criminaliteit ongewenst. Zowel de gewone politieregisters als de registers zware criminaliteit dienen de algemene politietoon en zijn in beginsel bestemd voor operationeel gebruik. Wanneer in het kader van een koppeling gegevens uit een gewoon politieregister worden vastgelegd in een register zware criminaliteit, dient dat noodzakelijk te zijn in het kader van de bestrijding van de zware criminaliteit. De registratie van gegevens die betrekking hebben op de zware criminaliteit is in beginsel voorbehouden aan de bijzondere politieregisters en in het bijzonder aan het register zware criminaliteit zelf. Met het oog hierop zal niet snel sprake zijn van een noodzaak om gegevens uit een gewoon politieregister te verwerken voor het doel van een register zware criminaliteit. Gegevens betreffende zware criminaliteit kunnen en mogen immers niet in gewone politieregisters worden opgeslagen. Het BPS vormt hierop een uitzondering.

---

113. *Kamerstukken II*, 1997/98, 25 398, nr. 6, p. 10.

### Het hulpverleningsregister en het register-MOT

Het hulpverleningsregister en het register-MOT zijn gewone politieregisters, waarvoor op grond van art. 12 BPolr rekening dient te worden gehouden met de doelbinding. Uit het hulpverleningsregister mag enkel worden verstrekt voor de doeleinden waarvoor dat register is aangelegd, tenzij een geregistreerde uitdrukkelijk instemt met het gebruik van zijn of haar gegevens. Het karakter van een ongericht dataminingonderzoek staat in beginsel het verkrijgen van een dergelijke instemming in de weg. Deze uitzondering op de doelbinding van een hulpverleningsregister in art. 12 lid 1*a* BPolr lijkt vooral bruikbaar voor afzonderlijke gevallen. In geval van een volledige koppeling met een hulpverleningsregister is het, vanuit zowel juridisch als praktisch oogpunt, onwenselijk hierop een beroep te doen.

Ook het register-MOT kent een afwijkend verstrekkingenregime, op grond waarvan een verstrekking in beginsel slechts mogelijk is voor het doel waarvoor het register is aangelegd. Hierop bestaan enkele uitzonderingen. Zo is een verstrekking uit het register-MOT mogelijk ten behoeve van opname in een register zware criminaliteit of wanneer uit de gegevens zelf een redelijk vermoeden voortvloeit dat een bepaalde persoon een misdrijf heeft begaan. In beide gevallen zullen de betreffende gegevens in aanmerking komen om als zelfstandig subject in het register zware criminaliteit te worden vastgelegd. In art. 12 lid 1*b* onder 3 BPolr is een uitzondering op die voorwaarde opgenomen. Op grond daarvan kunnen gegevens uit het register-MOT op verzoek aan leden van het OM worden verstrekt, voor zover zij deze behoeven in verband met hun gezag en zeggenschap over de politie dan wel over andere personen of instanties die met de opsporing van strafbare feiten zijn belast of voor de uitvoering van andere bij of krachtens wet opgedragen taken<sup>114</sup>. De gegevens dienen daarbij redelijkerwijs van belang te kunnen zijn ter voorkoming of opsporing van misdrijven als bedoeld in art. 1 lid 1 onder *k* WPolr. Het lijkt echter onwaarschijnlijk dat op grond hiervan gebruik kan worden gemaakt van gegevens in het register-MOT in het kader van een ongericht dataminingonderzoek met betrekking tot een register zware criminaliteit. In de praktijk zal het vooral gaan om het opvragen van gegevens in het register-MOT naar aanleiding van een bepaald geval of zaak betreffende de zware criminaliteit.

#### *9.7.3.2 De aard van de politietaak*

Het is in het kader van een dataminingonderzoek met betrekking tot een register zware criminaliteit niet vanzelfsprekend dat gebruik kan worden gemaakt van een politieregister dat niet is aangelegd in het kader van de politietaak met betrekking tot de strafrechtelijke handhaving van de rechtsorde. Zo is het gebruik van een hulpverleningsregister ongewenst met het oog op de doelbinding, maar ook vanwege de aard van de politietaak

---

114. Art. 15 lid 1 onder *a* WPolr.

waarvoor het is aangelegd. Het gebruik van gegevens in een OOH-register die zijn vastgelegd in het kader van de openbare orde is wellicht mogelijk, wanneer daarvoor een aantoonbare noodzaak aanwezig is. Daarvan lijkt in beginsel geen sprake te zijn.

#### *9.7.3.3 Koppeling*

Wanneer in het kader van een ongericht dataminingonderzoek gebruik van een gewoon politieregister wordt gemaakt, dient te worden voldaan aan de voor een koppeling geldende voorwaarden. Zo dient de koppeling op grond van art. 6 lid 1 WPolr noodzakelijk te zijn voor een goede uitvoering van de politietaak; een registratie van gegevens uit het betreffende gewone politieregister in het register zware criminaliteit dient noodzakelijk te zijn voor het doel van dat register. Voorts dienen de reglementen van beide registers in de mogelijkheid van een koppeling te voorzien.

#### **Modelreglement register zware criminaliteit**

Op grond van art. 17 van het modelreglement van een register zware criminaliteit kan dat register worden gekoppeld met een ander politieregister, voor zover dat noodzakelijk is voor het voorkomen en opsporen van misdrijven die een ernstige inbreuk op de rechtsorde opleveren. In dit verband dient het te gaan om een gewoon politieregister waarvan de doelstelling nauw aansluit bij die van het register zware criminaliteit. Over het algemeen is de noodzaak tot het gebruik van gegevens uit een gewoon politieregister eerder aanwezig, naarmate de doelstelling van dat register dichter bij die van het register zware criminaliteit ligt. Gezien de doelstelling en de aard van de gegevens van registers als het BPS en het register-MOT, lijken deze voor een koppeling in aanmerking te komen.

#### *9.7.3.4 De aard van het ongerichte dataminingonderzoek*

De aard van een ongericht dataminingonderzoek noopt tot een terughoudende opstelling bij de verwerking van externe gegevens. In dit verband zij ook gewezen op de CIE-regeling, waar in art. 4 lid 2 wordt bepaald dat de criminele inlichtingeneenheden bij hun werkzaamheden gebruik maken van een geautomatiseerde verwijzingsindex<sup>115</sup>. Een dergelijke index kan goede diensten bewijzen bij de informatie-uitwisseling tussen met name de bijzondere politieregisters onderling, bijvoorbeeld om te bezien of bepaalde personen bij andere criminele inlichtingeneenheden al bekend zijn, hetgeen aanleiding kan vormen tot onderling overleg. Het gebruik van gewone politieregisters is minder evident, laat staan dat er sprake kan zijn van een volledige koppeling met deze politieregisters.

In het kader van een ongericht dataminingonderzoek met betrekking tot een register zware criminaliteit kan slechts beperkt gebruik worden gemaakt van externe persoonsgegevens. Van de gewone politieregisters lijkt zelfs in het geheel geen gebruik te kunnen

---

115. *Stcrt.* 12 oktober 2000, nr. 198, p. 14.

worden gemaakt. Persoonsgegevens in een gewoon politieregister kunnen alleen overeenkomstig art. 13a lid 1 WPolr in een register zware criminaliteit worden vastgelegd. Dergelijke gegevens zullen in beginsel niet aanwezig zijn in een gewoon politieregister. Met het oog op het noodzakelijkheidsvereiste van art. 4 WPolr<sup>116</sup> is de registratie van die gegevens voorbehouden aan het register zware criminaliteit. Er kan zich een situatie voordoen waarin personen door verschillende bronnen in zowel een gewoon politieregister als in een register zware criminaliteit zijn vastgelegd. In dat geval kunnen gegevens over die personen in het gewone politieregister worden opgenomen in het register zware criminaliteit; zij voldoen immers aan de daarvoor geldende criteria. Voor het aantonen van een connectie tussen de gegevens in het gewone politieregister en die in het register zware criminaliteit dient een vergelijking tussen beide politieregisters te worden gemaakt. Een dergelijke vergelijking in het kader van een ongericht dataminingonderzoek is echter niet mogelijk, aangezien gegevens voortvloeiende uit een koppeling van een gewoon politieregister met een register zware criminaliteit, in het laatstgenoemde register niet mogen worden vastgelegd.

### Resumerend

In beginsel kan in het kader van een ongericht dataminingonderzoek met betrekking tot een register zware criminaliteit geen gebruik worden gemaakt van gegevens uit een gewoon politieregister. Naast andere beperkende factoren als de politietaak, de doelbinding en de koppeling, ligt hieraan vooral het verstrekkingenregime van het register zware criminaliteit ten grondslag. Het bepaalde in art. 13a lid 1 WPolr sluit de mogelijkheid van een koppeling met persoonsgegevens in de gewone politieregisters volledig uit. In de hoedanigheid van datawarehousing kan een register zware criminaliteit slechts een beperkte categorie persoonsgegevens bevatten, hetgeen de mogelijkheid tot koppeling in het kader van een dataminingonderzoek beperkt.

#### *9.7.4 Het gebruik van gegevens uit een bijzonder politieregister*

Hierna zal worden onderzocht in hoeverre het mogelijk is om gebruik te maken van gegevens in de bijzondere politieregisters.

##### *9.7.4.1 Het gebruik van een tijdelijk politieregister*

Een tijdelijk politieregister kan onder meer worden aangelegd in het kader van de bestrijding van de zware criminaliteit in een bepaald geval. Of in de praktijk ook gebruik kan worden gemaakt van de gegevens in een tijdelijk register is afhankelijk van een aantal hierna te bespreken factoren.

---

116. *Kamerstukken II*, 1996/197, 25 398, nr. 3, p. 9.

### De doelbinding

Op grond van art. 13 lid 2 WPolr vindt een verstrekking uit een tijdelijk politieregister aan een register zware criminaliteit slechts plaats voor het doel van het tijdelijk politieregister, tenzij de verstrekking plaatsvindt ten behoeve van opname in een register zware criminaliteit. Van die laatste verstrekkinggrond is alleen sprake wanneer de gegevens als zelfstandig subject in het register zware criminaliteit kunnen worden opgenomen. Het biedt geen wettelijke grondslag om gegevens die niet aan die voorwaarde voldoen in het kader van een dataminingonderzoek aan een register zware criminaliteit te verstrekken. Aangaande een verstrekking voor het doel van het tijdelijk politieregister zij opgemerkt dat de verstrekking aan een register zware criminaliteit hier in eerste instantie plaatsvindt ten behoeve van dat register en niet ten behoeve van het tijdelijk politieregister. Een verstrekking lijkt daarom niet mogelijk. Op grond van art. 4 lid 2 WPolr dient een registratie van de verstrekte gegevens uit een tijdelijk politieregister aan een register zware criminaliteit noodzakelijk te zijn voor het laatstgenoemde register. Nu een tijdelijk politieregister voor allerhande doeleinden kan worden aangelegd, zal van een zodanige noodzaak slechts sprake zijn wanneer het doel van het onderzoek waarvoor het tijdelijk register is aangelegd, is gelieerd is aan de bestrijding van de zware criminaliteit.

### Koppeling

Aangezien zowel een register zware criminaliteit als een tijdelijk politieregister in het kader van dezelfde politietaak wordt aangelegd, kan een koppeling van deze registers noodzakelijk zijn voor de politietaak. Hierbij speelt ook de doelbinding een rol. Op grond van art. 4 lid 2 BPolr zal het initiatief tot een koppeling (en daarmee een gegevensverstrekking) in beginsel steeds uitgaan van de beheerder van het tijdelijke politieregister, waarbij er vanuit het oogpunt van dat politieregister een noodzaak tot koppeling dient te zijn. Wanneer het ongerichte dataminingonderzoek, in het kader waarvan de verstrekking plaatsvindt, evenwel uitgaat van het register zware criminaliteit lijkt vanuit het tijdelijk politieregister geen noodzaak tot koppeling aanwezig te zijn. Dit kan ook worden afgeleid uit het feit dat een register zware criminaliteit is bestemd voor operationeel gebruik en kan worden bevroegd door de beheerder van een tijdelijk politieregister. Hierdoor is voor het verkrijgen van aanvullende informatie (voor het doel van het tijdelijk register) geen noodzaak aanwezig om te koppelen met een register zware criminaliteit<sup>117</sup>.

Bij een koppeling van twee bijzondere politieregisters dienen de reglementen van beide registers in de mogelijkheid daartoe te voorzien. Een tijdelijk register is voor bepaalde duur vrijgesteld van de verplichting om in een reglement te voorzien<sup>118</sup>. Zonder

---

117. Tenminste niet wanneer het initiatief om te koppelen uitgaat van het register zware criminaliteit, zoals hier het geval is.

118. Art. 13 lid 3 WPolr.

een reglement is echter geen koppeling mogelijk. Het modelreglement van een register zware criminaliteit bepaalt dat een koppeling noodzakelijk dient te zijn voor de bestrijding van de zware criminaliteit. Op grond van art. 17 van het modelreglement is een koppeling met een tijdelijk politieregister mogelijk, wanneer de doelstelling waarvoor het tijdelijk register is aangelegd nauw aansluit bij die van het register zware criminaliteit. Wanneer een tijdelijk register in het kader van een lichter vergrijp is aangelegd, is een combinatie van gegevens uit dat register met gegevens uit een register zware criminaliteit onwenselijk.

#### **De aard van het ongerichte dataminingonderzoek**

Bij een koppeling van een tijdelijk register met een register zware criminaliteit kan sprake zijn van een ontoelaatbare inbreuk op de privacy. Dit wordt duidelijk uit de daarop betrekking hebbende kamerstukken<sup>119</sup>, waar wordt opgemerkt dat de voormalige CID-regelgeving ook opslag van gegevens toeliet met betrekking tot misdrijven die, gezien hun frequentie dan wel het georganiseerd verband waarin zij worden gepleegd, een ernstige inbreuk op de rechtsorde maken zonder dat het vereiste van opname in art. 67 lid 1 Sv gold. Ten aanzien van deze categorieën van misdrijven kan na de (plaatsgevonden) wijziging van de WPolr geen registratie meer in het voorlopige register en het register zware criminaliteit plaatsvinden. Dit betekent niet dat dit in het geheel niet mogelijk is in concrete zaken waarin de noodzaak tot registratie van ‘zachte opsporingsinformatie’ met betrekking tot één van de misdrijven, behorende tot deze categorieën, zich voordoet. De aanleg van een tijdelijk register biedt in dat soort gevallen uitkomst. Het gebruik van die ‘zachte’ gegevens voor de opsporing van andere strafbare feiten is dan in beginsel echter niet toegestaan. Dat hangt weer samen met de functies van het register zware criminaliteit, op grond waarvan een verwerking van gegevens uit een tijdelijk politieregister in een register zware criminaliteit niet steeds mogelijk is. Een registratie van gegevens uit een tijdelijk register in het register zware criminaliteit dient in overeenstemming te zijn met art. 13a lid 1 WPolr. Daarvan kan sprake zijn wanneer het tijdelijk register betrekking heeft op de zware criminaliteit. In dat geval is een dubbele registratie mogelijk van gegevens in een register zware criminaliteit en een tijdelijk register. Gegevens in een tijdelijk politieregister die niet voldoen aan de voorwaarde van opslag als zelfstandig subject in een register zware criminaliteit kunnen niet worden gebruikt (tenzij het geen persoonsgegevens betreft). Wel kan gebruik worden gemaakt van een verwijzingsindex zoals het MRO-bestand, dat een overzicht verschaft van alle rechercheonderzoeken als bedoeld in de art. 126gg en 132a Sv en bijdraagt aan de informatievoorziening in het kader van de uitvoering van art. 2 Politiewet 1993. Hiermee wordt gegarandeerd dat uit een tijdelijk politieregister niet meer gegevens worden verstrekt dan strikt noodzakelijk is voor het doel waarvoor de verstrekking plaatsvindt.

---

119. *Kamerstukken I*, 1998/99, 25 398, nr. 63f, p. 2.

### Resumerend

Het gebruik van een tijdelijk politieregister is wenselijk, wanneer de doelstelling van dat register (sterk) overeenkomt met die van het register zware criminaliteit. In dat geval mogen de gegevens in het tijdelijk politieregister als zelfstandig subject op grond van art. 13a lid 2 WPolr worden verstrekt aan een register zware criminaliteit. Er is dan geen sprake van een koppeling, maar van een verstrekking van gegevens door de beheerder van het tijdelijk politieregister aan het register zware criminaliteit. Een tijdelijk politieregister kan ook gegevens bevatten die niet in aanmerking komen voor vastlegging als zelfstandig subject in een register zware criminaliteit. Wanneer het tijdelijk register niet is aangelegd in het kader van de bestrijding van de zware criminaliteit is het gebruik van die gegevens uitgesloten.

#### *9.7.4.2 Het gebruik van een voorlopig politieregister*

Het voorlopige politieregister is het voorportaal van het register zware criminaliteit. In deze sectie wordt onderzocht op welke wijze deze twee bijzondere politieregisters zich tot elkaar verhouden.

### De doelbinding

Uit een voorlopig politieregister wordt alleen verstrekt voor het doel waarvoor het register is aangelegd en voor zover de gegevens benodigd zijn ter identificatie. Een verstrekking aan een register zware criminaliteit lijkt mogelijk wanneer daarmee een verrijking van het voorlopige politieregister kan worden bewerkstelligd. In dit geval leidt een verstrekking echter niet direct tot een verrijking van de informatiepositie van het voorlopige politieregister, maar van die van het register zware criminaliteit. Bovendien zouden daarmee gegevens beschikbaar komen voor het register zware criminaliteit waarvan de wetgever (met de introductie van de bijzondere politieregisters) het gebruik in dat verband juist heeft willen uitsluiten.

Een verstrekking voor het doel van een voorlopig politieregister aan een register zware criminaliteit lijkt voorts onmogelijk met het oog op art. 13b lid 3 WPolr, waar wordt bepaald dat een dergelijke verstrekking niet in enig ander register wordt vastgelegd. Dit betekent dat de gegevens niet verwerkt kunnen worden in het kader van een ongericht dataminingonderzoek met betrekking tot een register zware criminaliteit. Uit een voorlopig politieregister kunnen op grond van art. 13b lid 2, tweede volzin WPolr ook gegevens worden verstrekt ten behoeve van opname in een ander bijzonder politieregister. In dat geval zullen de te verstrekken gegevens als zelfstandig subject moeten kunnen worden vastgelegd in een register zware criminaliteit. Het artikel biedt geen grondslag voor een verstrekking in het kader van een dataminingonderzoek.

### Koppeling

In het kader van art. 4 lid 2 WPolr dient een koppeling tussen een voorlopig register en een register zware criminaliteit noodzakelijk te zijn voor het doel van het laatstgenoemde register. Hoewel een koppeling met een voorlopig politieregister mogelijk waardevolle informatie oplevert ten behoeve van de bestrijding van de zware criminaliteit, lijkt de doelbinding die samenhangt met het verstrekkingenregime van het voorlopige politieregister een verstrekking aan een register zware criminaliteit in de weg te staan. In sectie 9.5.6.2 bleek dat ten behoeve van een voorlopig politieregister ook kan worden gekoppeld met een register zware criminaliteit<sup>120</sup>, waarbij geen gegevens uit het voorlopige politieregister aan het register zware criminaliteit behoeven te worden verstrekt. Met het oog daarop kan worden gesteld dat het voor het doel van een voorlopig politieregister niet noodzakelijk is om te koppelen met een register zware criminaliteit (in het kader van een dataminingonderzoek met betrekking tot dat register) waarbij gegevens uit het voorlopige register aan het register zware criminaliteit worden verstrekt.

*Modelreglementen voorlopige politieregister en register zware criminaliteit* – Op grond van art. 14 van het modelreglement van een voorlopig politieregister<sup>121</sup> kan dit register worden gekoppeld met een ander bijzonder politieregister, voor zover dat noodzakelijk is voor het doel van het voorlopige politieregister. Wanneer het initiatief tot koppeling uitgaat van het register zware criminaliteit, is in beginsel geen sprake van een dergelijke noodzaak. Bovendien kan de beheerder van een voorlopig politieregister de benodigde informatie zelf opvragen uit een register zware criminaliteit. Het modelreglement van het register zware criminaliteit laat een koppeling met een voorlopig politieregister evenwel open voor zover dat noodzakelijk is ter voorkoming en opsporing van misdrijven die een ernstige inbreuk op de rechtsorde opleveren. Gezien het doel van een voorlopig politieregister lijkt een koppeling mogelijk op grond van het modelreglement van het register zware criminaliteit.

### De aard van het ongerichte dataminingonderzoek

Gegevens in een voorlopig politieregister kunnen betrekking hebben op onschuldige personen. Een verwerking van dergelijke gegevens is enkel gerechtvaardigd wanneer het doel van het inbreukmakende onderzoek opweegt tegen de ernst van de inbreuk. Uit een voorlopig register worden geen gegevens verstrekt voor operationeel gebruik, aangezien zij nog niet voldoen aan het criterium voor opslag in het register zware criminaliteit. De waarborgen ter bescherming van de persoonlijke levenssfeer worden gevonden in het zeer beperkte verstrekkingenregime voor het voorlopige politieregister<sup>122</sup>. Met het oog hierop

---

120. Uitgezonderd de gegevens in een register zware criminaliteit die behoren tot categorie *c*.

121. Model privacyreglement voorlopig register, *Stcrt.* 12 oktober 2000, nr. 198, p. 17.

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

is het niet mogelijk om gegevens uit een voorlopig register vast te leggen in een register zware criminaliteit. Aangezien laatstgenoemd register is bestemd voor operationeel gebruik, resulteert een verstrekking in een ontoelaatbare inbreuk op de persoonlijke levenssfeer. De gegevens in een voorlopig politieregister komen nog niet in aanmerking voor registratie in het register zware criminaliteit en voldoen daarmee niet aan de criteria van art. 13a lid 1 WPolr. Met het oog hierop is het onmogelijk gegevens uit een voorlopig politieregister in het kader van een koppeling vast te leggen in het register zware criminaliteit. Door de ruime mogelijkheid tot raadpleging van het register zware criminaliteit wordt de analysefunctie van het register beperkt.

### Resumerend

In het kader van een ongericht dataminingonderzoek met betrekking tot een register zware criminaliteit kan in beginsel geen gebruik worden gemaakt van gegevens in een voorlopig politieregister. Gelet op het huidige verstrekkingenregime van het register zware criminaliteit is dit niet bevreemdend. De opslag van gegevens in een voorlopig register houdt rechtstreeks verband met de wettelijke doelbinding van het register zware criminaliteit. In het voorlopige register<sup>123</sup> worden gegevens opgeslagen die in de toekomst in samenhang met nog te verkrijgen gegevens mogelijk van een zodanig betrouwbaarheidsgehalte zullen zijn, dat zij kunnen worden overgeheveld naar het register zware criminaliteit. Omdat het daarbij gaat om tips en meldingen die nog niet bevestigd worden door andere bronnen, kent dit register een verstrekkingenregime dat aanmerkelijk restrictiever is dan dat van een register zware criminaliteit. Met het oog op de functie van voorportaal van het register zware criminaliteit is een verstrekking uit het voorlopige register aan het register zware criminaliteit uitgesloten.

#### *9.7.4.3 Het gebruik van een ander register zware criminaliteit*

Omdat de verschillende registers zware criminaliteit qua doelstelling, verstrekkingenregime en reglement identiek zijn, bestaan in beginsel geen juridische bezwaren tegen het onderling uitwisselen van gegevens tussen deze politieregisters. Ook in art. 6 van de CIE-regeling wordt benadrukt dat criminele inlichtingeneenheden onderling, gevraagd en ongevraagd, criminele inlichtingen uitwisselen indien dat van belang kan zijn voor de uitvoering van de politietaak. Daartoe wordt gebruik gemaakt van een modelformulier. Het is niet duidelijk of daarbij ook gegevens in een register zware criminaliteit, behorende tot categorie c), mogen worden uitgewisseld. Wanneer het gaat om de gebundelde informatiepositie van de verschillende registers zware criminaliteit is vooral het nationale register zware criminaliteit, dat wordt bijgehouden door de in sectie 9.1.2.2 besproken NCIE, interessant. Met betrekking tot de werkzaamheden van de NCIE blijkt uit art. 7

---

123. *Kamerstukken II*, 1997/98, 25 398, nr. 6, p. 3. Hier wordt het voorlopig register nog aangehaald als 'het vaststellingsregister'.

lid 1*b* en 8 lid 1*b* van de CIE-regeling dat alleen de personalia of bedrijfsgegevens van de overeenkomstig art. 13*a* lid 1 onder *a* en *b* WPolr geregistreerde personen worden vastgelegd in het nationale register zware criminaliteit. Hoewel het ook mogelijk is om gegevens in dit register vast te leggen die van nationale of internationale betekenis zijn, lijken er geen gegevens in te worden vastgelegd uit de registers zware criminaliteit die tot categorie *c*) behoren. Nu deze gegevens niet in een nationale verwijzindex worden opgenomen kan worden geconcludeerd dat het onwenselijk is, dat ten aanzien van deze categorie gegevens uitwisseling plaatsvindt met andere registers zware criminaliteit ter verbetering van de informatiepositie met betrekking tot de bestrijding van de zware criminaliteit.

#### 9.7.5 *Afsluitend*

De regeling van art. 6 CIE-regeling is in beginsel ongeschikt als grondslag voor een dataminingonderzoek ter verbetering van de informatiepositie van een voorlopig politieregister of een register zware criminaliteit. Ten eerste is de verplichting tot het onderling uitwisselen van gegevens min of meer vrijblijvend geformuleerd. Ook kost het gebruik van modelformulieren meer tijd dan een situatie waarbij sprake is van rechtstreekse toegang. De efficiëntie van deze regeling kan voorts in twijfel worden getrokken vanwege het feit, dat voor elk register afzonderlijk wordt gestreefd naar een verbetering van de informatiepositie. Op grond van art. 6 lid 2 en 3 kunnen registers zware criminaliteit rechtstreeks onderling worden geraadpleegd, hetgeen een efficiënte aanvulling en verificatie van gegevens mogelijk maakt. Een verbetering van de informatiepositie van een register zware criminaliteit op grond van art. 6 lid 2 en 3 CIE-regeling heeft als voordeel (ten opzichte van art. 6 lid 1) dat er sprake is van een directe toegang. Nadeel is dat een dergelijke verbetering alleen met betrekking tot registers zware criminaliteit kan worden nagestreefd; bovendien is een centrale regeling niet mogelijk, doch dient elk register afzonderlijk te worden verbeterd.

Om te voorzien in een overkoepelend nationaal informatiebeheer op dit punt lijkt de NCIE de aangewezen instantie. Hiervoor dient de wijze waarop de CIE-regeling middels art. 8 in een nationaal gegevensbeheer voorziet, op enkele punten te worden herzien. Of met de NCIE-analyse de gegevens in de betrokken bijzondere politieregisters daadwerkelijk ten volle worden benut hangt onder meer af van de juiste keuze of een bepaald gegeven al dan niet van nationaal of internationaal belang is. Een aandachtspunt is voorts dat de verwijzindex die wordt aangelegd geen overzicht lijkt te verschaffen van de personen die op grond van art. 13*a* lid 1 onder *c* WPolr worden geregistreerd. In het streven naar een zo efficiënt mogelijk gebruik van de voorhanden zijnde criminele inlichtingen kan worden overwogen te kiezen voor afschaffing van het onderscheid tussen de afzonderlijke lokale voorlopige politieregisters en registers zware criminaliteit en hun nationale equivalenten, en de afzonderlijke lokale registers te vervangen door twee nationale registers. Het is onduidelijk wat de toegevoegde waarde is van het hanteren van afzonderlijke

registers naast de overkoepelende nationale registers. In plaats van gegevens voortdurend over en weer te sturen en dubbel te registreren kan worden geopteerd voor één nationaal systeem waartoe eenieder, al dan niet beperkt, toegang heeft. CIE's blijven daarbij verantwoordelijk voor de inhoud c.q. juistheid van de nationale registers, terwijl de beheerstaak en vooral de analyserende taak bij de NCIE ligt. Een analyse kan plaatsvinden op nationaal niveau met betrekking tot alle voorhanden zijnde gegevens. Het resultaat van een dergelijke analyse komt steeds ten goede aan alle gebruikers van dat register die hierop bij of krachtens de WPolr aanspraak kunnen maken.

In beginsel is het wenselijk dat ook gebruik kan worden gemaakt van bijvoorbeeld tips of meldingen die kortstondig zijn vastgelegd in de voor die doeleinden bestemde registers, zoals het BPS. Met het oog op de toepassing van datamining zij opgemerkt dat art. 5a lid 1 onder *b* WPolr weliswaar een mogelijkheid biedt tot registratie van gegevens ten einde deze te kunnen analyseren, maar dat het register daarbij in beginsel niet zelf als datawarehouse kan dienen. Bij een analyse van de gegevens in dit register dient ook gebruik te kunnen worden gemaakt van gegevens uit andere (bijzondere) politieregisters. Het is echter niet de bedoeling dat gegevens die al in een (bijzonder) politieregister zijn vastgelegd, vervolgens op grond van art. 5a WPolr worden overgeheveld naar een register als het BPS. In dat geval komen zij namelijk in aanmerking voor operationeel gebruik, hetgeen strijdig is met het beperkte verstrekkingenregime van de bijzondere politieregisters. Een interpretatie van art. 5a WPolr, waarbij zachte gegevens (waarop normaal gesproken een beperkt verstrekkingenregime van toepassing is) te pas en te onpas in een gewoon politieregister kunnen worden opgenomen, is onwenselijk. Het ligt daarom voor de hand dat de gegevens die in het kader van een analyse worden verwerkt (datawarehouse) worden vastgelegd in het register zware criminaliteit of het voorlopige politieregister zelf (basisregister).

Ten slotte kan er bij een koppeling van een voorlopig politieregister met een gewoon politieregister in beginsel niet meer van passief onderzoek worden gesproken. Wanneer het belang van de bestrijding van de zware criminaliteit de grondslag vormt voor een koppeling dan ligt een vergelijking met een ander bijzonder politieregister eerder voor de hand dan een vergelijking met een gewoon politieregister. Koppeling met het BPS vormt hierop een uitzondering. Vanwege de functie van het BPS als voorportaalregister en de mogelijkheid hierin ook zachte gegevens vast te leggen is het wenselijk, om met dit politieregister te kunnen koppelen. Een zodanige koppeling kan als noodzakelijk voor een voorlopig politieregister worden aangemerkt. In dit verband zij wederom gewezen op de mogelijkheid om verwijsindexen, waarin zachte gegevens kunnen worden vastgelegd, als bijzondere politieregisters aan te merken, dan wel middels een wettelijke regeling in een beperkt verstrekkingenregime voor deze registers te voorzien. Daarmee zou een eventuele

koppeling van het BPS met een voorlopig politieregister in overeenstemming worden gebracht met het uitgangspunt van de wetgever op dit punt<sup>124</sup>.

### *Overzicht en schema*

Terwijl een register zware criminaliteit zich qua doel en inhoud bij uitstek leent voor de toepassing van dataminingonderzoek, blijken de mogelijkheden daartoe in de praktijk beperkt. De huidige wet- en regelgeving stelt, al dan niet terecht, vergaande beperkingen aan de verwerking van gegevens in het kader van de bestrijding van de zware criminaliteit.

### *Geen gebruik van externe gegevens*

Bij een ongericht dataminingonderzoek ter verbetering van de informatiepositie van een register zware criminaliteit, waarbij geen gebruik van externe gegevens wordt gemaakt, dienen de op elk dataminingonderzoek van toepassing zijnde algemene voorwaarden in acht te worden genomen.

### *Gebruik van gegevens die niet afkomstig zijn uit een politieregister*

Met betrekking tot het gebruik van gegevens van buiten de politieke levenssfeer dient te worden onderscheiden naar persoonsgegevens en overige gegevens. Een koppeling met externe gegevensverzamelingen is slechts op beperkte schaal mogelijk. Met het oog op het doel van een register zware criminaliteit kan actief worden gezocht naar externe gegevens, voor zover die betrekking hebben op de zware criminaliteit. Wanneer het persoonsgegevens betreft, zijn de mogelijkheden verder beperkt. Een verwerking van gegevens omtrent onverdachte personen is een ingrijpend middel, waarvoor een wettelijke grondslag aanwezig dient te zijn. Persoonsgegevens die niet in aanmerking komen voor een zelfstandige registratie in een register zware criminaliteit kunnen in het geheel niet worden verwerkt.

### *Gebruik van gegevens uit een gewoon politieregister*

Wanneer in het kader van een ongericht dataminingonderzoek gebruik wordt gemaakt van gegevens uit een gewoon politieregister is sprake van koppeling. Naast de algemene voorwaarden dient in dat geval ook rekening te worden gehouden met aanvullende voorwaarden. Omdat gegevens inzake de zware criminaliteit in beginsel alleen in een bijzonder politieregister kunnen worden vastgelegd lijkt het uitgesloten dat een gewoon politieregister gegevens bevat die in aanmerking komen om als zelfstandig subject te worden vastgelegd in een register zware criminaliteit. Een gewoon politieregister als het BPS kan daarop een uitzondering vormen. Om vast te stellen of dit het geval is dienen de gege-

---

124. Als uiteengezet in sectie 9.5.3.1 onder het kopje *De aard van het ongerichte dataminingonderzoek*.

vens in het BPS echter te worden geanalyseerd; het register zware criminaliteit biedt daarvoor geen ruimte<sup>125</sup>.

*Gebruik van gegevens uit een bijzonder politieregister*

Om diezelfde reden zal in beginsel slechts beperkt gebruik kunnen worden gemaakt van gegevens uit de bijzondere politieregisters. De gegevens in een tijdelijk register kunnen mogelijk als zelfstandig subject worden opgenomen in een register zware criminaliteit. In dat geval is het gebruik van die gegevens middels een verwijzindex mogelijk. Dit geldt niet voor de gegevens in een voorlopig politieregister die nog niet voldoen aan de criteria voor registratie in een register zware criminaliteit. Daarmee is het gebruik van die gegevens in het kader van het ongericht dataminingonderzoek uitgesloten. Het is in beginsel wel mogelijk om gegevens tussen verschillende registers zware criminaliteit onderling uit te wisselen, uitgezonderd de gegevens in een register zware criminaliteit die tot categorie c) worden gerekend. Eén en ander resulteert in het volgende schema:

Onggericht datamining-onderzoek	Koppeling	Beperkingen	Gebruik
Geen gebruik externe gegevens	Nee	Algemeen	Onbeperkt
Gebruik externe gegevens*	Ja**	Algemeen/koppeling/ (specifiek)	Beperkt
Gegevens uit een gewoon politieregister	Ja	Algemeen/koppeling/specifiek	Nee
Gegevens uit een bijzonder politieregister	Ja	Algemeen/koppeling/specifiek	In beperkte mate zowel het tijdelijk politieregister als het register zware criminaliteit

\* Uitgezonderd de gegevens die in de politieregisters liggen opgeslagen.

\*\* Tenzij de externe gegevens niet tot enig zelfstandig register behoren.

*Schema 14 Toepassing ongericht dataminingonderzoek ter verbetering van de informatiepositie van een register zware criminaliteit*

125. Art. 13a lid 1 WPolr

Een register zware criminaliteit leent zich met het oog op art. 13a lid 1 WPolr met name voor een verbetering van de informatiepositie waarbij *geen* gebruik wordt gemaakt van externe gegevens. Voor het gebruik van externe gegevens dient op voorhand duidelijk te zijn dat het gaat om gegevens betreffende de personen die art. 13a lid 1 WPolr noemt. Teneinde zekerheid hieromtrent te verkrijgen met betrekking tot externe gegevens zal in beginsel eerst onderzoek nodig zijn. Het register zware criminaliteit biedt daartoe echter geen ruimte.



---

## 10 Het gerichte dataminingonderzoek

Dataminingonderzoek kan tevens worden gebruikt ter verbetering van de informatiepositie in een bepaald geval. Het betreft dan gericht dataminingonderzoek ten behoeve van operationele opsporing. Een gericht dataminingonderzoek ziet op de politietask in een bepaald geval of op een bepaalde groep van personen, waarbij gericht wordt gezocht naar informatie die aanleiding kan vormen tot een opsporingsonderzoek of daaraan kan bijdragen. In dit hoofdstuk staat de toepassing van gericht dataminingonderzoek centraal, waarbij onder meer wordt gekeken naar de kenmerken van deze dataminingsvariant en de kwalificatie van het datawarehouse dat in het kader daarvan tot stand komt, de verhouding van het onderzoek tot het proces van informatiegaring en de praktische toepassing van gericht dataminingonderzoek.

### 10.1 Kenmerken gericht dataminingonderzoek

Bij een gericht dataminingonderzoek verlegt het zwaartepunt zich van een algemene verbetering van de informatiepositie naar een strafvorderlijke afdoening waarbij sprake kan zijn van opsporing. Het onderzoek zelf vindt plaats in het kader van de strafrechtelijke handhaving van de rechtsorde. De aanleiding tot het uitvoeren van een gericht dataminingonderzoek kan voortkomen uit het resultaat van een ongericht dataminingonderzoek, maar bijvoorbeeld ook uit een binnengekomen tip. In sectie 3.4.2 werd ingegaan op de kenmerken van een gericht dataminingonderzoek. Daarbij bleek onder meer dat het onderzoek een gerichte doelstelling heeft wanneer het is toegespitst op een situatie of groep van personen ten aanzien van wie een bepaalde mate van verdenking is gerezen. Een gericht onderzoek dient meer inzicht of bijzonderheden te verschaffen. Juist vanwege de aanwezigheid van een bepaalde mate van verdenking zijn verdergaande inbreuken op de persoonlijke levenssfeer gerechtvaardigd dan bij een ongericht dataminingonderzoek. Afhankelijk van de mate van verdenking kan gebruik worden gemaakt van zwaardere opsporingsmethoden. De toepassing van een bijzondere opsporingsbevoegdheid is alleen toegestaan in het belang van het onderzoek en dient gericht te zijn op het nemen van strafvorderlijke beslissingen. Omdat een gericht dataminingonderzoek ziet op een concrete zaak, heeft het in beginsel een tijdelijk karakter. Wanneer het doel wordt bereikt loopt het onderzoek ten einde. Een gericht dataminingonderzoek betreft in beginsel steeds 'nieuw' onderzoek, wat wil zeggen dat bij aanvang nog weinig of geen gegevens beschikbaar zijn. Hierdoor bestaat grote behoefte aan het gebruik van externe gegevens. Gaandeweg het onderzoek wordt het zwaartepunt verlegd naar de tot dan toe

verzamelde informatie en is de noodzaak tot het verzamelen van nieuwe gegevens minder prominent aanwezig. Samenvattend heeft een gericht dataminingonderzoek de volgende kenmerken:

- een gerichte doelstelling;
- geen ontoelaatbare inbreuken op de persoonlijke levenssfeer;
- de mogelijkheid tot ingrijpende<sup>1</sup> inbreuken op de privacy (vanwege het gerichte karakter);
- tijdelijk van aard;
- een actief gebruik van externe gegevens;
- primair gericht op de verwerking van externe gegevens.

### **10.2 Positie binnen het proces van informatiegaring**

Op het terrein van de strafrechtelijke handhaving kan het vervolg van de algemene informatiegaring bestaan uit een verkennend onderzoek of een opsporingsonderzoek. Deze keuze hangt af van de aard, de omvang en de kwaliteit van de beschikbare informatie. Indien aanwijzingen bestaan dat binnen een groep van personen strafbare feiten worden beraamd of gepleegd die een ernstige inbreuk op de rechtsorde opleveren, kan een verkennend onderzoek aan een strafrechtelijk opsporingsonderzoek vooraf gaan. Indien uit de verkregen informatie al voldoende concrete aanwijzingen volgen met betrekking tot het plegen of beramen van strafbare feiten als beschreven in art. 132a Sv wordt, indien dit opportuun is, een opsporingsonderzoek gestart. Van een gericht dataminingonderzoek kan sprake zijn in het tweede en derde stadium van de opsporing respectievelijk het verkennend onderzoek en het opsporingsonderzoek. Volledigheidshalve zij opgemerkt dat in alle stadia van de strafrechtelijke handhaving van de rechtsorde sprake kan zijn van informatiegaring. Dit betekent dat ook in het kader van een gericht dataminingonderzoek sprake kan zijn van het opbouwen en in stand houden van een zekere informatiepositie door het opslaan, bewerken, gebruiken en analyseren van gegevens of het vergaren van gegevens door de toepassing van niet-ingrijpende middelen. In dat geval kan het opbouwen van een zekere informatiepositie echter niet het enige doel zijn. Ter verduidelijking kan schema 4 op de onderstaande wijze (schema 15) worden aangevuld.

---

1. In vergelijking met een ongericht dataminingonderzoek.

	Ontdekken		Toetsing
<b>Toepassingsvarianten dataminingsproces</b>	Ongericht dataminingsonderzoek	Gericht dataminingsonderzoek	Verificatie
<b>Het proces van informatiegaring</b>	Opbouwen en instandhouden van de informatiepositie	Het verkennend onderzoek	Het opsporingsonderzoek
<b>Aanknopingspunten</b>	Geen verdenking	← Overgang ⇒	Verdachte

Schema 15 De relatie tussen de drie dataminingsvarianten en de stadia van het proces van informatiegaring

### 10.2.1 Het verkennend onderzoek

Op basis van een goede informatiepositie kunnen prioriteiten in de opsporing worden gesteld en kan bijvoorbeeld worden besloten, verkennend onderzoek te doen. Daarvoor dienen er feiten of omstandigheden te zijn waaruit aanwijzingen voortvloeien, dat binnen verzamelingen van personen misdrijven worden beraamd of gepleegd. Er is sprake van een bepaalde mate van verdenking. De informatie die wordt verzameld, veredeld en geanalyseerd heeft, en mag slechts betrekking hebben, op een duidelijk afgebakende groep van personen<sup>2</sup>, hetgeen het gerichte karakter van het onderzoek onderstreept. De groep van personen hoeft geen enkele binding te hebben en kan op grond van allerehande kenmerken worden geselecteerd<sup>3</sup>. Het betreft meer algemeen onderzoek naar verzamelingen van personen (branches, sectoren van de samenleving, etc.) ten aanzien van wie aanwijzingen bestaan dat bepaalde typen criminaliteit er meer dan gemiddeld voorkomen<sup>4</sup>. Met een verkennend onderzoek wordt niet beoogd concrete feiten op te helderen of een georganiseerd verband in kaart te brengen. Het onderzoek heeft als doel te komen tot beslissingen over het starten van één of meer opsporingsonderzoeken<sup>5</sup>. Hierbij kunnen op grote schaal persoonsgegevens over onverdachte personen worden vastgelegd die afkomstig zijn uit open bronnen of zijn verkregen op basis van vrijwillige medewerking van particulieren. Met het oog hierop heeft het verkennend onderzoek een wettelijke grondslag. Het onderscheidt zich van het opsporingsonderzoek door het voorwerp

2. Dit blijkt onder meer uit de definitie in het eindrapport van de PEC (*Kamerstukken II*, 1995/96, 24 072, nrs. 10-11) en uit het *Handboek voor de opsporingspraktijk* 2000, sectie 1.2.2, 'begripsbepaling verkennend onderzoek'.
3. Dat is een essentieel onderscheid ten opzichte van het 'georganiseerd verband' van Titel V Sv waarbij het gaat om een groep van personen die in een bepaald verband of wisselende verbanden systematisch misdaden beramen en plegen met ernstige gevolgen voor de samenleving, en die door de wijze waarop dat plaatsvindt zulk een bedreiging vormt dat zij zelfstandig onderzoek rechtvaardigt. *Kamerstukken II*, 1996/97, 25 403, nr. 3, p. 58.
4. *Kamerstukken II*, 1996/97, 25 403, nr. 3, p. 57.
5. *Kamerstukken II*, 1996/97, 25 403, nr. 3, p. 49.

van het onderzoek. Het betreft een grote verzameling burgers ten aanzien van wie geen verdenking en zelfs geen beeld van een concreet misdrijf hoeft te bestaan. Voorts verschilt de aard van het onderzoek; het betreft gegevensvergelijking en -vergarings, waarbij geen bijzondere opsporingsbevoegdheden worden toegepast.

#### **Toepassing gericht dataminingonderzoek**

Voor het uitvoeren van een gericht dataminingonderzoek kan aansluiting worden gezocht bij de regeling van het verkennend onderzoek van art. 126gg Sv. Zoals de naam al aangeeft heeft dit onderzoek een verkennende functie waarbij informatie wordt verzameld, veredeld en geanalyseerd, hetgeen uiteindelijk kan resulteren in concrete feiten als een verdenking. Op basis van art. 126gg lid 2 Sv is het mogelijk dat wordt gekoppeld met nader aan te geven openbare registers die bij wet zijn ingesteld. Hoewel deze gegevens voor een ander doel zijn vastgelegd mogen zij worden verwerkt, indien dit noodzakelijk is voor de uitvoering van het onderzoek<sup>6</sup>. Datamining heeft grotendeels dezelfde functie als een verkennend onderzoek, te weten het bijeenbrengen van gegevens om daaruit concrete kennis te destilleren die eventueel aanleiding vormt voor verder onderzoek. Wanneer een verkennend onderzoek een concrete verdenking oplevert eindigt het verkennend onderzoek en neemt het opsporingsonderzoek een aanvang. Met behulp van gericht dataminingonderzoek kan daarom ook uitvoering worden gegeven aan een verkennend onderzoek. Wanneer bijvoorbeeld aanwijzingen bestaan dat via internet gestolen goederen worden aangeboden en verhandeld, kan dat aanleiding zijn om hiernaar een gericht onderzoek in te stellen. Daarbij kan worden uitgegaan van het misdrijf heling (art. 416 Sv), waarop een gevangenisstraf van maximaal vier jaren staat. In het kader van het betreffende verkennende onderzoek kunnen gegevens over veilingsites, alsook de personen die daarmee in verband kunnen worden gebracht, worden vastgelegd en geanalyseerd. Daarbij worden ook gegevens over onverdachte personen verwerkt. Het is daarom van belang dat bij aanvang van het onderzoek vaststaat, op welke wijze het onderzoek wordt verricht en welke internetsites bij het onderzoek worden betrokken. Wanneer inderdaad blijkt van strafbare handelingen kan een opsporingsonderzoek worden ingesteld. Een ander voorbeeld van een situatie waarin een gericht dataminingonderzoek kan worden overwogen is de bestrijding van kinderporno (art. 240b Sv) waarop een gevangenisstraf van vier jaren staat. Indien er aanwijzingen zijn dat personen zich hieraan middels bepaalde internetsites of chatkanalen strafbaar maken, kan daar gericht dataminingonderzoek naar worden gedaan.

##### *10.2.1.1 Beperkingen van het verkennend onderzoek*

Een gericht dataminingonderzoek dat wordt uitgevoerd in het kader van een verkennend onderzoek wordt qua mogelijkheden beperkt door de daarvoor geldende voorwaarden.

---

6. *Kamerstukken II*, 1998/99, 26 410, nr. 3, p. 10-11.

Met het oog op de persoonlijke levenssfeer kan een verkennend onderzoek alleen worden ingesteld op bevel van de OvJ ter bestrijding van de zware criminaliteit waarbij bovendien sprake dient te zijn van een ernstige inbreuk op de rechtsorde. Hierbij kan het gaan om gepleegde feiten, maar ook om feiten die worden beraamd. Hoewel een gericht dataminingonderzoek van nut kan zijn voor de politietaak als geheel is, de toepassing ervan in het kader van art. 126gg Sv beperkt tot misdrijven. Bovendien blijkt uit het feit dat wordt gesproken over branches en sectoren dat een verkennend onderzoek een vrij ongegericht karakter heeft. Een gericht dataminingonderzoek, daarentegen, kan ook worden gebruikt bij onderzoek dat qua doelstelling en reikwijdte nader is gespecificeerd. Een andere beperkende factor is de voorwaarde dat de feiten, waarop een verkennend onderzoek ziet, dienen plaats te vinden binnen verzamelingen van personen. Zo is het op grond van art. 126gg Sv niet zonder meer mogelijk verkennend onderzoek te doen naar de teelt van softdrugs aan de hand van een aantal criteria als hoog water- en stroomverbruik in combinatie met een afwijkend uitgavenpatroon. In dat geval is geen sprake van een afgebakende groep waarop het onderzoek betrekking heeft. Een zodanig verkennend onderzoek zou wel denkbaar zijn ten aanzien van bijvoorbeeld een bepaald woonwagencamp<sup>7</sup>; in dat geval is namelijk wel sprake van een afgebakende groep van personen. Een ander nadeel van het verkennend onderzoek is de beperkte mogelijkheid tot gegevensverwerking. In dit verband zij gewezen op hetgeen in het wetsvoorstel 'Vorderen gegevens telecommunicatie' omtrent het verkennend onderzoek van art. 126gg Sv<sup>8</sup> wordt opgemerkt<sup>9</sup>. In het hierna volgende wordt ingegaan op de vraag, in hoeverre het daardoor mogelijk is om op efficiënte wijze uitvoering te geven aan een verkennend onderzoek.

### Oorspronkelijk wetsvoorstel

Het inmiddels in werking getreden wetsvoorstel 'Vorderen gegevens telecommunicatie'<sup>10</sup> voorziet onder meer in de mogelijkheid om gebruikersgegevens te verwerken betreffende naam, adres, postcode, woonplaats, nummer en soort dienst van personen die gebruik maken van telecommunicatienetwerken of -diensten<sup>11</sup>. In het rapport van de commissie Mevis inzake de strafvorderlijke gegevensvergaring in de informatiemaatschappij<sup>12</sup> worden die gebruikersgegevens ook als identificerende gegevens aangeduid. Hierna zal worden gesproken van naam-, adres-, en woonplaats-, ofwel NAW-gegevens. NAW-gegevens vormen een onmisbaar onderdeel van veel strafrechtelijk onderzoek. Zij stellen een opsporingsambtenaar in staat te bepalen, met welke persoon hij van doen heeft als hij beschikt over een bepaald nummer of adres. Men heeft bij de start van een onderzoek

7. Mits er is voldaan aan de overige voorwaarden voor het instellen van een verkennend onderzoek.

8. *Kamerstukken I*, 2002/03, 28 059, nr. 187.

9. Zie ook Sietsma 2004.

10. *Stb.* 2004, 105.

11. *Kamerstukken II*, 2001/02, 28 059, nr. 3, p. 1.

12. Commissie Mevis 2001, p. 9 en 51.

kennis van enkele feiten en personen en kan door het vergaren van aanvullende gegevens verbanden leggen. Daarnaast zijn NAW-gegevens vaak nodig, alvorens andere bevoegdheden als het vorderen van verkeersgegevens<sup>13</sup> en het opnemen van telecommunicatie kunnen worden toegepast<sup>14</sup>. Zowel bij opsporingsautoriteiten als bij de houders van NAW-gegevens bestond tot voor kort onduidelijkheid over de verwerking van die gegevens in het kader van de opsporingstaak. De term ‘verwerken’ sluit aan op de terminologie van de Wbp en ziet op elke handeling met betrekking tot NAW-gegevens. In beginsel is steeds een wettelijke grondslag vereist voor het gebruik van deze gegevens. Ook voor het vergaren van de gegevens dient een wettelijke basis aanwezig te zijn. Met de wet ‘Vorderen gegevens telecommunicatie’ heeft de wetgever tegemoet willen komen aan de daaraan klevende nadelen, zoals het ontbreken van een duidelijke wettelijke grondslag en de afhankelijkheid van opsporingsautoriteiten van de vrijwillige medewerking van de houder van gegevens. Bovendien zorgt de regeling ervoor dat niet die houder meer verantwoordelijk is voor de afweging die bij de verstrekking gemaakt dient te worden<sup>15</sup>, maar de opsporingsambtenaar die de verstrekking vordert<sup>16</sup>. Het oorspronkelijke wetsvoorstel, dat in een later stadium op een aantal essentiële punten is herzien, bevatte een bevoegdheid<sup>17</sup> tot het vorderen van NAW-gegevens, toe te kennen aan opsporingsambtenaren in het geval van verdenking van een strafbaar feit, ingeval van onderzoek naar het in georganiseerd verband beramen of plegen van misdrijven die een ernstige inbreuk op de rechtsorde opleveren, en aan de OvJ in het geval van een verkennend onderzoek. Binnen het proces van informatiegaring kon die bevoegdheid worden toegepast in het kader van het opsporingsonderzoek en het verkennend onderzoek. De wetgever geeft daarmee aan, dat de bevoegdheid tot het vorderen van NAW-gegevens onmisbaar is bij een verkennend onderzoek. Aangezien het onderzoek naar gegevens uit bestaande persoonsregistraties centraal staat, kunnen enkel goede resultaten worden verkregen wanneer ruimte aanwezig is voor het verkrijgen van dergelijke gegevens. Het vergaren van identificerende gegevens is daarbij van groot belang. Nu NAW-gegevens behoren tot een beperkte categorie gegevens en het verkennend onderzoek zich richt op aanwijzingen dat ernstige misdrijven worden beraamd of gepleegd, kan het belang van de opsporing zwaarder worden gewogen dan het belang van de bescherming van persoonsgegevens<sup>18</sup>.

13. Zie ook Asscher & Ekker 2003.

14. *Kamerstukken II*, 2001/02, 28 059, nr. 3, p. 6.

15. *Kamerstukken II*, 2001/02, 28 059, nr. 5, p. 4 en *Kamerstukken I*, 2003/04, 28 059, A, p. 11.

16. Ook de PEC achtte een duidelijke wettelijke normering terzake van de verstrekkingen op basis van het toenmalige art. 11 lid 2 Wpr gewenst (*Kamerstukken II*, 1995/96, 24 072, nrs. 10-11, p. 466). Het wetsvoorstel strekt mede tot uitvoering van deze aanbeveling van de *Parlementaire Enquêtecommissie Opsporingsmethoden*.

17. De bevoegdheid zou worden geregeld in de art. 126na, 126ua en 126gg lid 3 Sv, waarbij het steeds gaat om een vordering van gegevens van een aanbieder van een openbaar telecommunicatienetwerk of een openbare telecommunicatiedienst.

18. *Kamerstukken II*, 2001/02, 28 059, nr. 3, p. 11-12 en 20.

### Het aangepaste wetsvoorstel

Het wetsvoorstel zoals dat in het *Staatsblad*<sup>19</sup> is geplaatst werd uiteindelijk op een aantal essentiële punten herzien<sup>20</sup>. In de gewijzigde regeling is het opvragen van NAW-gegevens enkel mogelijk in het stadium van het opsporingsonderzoek. Bovendien mag de bevoegdheid slechts worden gebruikt bij (gepleegde) misdrijven of het in georganiseerd verband beramen of plegen van misdrijven die een ernstige inbreuk op de rechtsorde opleveren. De opvallendste aanpassing is dat bij een verkennend onderzoek geen NAW-gegevens mogen worden opgevraagd. De bevoegdheid tot het vorderen van NAW-gegevens wordt beperkt tot de gevallen van verdenking van een misdrijf (in plaats van een verdenking van een strafbaar feit) en wordt niet toegekend ten behoeve van het verkennend onderzoek. Deze beperking hangt volgens de wetgever samen met de afweging, voor de opsporing van welke strafbare feiten de bevoegdheid dient te kunnen worden toegepast. De vordering van NAW-gegevens is op zichzelf niet ingrijpend voor de persoonlijke levenssfeer; de toepassing van de bevoegdheid voor elk strafbaar feit voldoet echter niet aan het noodzakelijkheids criterium. Het individuele belang van de burger bij de bescherming van zijn persoonsgegevens dient, voor zover het gaat om strafbare feiten die geen misdrijven zijn, zwaarder te wegen dan het algemene belang van de opsporing, ook al zijn die gegevens op zichzelf niet ingrijpend voor de persoonlijke levenssfeer. Volgens verklaart de wetgever dat dit ook het geval is voor het verkennend onderzoek, maar aangezien een verkennend onderzoek alleen betrekking heeft op misdrijven lijkt geen grond aanwezig voor uitsluiting van de bevoegdheid voor een verkennend onderzoek<sup>21</sup>. Deze stap is des te opmerkelijker gezien de uitgebreide motivatie van de wetgever voor de introductie van de bevoegdheid voor juist in eerste instantie het verkennend onderzoek. Er wordt slechts opgemerkt dat op een andere plaats nog nader op het verkennend onderzoek wordt ingegaan; onduidelijk blijft waar dat dan is. Mogelijk wordt bedoeld op een passage verderop in de Nota, met betrekking tot het verslag<sup>22</sup> waar wordt ingegaan op de vraag of het vorderen van NAW-gegevens wel met voldoende waarborgen is omgeven; met het oog daarop wordt voorgesteld de bevoegdheid niet bij de opsporingsambtenaar neer te leggen, maar bij de OvJ. Volgens de wetgever dient het gewijzigde voorstel mede te worden uitgelegd in het licht van de behoefte aan voldoende waarborgen. In plaats van de bevoegdheid echter bij een hogere instantie neer te leggen, is gekozen voor het aanbrengen van inhoudelijke beperkingen in de vorm van inkrimping van de bevoegdheid. Deze inkrimping is des te opmerkelijker gezien het feit, dat in

19. *Stb.* 2004, 105.

20. *Kamerstukken I*, 2002 /03, 28 059, nr. 187.

21. Zie ook *Kamerstukken II*, 2001 /02, 28 059, nr. 5, p. 10. Ook kunnen ten behoeve van een verkennend onderzoek, bijvoorbeeld naar groepen gebruikers van internet, geen gebruikersgegevens worden gevorderd. Hierbij kan worden opgemerkt dat dit bij een toenemend gebruik van internet en het mobiele gebruik van Internet in de toekomst wellicht weer anders gewaardeerd moet worden.

22. *Kamerstukken II*, 2001 /02, 28 059, nr. 5, p. 21.

het oorspronkelijke wetsvoorstel de bevoegdheid tot vordering van NAW-gegevens in het kader van verkennend onderzoek al was toegekend aan de OvJ. Dit, in combinatie met de wijze waarop de gegevens in dat kader worden verwerkt, waarborgt in beginsel een verantwoorde verwerking<sup>23</sup>. Het blijft derhalve onduidelijk, waarom de bevoegdheid tot het vorderen van NAW-gegevens in het gewijzigde wetsvoorstel is ingeperkt voor het verkennend onderzoek, temeer daar de wetgever in eerste instantie met betrekking daarop stelt:

*‘Het verkennend onderzoek is bij uitstek onderzoek naar gegevens uit bestaande persoonsregistraties. Alleen wanneer er ruimte is dergelijke gegevens te verkrijgen, kan het tot goede resultaten leiden.’<sup>24</sup>*

Nu de bedoelde ruimte in de uiteindelijke wettelijke regeling ontbreekt kan worden geconcludeerd, dat het verkennend onderzoek in de huidige vorm eigenlijk een onbruikbaar instrument is. Dit lijkt een gemiste kans, nu het verkennend onderzoek – mede gezien de plaats ervan binnen het proces van informatiegaring – een belangrijke bijdrage kan leveren aan een succesvolle uitvoering van de opsporingstaak. Daarbij is het, zoals de wetgever in beginsel onderkent, van belang dat kan worden beschikt over NAW-gegevens. Het op vrijwillige basis opvragen van deze gegevens is ongewenst en onrechtmatig<sup>25</sup>. Gezien het doel van een verkennend onderzoek en het belang van de bestrijding van de zware criminaliteit in een vroegtijdig stadium, ligt een herziening van de reikwijdte en invulling van art. 126gg Sv dan ook in de rede.

#### *10.2.1.2 Datawarehouse*

Ook in het kader van een gericht dataminingonderzoek dienen de gegevens die daarbij worden verwerkt op een verantwoorde wijze te worden vastgelegd, vooral nu in het kader van een verkennend onderzoek in beginsel ook gegevens omtrent onverdachte personen kunnen worden verwerkt<sup>26</sup>. Met het oog hierop is bepaald dat de in het kader van een verkennend onderzoek verwerkte gegevens worden vastgelegd in een speciaal voor dat doel ingesteld tijdelijk register als bedoeld in art. 13 WPolr<sup>27</sup>. Een tijdelijk politieregister kan voor allerhande doeleinden worden aangelegd en is dus bij uitstek geschikt om te dienen als datawarehouse in het kader van een gericht dataminingonderzoek. Bovendien geldt dat met het bereiken van het doel van het dataminingonderzoek ook het onderzoek zelf eindigt. Dit doel kan worden bereikt wanneer het verkennend onderzoek concrete

---

23. *Kamerstukken II*, 2001 /02, 28 059, nr. 3, p. 12.

24. *Kamerstukken II*, 2001 /02, 28 059, nr. 3, p. 11.

25. Dit kan anders zijn wanneer het gaat om gegevens niet zijnde persoonsgegevens.

26. Met het oog op het standpunt van de wetgever inzake de wet ‘Vorderen gegevens telecommunicatie’ is het overigens de vraag, in hoeverre dit ook in de toekomst mogelijk blijft.

27. *Kamerstukken II*, 1996 /97, 25 403, nr. 3, p. 49 en 95.

aanwijzingen oplevert die aanleiding vormen tot het starten van een opsporingsonderzoek. Ook wanneer het verkennend onderzoek niets oplevert, vindt beëindiging plaats. Dit is gebaseerd op het, in het schriftelijk bevel dat aan een verkennend onderzoek ten grondslag ligt, opgenomen tijdpad. Op welk tijdstip redelijkerwijs kan worden gesteld dat het verkennend onderzoek niet tot resultaten leidt dient, al naar gelang de omstandigheden, per onderzoek te worden beoordeeld. Wanneer gegevens in een tijdelijk politieregister voldoen aan de criteria die andere registers stellen, kunnen zij naar die registers worden overgeheveld, anders dienen zij te worden vernietigd<sup>28</sup>. Zoals bleek in sectie 9.2 zijn de registratie- en analysefunctie bij een tijdelijk politieregister onlosmakelijk met elkaar verbonden. Registratie van gegevens vindt plaats om deze te kunnen analyseren, hetgeen weer noodzakelijk is ter realisatie van het doel waarvoor het tijdelijk register is aangelegd. Voor een gericht dataminingonderzoek betekent dit, dat een tijdelijk politieregister ook kan worden aangemerkt als datawarehouse<sup>29</sup>.

### Reglement

Een tijdelijk politieregister kent een tijdelijke ontheffing van de reglementspllicht. Een reglement is op grond van art. 13 lid 3 WPolr ook niet noodzakelijk om in het kader van een gericht dataminingonderzoek te kunnen koppelen. De uitzonderingsregeling voor een tijdelijk register is in de WPolr vooral opgenomen voor situaties waarin onmiddellijk politieoptreden is vereist en waarvoor de opslag van gegevens in het register zware criminaliteit (CIE-register) niet mogelijk dan wel minder opportuun is, omdat er geen aanwijzingen zijn die verband houden met de misdrijven waarvoor dit register is aangelegd. De noodzaak tot onmiddellijk optreden vereist een voorziening die de aanleg van een register mogelijk maakt, zonder dat eerst een reglement wordt opgesteld<sup>30</sup>. In beginsel is bij de aanleg van een tijdelijk politieregister in het kader van een gericht dataminingonderzoek geen sprake van een noodzaak tot onmiddellijk optreden. Desondanks kan de aanleg van een reglement om twee redenen onwenselijk zijn. Ten eerste is het onhaalbaar om in het kader van elk gericht dataminingonderzoek een apart reglement op te stellen. De procedure van art. 9 WPolr is hiervoor te tijdrovend en belemmert de uitoefening van de opsporingstaak. Ten tweede maakt het feit dat een tijdelijk politieregister voor allerhande onderzoek kan worden aangelegd het niet eenvoudig om in een specifiek reglement te voorzien. Omdat de aanwezigheid van een reglement toegevoegde waarde kan hebben voor een gericht dataminingonderzoek kan worden overwogen, gebruik te maken van het modelreglement<sup>31</sup> voor een tijdelijk politieregister. Omdat een gericht datamining-

28. Art. 8 BPolr bepaalt dat gegevens in tijdelijke registers vernietigd dienen te worden wanneer het doel waarvoor het register is aangelegd is bereikt, voor zover deze gegevens geen betekenis hebben voor een eventueel verder strafrechtelijk onderzoek in verband met het verkennend onderzoek.

29. Zie ook sectie 5.2.2.1.

30. *Kamerstukken II*, 1997/198, 25 398, nr. 6, p. 6.

31. *Stert. 11 juli 2003, nr. 131.*

onderzoek veelvuldig kan worden toegepast in de opsporingspraktijk ligt de keuze voor een modelreglement voor de hand.

### **Gebruik datawarehouse**

In dit onderzoek is er voortdurend op gewezen dat het met betrekking tot de gegevens in een datawarehouse wenselijk is, dat zij slechts (kunnen) worden verwerkt voor het doel waarvoor zij zijn vastgelegd. Bij een gericht dataminingonderzoek zijn de omstandigheden waaronder de verwerking plaatsvindt echter anders dan bij een ongericht dataminingonderzoek. In het kader van een gericht dataminingonderzoek zullen veelal nieuwe gegevens worden verwerkt die (nog) niet elders binnen het politieapparaat aanwezig zijn. Wanneer deze gegevens niet op een andere manier kunnen worden verkregen en bovendien van belang kunnen zijn voor ander gericht onderzoek (naar de zware criminaliteit), kan, teneinde deze gegevens op ruimere schaal te kunnen benutten, worden overwogen een ander verstrekkingenregime van toepassing te verklaren. Hierdoor kunnen deze, bijvoorbeeld door middel van verwijzingsindexen, veel effectiever worden verwerkt.

#### *10.2.2 Het opsporingsonderzoek*

Een gericht dataminingonderzoek dat plaatsvindt in het stadium van het opsporingsonderzoek dient te voldoen aan de voorwaarden van art. 132a Sv. Een opsporingsonderzoek is gericht op het nemen van strafvorderlijke beslissingen en vindt plaats onder leiding van de OvJ. Het kan worden gestart wanneer een redelijk vermoeden bestaat dat een strafbaar feit is begaan, waarbij het eender welke strafbare gedraging kan betreffen. Voorts kan een opsporingsonderzoek worden gestart bij een redelijk vermoeden dat in georganiseerd verband misdrijven worden beraamd of gepleegd als omschreven in art. 67 lid 1 Sv die, gezien hun aard of samenhang met andere misdrijven die in dat georganiseerd verband worden beraamd of gepleegd, een ernstige inbreuk op de rechtsorde opleveren. Hierbij is sprake van een proactief element, waarbij de mogelijkheid tot het doen van een gericht dataminingonderzoek is beperkt tot de zeer zware criminaliteit.

### **Toepassing gericht dataminingonderzoek**

In het kader van het opsporingsonderzoek zijn de mogelijkheden tot het doen van gericht dataminingonderzoek in beginsel ruimer dan bij het verkennend onderzoek van art. 126gg Sv. Bij een redelijk vermoeden dat een strafbaar feit is begaan maakt art. 132a Sv geen onderscheid tussen de fase, waarin sprake is van een redelijk vermoeden van een gepleegd strafbaar feit en waarbij sprake is van een verdenking, en de fase waarin sprake is van een redelijk vermoeden van schuld aan een gepleegd strafbaar feit waarbij er, naast een verdenking, een verdachte is. Dit verschil, dat wel werd gemaakt door de PEC<sup>32</sup>, is

---

32. Zie sectie 2.3.3.2.

van belang in het kader van het dataminingsproces. Wanneer er sprake is van een verdenking én een verdachte bestaat in beginsel geen behoefte meer aan dataminingonderzoek, maar aan verificatie. In het geval van een gepleegd strafbaar feit of een vermoeden dat dit is begaan, kan steeds een gericht dataminingonderzoek worden verricht ter opheldering van dat feit. Het gaat daarbij in beginsel om de politietaak in een bepaald geval, zoals bedoeld in art. 1 lid 1 onder *j* WPolr. Gericht dataminingonderzoek is niet alleen wenselijk wanneer een verdenking bestaat ten aanzien van een beperkte, aanwijsbare groep van personen, maar kan ook van belang zijn voor opsporingsactiviteiten ten aanzien van politieonderzoek in het algemeen<sup>33</sup>. Het kan daarbij een zaak betreffen waarbij opsporingsautoriteiten worden geconfronteerd met een grote hoeveelheid gegevens of een zaak, waarbij de behoefte bestaat om zo breed mogelijk naar aanwijzingen te zoeken. In dit derde stadium van het proces van informatiegaring kan, al naar gelang de aard van de verdenking, gebruik worden gemaakt van ingrijpender opsporingsmethoden. Indien een gericht dataminingonderzoek plaatsvindt in het kader van een opsporingsonderzoek zijn de onderzoeksmogelijkheden ruimer dan in het kader van een verkennend onderzoek.

#### Datawarehouse

Gegevens omtrent personen die van belang zijn voor het opsporingsonderzoek kunnen in beginsel in een tijdelijk politieregister worden opgeslagen<sup>34</sup>. Dit blijkt ook uit art. 1 lid 1 onder *j* WPolr, waar wordt bepaald dat in het kader van de politietaak in een bepaald geval een tijdelijk politieregister als bedoeld in art. 13 WPolr wordt aangelegd. In sectie 9.6 bleek dat voor een algemene verbetering van de informatiepositie op het gebied van de zware criminaliteit gebruik kan worden gemaakt van een register zware criminaliteit. In dat geval gaat het om een ongericht dataminingonderzoek met betrekking tot dit politieregister, waarbij de mogelijkheden tot een analyse erg beperkt bleken. In het kader van de bestrijding van de zware criminaliteit kunnen er omstandigheden zijn waardoor een meer ingekaderde, en op het specifieke geval gerichte, registratie te prefereren is. Er kan dan voor de duur van het onderzoek een tijdelijk register worden aangelegd naar dat, naar tijd en ruimte omgrensde, geval. In dat register worden dan enkel die gegevens opgenomen die van betekenis kunnen zijn voor oplossing van dat bepaalde ernstige misdrijf. Wanneer het daarmee verband houdende opsporingsonderzoek tot een einde komt, kan het register vervolgens worden beëindigd<sup>35</sup>. In dit geval kan worden gesproken van een gericht dataminingonderzoek, waarbij wederom gebruik kan worden gemaakt van een tijdelijk politieregister om de gegevens in vast te leggen die in het kader

33. *Kamerstukken II*, 1995/96, 24 072, nr. 14, p. 357. 'Voor omvangrijke tactische rechercheonderzoeken wordt veelal een tijdelijk register aangelegd. In het tijdelijk register kunnen alle gegevens over personen en voorwerpen, die in de loop van het onderzoek naar voren komen, worden opgenomen'.

34. *Kamerstukken II*, 2001/02, 28 059, nr. 5, p. 6.

35. *Kamerstukken II*, 1997/98, 25 398, nr. 6, p. 10.

van dat onderzoek worden verwerkt. Voor het gebruik van een tijdelijk politieregister als datawarehouse zij verwezen naar hetgeen daaromtrent in sectie 10.2.1.2 is opgemerkt.

### *10.2.3 Toepassingsmogelijkheden van het gerichte dataminingonderzoek*

Een gericht dataminingonderzoek biedt verschillende mogelijkheden ter verbetering van de informatiepositie. Voor een overzicht speelt onder meer de aard van de verdenking een rol, waarbij kan worden onderscheiden naar een situatie waarbij sprake is van:

- Criterion A: feiten of omstandigheden waaruit aanwijzingen voortvloeien (verkenkend onderzoek);
- Criterion B: een redelijk vermoeden (opsporingsonderzoek).

Hieronder wordt, al naar gelang de aard van de verdenking, aangegeven wanneer een gericht dataminingonderzoek mogelijk is. Daarbij wordt ingegaan op proactief onderzoek en onderzoek naar feiten die al zijn gepleegd.

#### **Criterion A**

- Proactief: in het geval van misdrijven die worden beraamd binnen verzamelingen van personen en die, gezien hun aard of de samenhang met andere binnen die groep gepleegde of beraamde misdrijven, een ernstige inbreuk op de rechtsorde opleveren.
- Gepleegde feiten: in het geval van misdrijven die zijn gepleegd binnen verzamelingen van personen en die, gezien hun aard of de samenhang met andere binnen die groep gepleegde misdrijven, een ernstige inbreuk op de rechtsorde opleveren.

#### **Criterion B**

- Proactief: in het geval van misdrijven die in georganiseerd verband worden beraamd en die, gezien hun aard of samenhang met andere misdrijven die in dat georganiseerd verband worden beraamd of gepleegd, een ernstige inbreuk op de rechtsorde opleveren.
- Gepleegde feiten: ieder gepleegd strafbaar feit.

De mogelijkheden tot het verrichten van een gericht dataminingonderzoek zijn het grootst wanneer is voldaan aan criterium B; het regime van dat criterium is namelijk strenger dan dat van A, zodat van beide mogelijkheden gebruik kan worden gemaakt. Vanwege onder meer de toenemende dreiging van het terrorisme lijkt proactief onderzoek een onmisbaar instrument voor opsporingsautoriteiten. Wanneer het gaat om het beramen van een aanslag lijkt daartoe binnen het proces van informatiegaring de mogelijkheid te ontbreken. Het voorbereiden van een misdrijf is echter een strafbaar feit op zich<sup>36</sup> en derhalve zal proactief onderzoek in de praktijk wel degelijk tot de mogelijkhe-

---

36. Art. 45 en 46 Sr.

den behoren. Gericht dataminingonderzoek naar nog te plegen strafbare gedragingen is in beginsel alleen mogelijk wanneer het gaat om de zware criminaliteit. Deze beperking met betrekking tot het onderzoeksterrein is van essentieel belang met het oog op de bescherming van de persoonlijke levenssfeer. Wanneer deze ontbreekt zullen onschuldige burgers onderwerp gaan uitmaken van politieel optreden, zonder dat zij daartoe enige aanleiding hebben gegeven. Aangezien de beperking tot de zware criminaliteit die mogelijkheid niet helemaal uitsluit, dienen dergelijke inbreuken alleen in uiterste noodzaak plaats te vinden en zal de inbreuk op de persoonlijke levenssfeer tot een minimum beperkt moeten blijven. Zo is gericht dataminingonderzoek bij de aanpak van de verspreiding van kinderporno op het internet slechts mogelijk, wanneer dat onderzoek zich beperkt tot een bepaalde groep van personen.

De ruime toepassingsmogelijkheden van een gericht dataminingonderzoek zijn mede terug te leiden tot de wijze waarop de gegevens in het kader van dat onderzoek worden opgeslagen. De ruime registratie- en analysefunctie van een tijdelijk politieregister, in combinatie met de beperkte mogelijkheid om dit register te raadplegen, maakt het geschikt voor met name deze vorm van dataminingonderzoek. Binnen de grenzen van de WPolr en het BPolr kunnen in het kader van een gericht dataminingonderzoek allerhande gegevens worden verwerkt. Daarbij waarborgt het verstrekkingenregime van het tijdelijk register dat de gegevens (in het datawarehouse) slechts worden verwerkt voor het doel waarvoor zij zijn vastgelegd, namelijk het dataminingonderzoek<sup>37</sup>.

### 10.3 Gericht dataminingonderzoek en het tijdelijke politieregister

Bij een gericht dataminingonderzoek gaat het, in tegenstelling tot een ongericht dataminingonderzoek, niet om een algemene verbetering van de informatiepositie van een bestaand register, maar om de verbetering van de informatiepositie van een nieuw register dat is aangelegd in het kader van een bepaald geval<sup>38</sup>. Laatstbedoeld register is een tijdelijk politieregister dat tevens fungeert als datawarehouse<sup>39</sup>. In sectie 10.2.1.2 bleek, dat het bijzondere politieregister daarvoor uitermate geschikt is. In het navolgende worden de mogelijkheden onderzocht van een gericht dataminingonderzoek (dat steeds betrekking heeft op een tijdelijk politieregister) en wel onder de volgende omstandigheden:

- er wordt geen gebruik gemaakt van externe gegevens;

37. *Kamerstukken II*, 1997/98, 25 398, nr. 6, p. 5. ‘De verstrekkingenregimes van het hulpverleningsregister, het tijdelijk register, het MOT-register en het vaststellingsregister hebben met elkaar gemeen, dat in beginsel alleen uit deze registers informatie kan worden verstrekt voor het doel waarvoor het register is aangelegd. De reden daarvoor moet, zoals reeds is aangegeven, worden gevonden in aard en doel van de opgeslagen informatie.’

38. Er is in beginsel geen sprake van een basisregister, zie hieromtrent sectie 5.2.1.

39. Zie ook sectie 9.3.

- er wordt gebruik gemaakt van externe gegevens die niet afkomstig zijn uit een politieregister;
- er wordt gebruik gemaakt van externe gegevens afkomstig uit een gewoon politieregister;
- er wordt gebruik gemaakt van externe gegevens afkomstig uit een bijzonder politieregister.

### *10.3.1 Geen gebruik van externe gegevens*

Een gericht dataminingonderzoek met betrekking tot een tijdelijk politieregister is in eerste instantie niet mogelijk zonder dat daarbij gebruik wordt gemaakt van externe gegevens. In het beginstadium van het onderzoek zijn eenvoudigweg nog geen gegevens in het tijdelijk register voorhanden om te kunnen analyseren. In een later stadium van een gericht dataminingonderzoek ligt de nadruk minder op het vergaren van gegevens en meer op het analyseren van de reeds vergaarde gegevens. Hiermee is de verwerking van externe gegevens een essentiële voorwaarde om een gericht dataminingonderzoek te kunnen verrichten.

Bij een gericht dataminingonderzoek gelden dezelfde algemene voorwaarden als waarvan sprake is bij de ongerichte dataminingsvariant<sup>40</sup>. Het onderzoek dient noodzakelijk te zijn voor een goede uitvoering van de politietaak en rekening dient te worden gehouden met het doelbindingsbeginsel. Nu een gericht dataminingonderzoek geen betrekking heeft op een bestaand politieregister is het niet noodzakelijk dat het onderzoek wordt uitgevoerd door, dan wel onder het gezag van, de beheerder van het politieregister. Bij een ongericht dataminingonderzoek is deze voorwaarde wel van belang, omdat het al dan niet van toepassing zijn van het verstrekkingenregime van het basisregister daarmee samenhangt. Bij gericht dataminingonderzoek is in beginsel geen sprake van een basisregister. Het van toepassing zijnde verstrekkingenregime is het tijdelijk politieregister (het datawarehouse), ongeacht wie het gerichte dataminingonderzoek uitvoert.

### *10.3.2 Gebruik van niet uit een politieregister afkomstige gegevens*

Externe gegevens van buiten de politieke sfeer vormen een belangrijke informatiebron bij een gericht dataminingonderzoek. Het gebruik van deze gegevens wordt beperkt door het noodzakelijkheids criterium en het doelbindingsbeginsel. Het uitgangspunt dat een verwerking van persoonsgegevens in beginsel alleen noodzakelijk is bij de bestrijding van misdrijven impliceert, dat persoonsgegevens niet kunnen worden verwerkt in het kader van een gericht dataminingonderzoek dat geen betrekking heeft op de bestrijding van de zware criminaliteit. Terwijl het gebruik van persoonsgegevens in het kader van een verkennend onderzoek steeds mogelijk is, ligt dit anders bij onderzoek dat plaatsvindt in

---

40. *Kamerstukken II*, 1997/98, 25 398, nr. 6, p. 7.

het kader van een opsporingsonderzoek. Dat kan namelijk betrekking hebben op allereerste (gepleegde) strafbare feiten. Op grond van art. 4 WPolr kunnen gegevens in een tijdelijk politieregister enkel worden verwerkt met het oog op het doel van het onderzoek waarvoor dat register is aangelegd. Wanneer het tijdelijk politieregister is gelieerd aan de bestrijding van de zware criminaliteit is minder snel sprake van een beperkende werking van het doelbindingsbeginsel<sup>41</sup>. Andere factoren die van invloed zijn op het gebruik van externe gegevens van buiten de politieke sfeer in het kader van een gericht dataminingonderzoek zijn de aard van dat onderzoek, de koppelingsregeling en de aard van de externe gegevens.

#### *10.3.2.1 De aard van het gerichte dataminingonderzoek*

Wanneer gegevens worden vergeleken van en kennis wordt vergaard over personen ten aanzien van wie geen feiten of omstandigheden bekend zijn dat zij zich bezig houden met strafbare feiten, is er sprake van een ingrijpende bevoegdheid<sup>42</sup>. Voor een dergelijke verwerking in het kader van een gericht dataminingonderzoek dient een wettelijke grondslag aanwezig te zijn die voorziet in voldoende waarborgen ter bescherming van de privacy van de burger. Met het oog op de aard van een gericht dataminingonderzoek lijkt een dergelijke regeling onmisbaar. In tegenstelling tot de ongerichte dataminingsvariant, wordt bij een gericht dataminingonderzoek actief en gericht gezocht naar externe gegevens. Dit wordt onder meer gerechtvaardigd door de aard van de verdenking en de wijze waarop de vergaarde gegevens worden vastgelegd. De verwerking van externe gegevens in het kader van een gericht dataminingonderzoek wordt niet beperkt tot eigen kennis of informatie, verkregen door het openhouden van ogen en oren dan wel door tips en meldingen. Afhankelijk van de ruimte die een wettelijke grondslag biedt, kan in beginsel gebruik worden gemaakt van alle denkbare bronnen.

#### *10.3.2.2 Koppeling*

Ingeval van een verwerking van externe gegevens middels een koppeling in de zin van art. 6 WPolr<sup>43</sup>, mag een tijdelijk politieregister alleen worden gekoppeld met een ander politieregister of een persoonsregistratie van het Rijk, provincies, gemeenten en andere openbare lichamen met inbegrip van de daaronder ressorterende diensten, instellingen en bedrijven<sup>44</sup>. Dit impliceert een vergaande beperking van het gebruik van externe gegevensverzamelingen. Daarom is een koppeling van registers en bestanden die het karakter heeft van de zogeheten 'Rasterfahndung'<sup>45</sup> naar huidig recht alleen toegestaan tussen

---

41. *Kamerstukken II*, 1997/98, 25 880, nr. 1-2, p. 83.

42. *Kamerstukken II*, 1997/98, 25 880, nr. 1-2, p. 83.

43. Indien de externe gegevens tenminste tot een zelfstandige gegevensverzameling behoren.

44. Zoals bedoeld in art. 17, aanhef en onder *a* Wpr.

45. Zie sectie 1.3.4.

politierregisters en registers in de publieke sector. De wetgever geeft aan dat ‘Rasterfahndung’ als opsporingsmethode genormeerd dient te worden in het Wetboek van Strafvordering en er toestemming dient te zijn van de OvJ. De koppeling van politierregisters met registers uit de niet-publieke sector is naar huidig recht voor opsporingsdoeleinden niet toegestaan. Dit dient volgens de wetgever zo te blijven. Ook het ‘ruilen’ van gesloten informatie uit politierregisters met derden (als particuliere recherchebureaus) dient expliciet verboden te worden<sup>46</sup>. Wanneer externe gegevens worden vastgelegd in een tijdelijk politieregister dient die registratie, en daarmee het gebruik van de externe gegevens, noodzakelijk te zijn voor het doel van het tijdelijk politieregister<sup>47</sup>. Aangezien de doeleinden van een tijdelijk register zo verschillend kunnen zijn, dient dit per geval te worden beoordeeld. De doelbinding wordt nogmaals bevestigd in het BPolr waar wordt bepaald, dat een tijdelijk register slechts met een ander register kan worden gekoppeld voor zover dit noodzakelijk is voor het doel waarvoor het tijdelijk register is aangelegd.

#### *10.3.2.3 Vrijwillige verstrekking*

Evenals bij een verbetering van de informatiepositie van een voorlopig politieregister, kunnen in een tijdelijk politieregister, aangelegd in het kader van een gericht dataminingonderzoek, vrijwillig verstrekte tips en meldingen worden vastgelegd. In het kader van een gericht onderzoek is het wenselijk dat degene die het onderzoek uitvoert zelf ook om die gegevens kan verzoeken. Hiervoor dient dan wel een wettelijke grondslag te zijn, vooral wanneer het verzoek plaatsvindt voor een ander doel dan waarvoor de gegevens in eerste instantie zijn vastgelegd. De wetgever is, naar aanleiding van de bevindingen van de commissie Mevis, doende hierin te voorzien<sup>48</sup>.

#### *10.3.2.4 Gebruik van gegevens uit openbare registers*

Het gebruik van gegevens uit openbare registers ten behoeve van de opsporing is enkel mogelijk bij een verkennend onderzoek, een verdenking of een andere uitvoering van de politietaak in een bepaald geval<sup>49</sup>. Vergaring van gegevens over een onbepaalde groep burgers voor algemene politieke doeleinden is onwenselijk<sup>50</sup>. Aangezien het bij een gericht dataminingonderzoek gaat om een verbetering van de informatiepositie in een bepaald geval, kan gebruik worden gemaakt van gegevens uit openbare registers.

### **Resumerend**

In het kader van een gericht dataminingonderzoek kan op ruime schaal gebruik worden gemaakt van externe gegevens van buiten de politieke levenssfeer. Dit geldt zeker wanneer

---

46. *Kamerstukken II*, 1995/196, 24 072, nr. 46, p. 16.

47. Art. 4 lid 2 WPolr.

48. Zie in dit verband ook *Kamerstukken* 29 441, 28 353 en 28 059.

49. *Kamerstukken II*, 1998/199, 26 410, nr. 3.

50. *Kamerstukken II*, 1998/199, 26 410, nr. 3, p. 11.

dat onderzoek samenhangt met de bestrijding van de zware criminaliteit. De aard van de verdenking bij een gericht dataminingonderzoek rechtvaardigt dat actief en gericht kan worden gezocht naar externe gegevens. Wanneer daarbij persoonsgegevens worden verwerkt dient daarvoor wel steeds een wettelijke grondslag aanwezig te zijn.

### *10.3.3 Het gebruik van gegevens uit een gewoon politieregister*

Het ligt voor de hand dat in het kader van een gericht dataminingonderzoek ook gebruik wordt gemaakt van gegevens die al binnen het politieapparaat aanwezig zijn. Zeker in het kader van deze dataminingsvariant lijkt optimaal gebruik te kunnen worden gemaakt van het vrije verkeer van gegevens dat van toepassing is op de informatie in de gewone politieregisters. In deze sectie wordt onderzocht op welke wijze daarbij rekening dient te worden gehouden met de beperkingen die gelden voor het gebruik daarvan.

#### *10.3.3.1 De doelbinding*

Wanneer in het kader van een gericht dataminingonderzoek gegevens uit een gewoon politieregister in een tijdelijk register worden vastgelegd, dient dat noodzakelijk te zijn voor het doel van het tijdelijke politieregister. De gewone politieregisters dienen in beginsel de algemene politietaak, op grond waarvan ook een verwerking ten behoeve van een gericht dataminingonderzoek mogelijk is. Met betrekking tot de verwerking van gegevens in het hulpverleningsregister en het register-MOT is voorzien in een directe doelbinding<sup>51</sup>, waardoor die verwerking is beperkt.

#### **Het hulpverleningsregister en het register-MOT**

Uit het hulpverleningsregister worden slechts gegevens verstrekt voor de doeleinden waarvoor het is aangelegd, tenzij een geregistreerde, wanneer dat noodzakelijk is in het kader van een gericht dataminingonderzoek, uitdrukkelijk instemt met het gebruik van zijn of haar gegevens. Op grond hiervan is het niet uitgesloten dat in het kader van een gericht dataminingonderzoek, wanneer aan de overige voorwaarden voor een zodanige verwerking is voldaan, beperkt van dat register gebruik wordt gemaakt.

Ook voor het register-MOT geldt, dat een verstrekking daaruit slechts mogelijk is voor het doel waarvoor het is aangelegd. In art. 12 lid 1 onder *b* BPolr worden enkele uitzonderingen op die bepaling genoemd. Zo kunnen op grond van art. 15 lid 1 onder *a* WPolr gegevens worden verstrekt aan bijvoorbeeld de OvJ wanneer die redelijkerwijs van belang kunnen zijn ter voorkoming of opsporing van misdrijven als bedoeld in art. 1 lid 1 onder *k* WPolr. De OvJ kan op grond daarvan in het kader van een gericht dataminingonderzoek een verzoek tot informatie doen aan het Meldpunt.

---

51. Art. 12 BPolr.

#### *10.3.3.2 De aard van de politietaak*

Ook in het kader van een gericht dataminingonderzoek dient terughoudend te worden omgegaan met het gebruik van gegevens uit politieregisters die niet zijn aangelegd in het kader van de politietaak met betrekking tot de strafrechtelijke handhaving van de rechtsorde en politieregisters die in het geheel niet zijn aangelegd in het kader van de politietaak als omschreven in art. 2 Politiewet 1993. De laatste categorie kan alleen worden gebruikt onder de voorwaarden die gelden voor het gebruik van externe gegevens die afkomstig zijn van buiten de politieke sfeer.

#### **De handhaving van de openbare orde en de hulpverleningstaak**

Of in het kader van een gericht dataminingonderzoek gebruik kan worden gemaakt van het OOH-register hangt af van het doel waarvoor het tijdelijke politieregister is aangelegd. Wanneer het voor dat doel noodzakelijk is gebruik te maken van gegevens die in het kader van de handhaving van de openbare orde worden vastgelegd, is een verwerking denkbaar. Hoewel een hulpverleningsregister voor een afwijkende politietaak wordt aangelegd, kan het beperkt worden gebruikt in het kader van een gericht dataminingonderzoek wanneer er een aantoonbare noodzaak is om de gegevens in dat register voor een bepaald onderzoek te verwerken.

#### *10.3.3.3 Koppeling*

Wanneer ten behoeve van een gericht dataminingonderzoek wordt gekoppeld met gegevens in een gewoon politieregister dient rekening te worden gehouden met de daarvoor geldende aanvullende voorwaarden. De koppeling dient tenminste noodzakelijk te zijn voor een goede uitvoering van de politietaak voor zover het de strafrechtelijke handhaving van de rechtsorde betreft. Bovendien dient het reglement van het gewone politieregister in de mogelijkheid van een koppeling te voorzien.

#### *10.3.3.4 De aard van het gerichte dataminingonderzoek*

In beginsel is er niets dat het tijdelijk vastleggen van gegevens uit een gewoon politieregister in een tijdelijk politieregister in het kader van een gericht dataminingonderzoek in de weg staat. Door het beperkte verstrekkingenregime van een tijdelijk register blijft, in het geval van een verwerking, de bescherming van de persoonlijke levenssfeer (meer dan) gewaarborgd. De aard van een gericht dataminingonderzoek impliceert onder meer dat gericht in de gewone politieregisters kan worden gezocht, hetgeen een volledige koppeling met gewone politieregisters in beginsel overbodig maakt. Het gebruik van verwijzingsindexen is gewenst, aangezien daarbij niet meer gegevens worden verwerkt dan noodzakelijk is voor het doel van het dataminingonderzoek.

#### *10.3.3.5 Het BPS*

Voorals het BPS kan als gewoon politieregister zeer waardevolle informatie bevatten voor een gericht dataminingonderzoek. Ongeacht of het tijdelijk politieregister is aangelegd

in het kader van de bestrijding van de zware criminaliteit is het wenselijk, de gegevens in het BPS te toetsen op hun bruikbaarheid. Op deze wijze kunnen de gegevens in het BPS op zeer effectieve wijze operationeel worden gecheckt waarbij gegevens snel te bestemder plaatse komen. Deze toetsing van een tijdelijk politieregister aan het BPS is niet alleen mogelijk doordat de gegevens in het BPS gedurende vier maanden in aanmerking komen voor operationeel gebruik, maar ook vanwege het beperkte verstrekkingenregime van het tijdelijk politieregister. Ook hier heeft het gebruik van een verwijzindex de voorkeur.

### Resumerend

In het kader van een gericht dataminingonderzoek kan in beginsel steeds gebruik worden gemaakt van de gegevens in de gewone politieregisters wanneer dat noodzakelijk is voor het doel van het gerichte dataminingonderzoek. Opvallend is dat bij een gericht dataminingonderzoek onder bepaalde voorwaarden ook gebruik kan worden gemaakt van de gegevens in het hulpverleningsregister en het register-MOT.

## 10.4 Het gebruik van gegevens uit een bijzonder politieregister

In deze sectie zal voor elk van de bijzondere politieregisters worden onderzocht in hoeverre deze gebruikt kunnen worden in het kader van een gericht dataminingonderzoek.

### 10.4.1 Het gebruik van een tijdelijk politieregister

Het gebruik van gegevens uit een ander tijdelijk politieregister in het kader van een gericht dataminingonderzoek (met betrekking tot een bepaald tijdelijk politieregister) is niet vanzelfsprekend, doch hangt samen met een aantal, hierna te bespreken, factoren.

#### 10.4.1.1 De doelbinding

Gegevens in tijdelijke politieregisters zijn niet zonder meer onderling uitwisselbaar, aangezien die registers voor allerhande doeleinden kunnen worden aangelegd. Een verstrekking van gegevens uit een tijdelijk politieregister is in beginsel alleen mogelijk voor het doel waarvoor dat register is aangelegd. Wanneer een bepaald tijdelijk politieregister een (geheel) ander doel dient dan het tijdelijk politieregister dat in het kader van het gericht onderzoek is aangelegd en waaraan wordt verstrekt, is die verstrekking in strijd met de doelbinding. Ieder tijdelijk register heeft in beginsel een eigen, specifieke doelstelling. Verstrekking uit deze tijdelijke politieregisters vindt in beginsel enkel plaats ter verrijking van die registers zelf. De verstrekking in het kader van een gericht dataminingonderzoek vindt niet plaats voor het doel van het tijdelijk register *waaruit* wordt verstrekt maar voor het doel van het tijdelijk politieregister *waaraan* wordt verstrekt. Dit betekent dat een verstrekking op grond van art. 13 lid 2 WPolr in beginsel niet mogelijk is. Men kan zich afvragen in hoeverre deze vergaande beperking (nog) wenselijk is. In het kader van een gericht dataminingonderzoek verwerkte gegevens kunnen eveneens van belang zijn voor ander gericht dataminingonderzoek. Hoewel het de vraag is in hoeverre de verwerking die plaatsvindt in het kader van een MRO-bestand op grond van de huidige

wet- en regelgeving toelaatbaar is, komt dit register in beginsel reeds aan de genoemde problematiek tegemoet. Volledigheidshalve zij opgemerkt dat de gegevens die uit een ander tijdelijk politieregister zijn verstrekt worden vastgelegd in het register waarop het gerichte dataminingonderzoek betrekking heeft. Op grond van art. 4 lid 2 WPolr dient een zodanige registratie noodzakelijk te zijn voor het doel van het laatstgenoemde tijdelijke register. Dit betekent dat een eventueel gebruik van gegevens uit een ander tijdelijk politieregisters slechts mogelijk is indien dat noodzakelijk is voor het doel van het gerichte dataminingonderzoek. Daarvan zal met name sprake zijn wanneer het dataminingonderzoek ziet op de bestrijding van de zware criminaliteit.

#### *10.4.1.2 Koppeling*

Een koppeling tussen twee tijdelijke politieregisters dient noodzakelijk te zijn voor de politietaak en is op grond van art. 4 lid 2 BPolr slechts mogelijk voor zover dit noodzakelijk is voor het doel waarvoor het register is aangelegd. Bij een koppeling van twee tijdelijke politieregisters betekent dit dat de koppeling voor elk van deze registers afzonderlijk noodzakelijk dient te zijn voor de specifieke doeleinden waarvoor die registers zijn aangelegd. Met het oog op de in de voorgaande sectie besproken doelbinding blijkt dat niet steeds het geval te zijn. Gezien het beperkte verstrekkingenregime van een tijdelijk register zal, teneinde te kunnen beschikken over gegevens in een ander tijdelijk politieregister, een koppeling noodzakelijk zijn.

Uit de formulering van art. 4 lid 2 BPolr kan verder worden opgemaakt dat het initiatief tot een koppeling in beginsel dient uit te gaan van de beheerder van het tijdelijk politieregister, zo ook voor de beheerder van het tijdelijke politieregister waarop het gericht dataminingonderzoek betrekking heeft. Aangezien het hier echter gaat om een koppeling van twee tijdelijke politieregisters geldt art. 4 lid 2 BPolr tevens voor het tijdelijke politieregister waaruit de verstrekking plaatsvindt. Maar het initiatief tot koppeling ligt niet bij de beheerder van dat laatstgenoemde register, waardoor in beginsel niet wordt voldaan aan art. 4 lid 2 BPolr. Dit zal een koppeling in de weg staan.

#### *10.4.1.3 De aard van het gerichte dataminingonderzoek*

Met par. 3a WPolr heeft de wetgever beoogd het gebruik, de opslag en de verstrekking van zachte opsporingsinformatie nader te normeren. Nu in een tijdelijk politieregister zachte gegevens kunnen worden vastgelegd kent het een strikt verstrekkingenregime, dat het gebruik van de gegevens in dit register beperkt. Het is de vraag of de aard van de gegevens in een tijdelijk politieregister een zodanig strikt verstrekkingenregime onder alle omstandigheden noodzakelijk maakt.

De huidige WPolr maakt geen onderscheid tussen een tijdelijk register dat is aangelegd in het kader van de bestrijding van de zware criminaliteit of in het kader van de politietaak in een ander geval. De verwerking van persoonsgegevens in een tijdelijk politieregister is in beginsel slechts mogelijk in het kader van de bestrijding van de zware criminaliteit. Volgens de wetgever dient het individuele belang van de burger bij de

bescherming van zijn persoonsgegevens, voor zover het gaat om strafbare feiten die geen misdrijven zijn, zwaarder te wegen dan het algemene belang van de opsporing, ook al zijn die gegevens op zichzelf niet ingrijpend voor de persoonlijke levenssfeer<sup>52</sup>. Ook wanneer geen gebruik wordt gemaakt van zachte gegevens zijn de gegevens in een tijdelijk politieregister enkel beschikbaar voor het onderzoek waartoe dat register is aangelegd. Bij het ontbreken van zachte gegevens lijkt het strenge verstrekkingenregime echter niet direct noodzakelijk te zijn. Daarom kan worden overwogen om een tijdelijk register alleen aan te leggen voor de politietaak in een bepaald geval (of verkennend onderzoek) voor zover het de zware criminaliteit betreft. In alle andere gevallen zou een gewoon politieregister kunnen worden gebruikt, dat immers wel bestemd is voor operationeel gebruik. De reden waarom een koppeling tussen verschillende tijdelijke politieregisters niet mogelijk is betreft niet het verstrekkingenregime – beide zijn identiek – maar de verschillende doeleinden waarvoor een tijdelijk politieregister kan worden aangelegd. Afhankelijk van het soort onderzoek waarvoor het tijdelijke politieregister wordt aangelegd kan daarom worden volstaan met de doelbinding als beperkende factor. In dat geval zou een koppeling tussen verschillende tijdelijke politieregisters mogelijk zijn wanneer zij dezelfde doelstelling hebben, te weten de bestrijding van de zware criminaliteit.

### Resumerend

Onder de huidige wet- en regelgeving staat het verstrekkingenregime van een tijdelijk politieregister een koppeling van verschillende tijdelijke politieregisters in beginsel in de weg. Het is de vraag of dit strikte verstrekkingenregime steeds noodzakelijk is. Wanneer het gebruik van gegevens in andere tijdelijke registers wenselijk wordt geacht, zou daarvoor gebruik kunnen worden gemaakt van verwijzindexen. In het geval van de tijdelijke politieregisters zij gewezen op het MRO-bestand dat een overzicht verschaft van alle rechercheonderzoeken als bedoeld in de art. 126gg en 132a Sv en dat bijdraagt aan de informatievoorziening in het kader van de uitvoering van art. 2 Politiewet 1993. In beginsel dient daarvoor eerst een wettelijke grondslag te worden gecreëerd.

## 10.5 Het gebruik van een voorlopig politieregister

In deze sectie wordt met betrekking tot de gegevens in een voorlopig politieregister onderzocht of deze in aanmerking komen om te worden verwerkt in het kader van een gericht dataminingonderzoek.

### 10.5.1 De doelbinding

Uit een voorlopig politieregister worden gegevens verstrekt voor het doel waarvoor het register is aangelegd en voor zover de gegevens benodigd zijn ter identificatie. Een zodanige verstrekking wordt op grond van art. 13b lid 3 WPolr niet in enig ander register

52. *Kamerstukken II*, 2001 /02, 28 059, nr. 5, p.10.

vastgelegd. Een verstrekking ten behoeve van een tijdelijk politieregister in het kader van een gericht dataminingonderzoek lijkt daarom niet mogelijk. Er kunnen uit een voorlopig politieregister echter ook gegevens worden verstrekt ten behoeve van de opname in een ander bijzonder politieregister. Het is de vraag of op grond daarvan een verstrekking aan een tijdelijk register mogelijk is. In tegenstelling tot een register zware criminaliteit en een voorlopig politieregister ontbeert een tijdelijk politieregister een vaste doelstelling. Bovendien gaat de registratiefunctie van een tijdelijk politieregister hand in hand met de analysefunctie van dat register. Voor een verstrekking uit een voorlopig politieregister ten behoeve van opname in een tijdelijk politieregister dienen de verstrekte gegevens als zelfstandig subject in aanmerking te komen voor een registratie in het tijdelijke politieregister. Als gevolg daarvan is een zodanige verstrekking mogelijk, wanneer die noodzakelijk is voor het doel van het tijdelijke politieregister, ofwel het gerichte dataminingonderzoek. De noodzaak vloeit ook voort uit art. 4 lid 2 WPolr, op grond waarvan een registratie van de verstrekte gegevens in het tijdelijke politieregister noodzakelijk dient te zijn voor het doel van dat register.

#### *10.5.2 Koppeling*

Niet alleen de registratie in, maar ook de koppeling met een tijdelijk politieregister dient noodzakelijk te zijn voor het doel van dat register. In beginsel zal hiervan sprake zijn nu ook het initiatief tot de koppeling uitgaat van de beheerder van het tijdelijke politieregister zelf. Aangezien de beheerder van een voorlopig politieregister in beginsel geen toegang heeft tot de gegevens in een tijdelijk politieregister<sup>53</sup> is het wenselijk, dat de beheerder van een tijdelijk register over de gegevens in een voorlopig politieregister kan beschikken. Voor een koppeling van deze twee politieregisters dient het modelreglement van het voorlopige politieregister in deze mogelijkheid te voorzien. Op grond van art. 14 van het modelreglement van een voorlopig politieregister kan dit register worden gekoppeld met een ander bijzonder politieregister voor zover dat noodzakelijk is voor het doel van het voorlopige politieregister. In beginsel zal een koppeling van een voorlopig met een tijdelijk politieregister noodzakelijk zijn voor het doel van het voorlopige register, wanneer het dataminingonderzoek ziet op een verbetering van de informatiepositie daarvan<sup>54</sup>. In dat geval vindt geen verstrekking plaats uit het voorlopige politieregister. Een gericht dataminingonderzoek heeft echter betrekking op de informatiepositie van een tijdelijk politieregister. In dat geval vindt een verstrekking plaats uit het voorlopige politieregister, die bovendien in beginsel niet noodzakelijk is voor het doel van het voorlopige politieregister. Vanwege het modelreglement van een voorlopig politieregister is een koppeling daarmee niet mogelijk.

---

53. Zie sectie 9.5.7.

54. Zie sectie 9.5.4.1 onder het kopje *Koppeling*. Wanneer een tijdelijk politieregister is aangelegd in het kader van de bestrijding van de zware criminaliteit zal in beginsel aan deze voorwaarde (welke overeenkomt met art. 4 lid 2 WPolr) zijn voldaan.

### *10.5.3 De aard van het gerichte dataminingonderzoek*

Gegevens in een voorlopig politieregister kunnen betrekking hebben op onschuldige personen. Een verwerking van die gegevens is alleen gerechtvaardigd indien het doel van het inbreukmakende onderzoek opweegt tegen de ernst van de inbreuk. Dit zal betekenen dat een verstrekking uit een voorlopig politieregister in het kader van een gericht dataminingonderzoek in beginsel slechts mogelijk is, wanneer dat dataminingonderzoek is gerelateerd aan de bestrijding van de zware criminaliteit. Hoewel een tijdelijk en een voorlopig politieregister eenzelfde verstrekkingenregime kennen, kan een tijdelijk politieregister voor zeer uiteenlopende onderzoeken worden aangelegd. Het is onwenselijk dat gegevens in een voorlopig politieregister middels een verstrekking ook kunnen worden gebruikt voor andere doeleinden dan de bestrijding van de zware criminaliteit. Overigens kan ten behoeve van een tijdelijk politieregister (of een gericht dataminingonderzoek) dat niet is gelieerd aan de zware criminaliteit geen gebruik worden gemaakt van zachte gegevens uit een voorlopig politieregister. Op grond van art. 4 lid 2 BPolr en art. 4 lid 2 WPolr kunnen gegevens uit een voorlopig politieregister slechts worden verwerkt indien dat noodzakelijk is voor het doel van het gerichte dataminingonderzoek. Indien dat doel niet samenhangt met dat van een voorlopig politieregister, is een verwerking van gegevens uit dit register in beginsel niet toegestaan.

In dit verband zij ook gewezen op de situatie waarbij gegevens uit een voorlopig politieregister zijn verstrekt aan en geregistreerd in een tijdelijk register. Wanneer gegevens in dat tijdelijk register (datawarehouse) vervolgens via een vermelding in een MRO-bestand beschikbaar komen voor operationeel gebruik dient te worden voorkomen, dat de uit het voorlopige politieregister verstrekte gegevens daarvan ook deel uitmaken. Het is immers onwenselijk dat die gegevens beschikbaar komen voor operationeel gebruik. Bovendien is het ten aanzien van die gegevens niet noodzakelijk dat zij uit een datawarehouse kunnen worden opgevraagd. Daarvoor kan ook een verzoek worden gedaan aan het voorlopige politieregister zelf, waarbij het verstrekkingenregime van dit register bepaalt of een verstrekking al dan niet mogelijk is.

#### **Resumerend**

Het gebruik van een voorlopig politieregister in het kader van een gericht dataminingonderzoek is in beginsel niet mogelijk, aangezien het modelreglement van een voorlopig politieregister een koppeling in de weg staat. Hoewel de gegevens in een voorlopig politieregister van groot belang kunnen zijn bij het doen van gericht dataminingonderzoek dat is gelieerd aan de zware criminaliteit, bestaat voor de beheerder van het voorlopige politieregister geen directe noodzaak om de gegevens ook daadwerkelijk te verstrekken en zullen de gegevens niet kunnen worden gebruikt.

### 10.6 Het gebruik van het register zware criminaliteit

Tot slot wordt onderzocht of in het kader van een gericht dataminingonderzoek gebruik kan worden gemaakt van de gegevens in een register zware criminaliteit. Daarbij zal, waar nodig, worden onderscheiden naar gegevens in een register zware criminaliteit betreffende:

- 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 beramen of plegen van misdrijven als bedoeld onder *a*;
- c. personen die in een bepaalde relatie staan tot degenen, bedoeld onder *a* en *b*.

#### 10.6.1 De doelbinding

Hoewel gegevens in het register zware criminaliteit zijn bestemd voor operationeel gebruik, dienen zij te worden verwerkt op een wijze die zoveel mogelijk in overeenstemming is met het doel waarvoor zij zijn geregistreerd<sup>55</sup>. Het gebruik van een register zware criminaliteit biedt daarom met name mogelijkheden voor gericht dataminingonderzoek dat is gelieerd aan de bestrijding van de zware criminaliteit. Een registratie van gegevens uit een register zware criminaliteit in een tijdelijk politieregister dient bovendien op grond van art. 4 lid 2 WPolr noodzakelijk te zijn voor het doel van het tijdelijke politieregister. Op grond daarvan kan in beginsel slechts gebruik worden gemaakt van gegevens uit een register zware criminaliteit, indien het doel van het gericht dataminingonderzoek samenhangt met de zware criminaliteit. Dit geldt vooral voor de gegevens in een register zware criminaliteit die tot de categorieën *a* en *b* behoren. Op de gegevens in categorie *c* is een stringenter verstrekkingenregime van toepassing.

#### Doelbinding gegevens categorie *c*

Op een verstrekking van de gegevens in een register zware criminaliteit die behoren tot categorie *c* is het verstrekkingenregime van een voorlopig politieregister van toepassing. Eerder bleek het mogelijk de gegevens in categorie *c* te vergelijken met gegevens uit andere politieregisters wanneer een contactpersoon daartoe zelf aanleiding geeft<sup>56</sup>. In dat geval komt die persoon in aanmerking voor opname als zelfstandig subject in een voorlopig register. Verstrekking van gegevens behorende tot categorie *c* in een register zware criminaliteit ten behoeve van een ander bijzonder politieregister is echter ook mogelijk op grond van art. 13*b* lid 2, tweede volzin WPolr. Wanneer een verstrekking plaatsvindt in het kader van een gericht dataminingonderzoek (met betrekking tot een tijdelijk politieregister) kunnen de verstrekte gegevens in aanmerking komen voor vastlegging als zelfstandig subject in het tijdelijke politieregister<sup>57</sup>, indien het voor dat register (en daarmee

---

55. Zie sectie 7.3.4.3 onder het kopje *Doelbinding*.

56. *Kamerstukken II*, 1996/197, 25 398, nr. 3, p. 19.

voor het gericht dataminingonderzoek) noodzakelijk is om de gegevens in categorie *c* te verwerken.

### *10.6.2 Koppeling*

Een koppeling van een register zware criminaliteit met een tijdelijk politieregister dient noodzakelijk te zijn voor het doel van het laatstgenoemde register. Dit is het geval wanneer een koppeling met een register zware criminaliteit in beginsel noodzakelijk is om de politietaak, voor zover deze de bestrijding van de zware criminaliteit betreft, op effectieve wijze te kunnen uitvoeren. Verder dient het modelreglement van het register zware criminaliteit in de mogelijkheid van een koppeling te voorzien. Dit modelreglement bepaalt in art. 17 lid 1 sub *a* dat een koppeling mogelijk is voor zover noodzakelijk ter voorkoming en opsporing van misdrijven die een ernstige inbreuk op de rechtsorde opleveren. Een koppeling met een tijdelijk politieregister is mogelijk wanneer de doelstelling van het gericht dataminingonderzoek in het kader waarvan het is aangelegd nauw aansluit bij die van het register zware criminaliteit.

### *10.6.3 De aard van het gerichte dataminingonderzoek*

In het kader van een gericht dataminingonderzoek kan in beginsel gebruik worden gemaakt van gegevens uit een register zware criminaliteit, zonder dat dit resulteert in een ontoelaatbare inbreuk op de persoonlijke levenssfeer. Een dergelijke verwerking van gegevens is in beginsel enkel mogelijk voor het doel waarvoor die gegevens zijn vastgelegd. Het op een tijdelijk politieregister van toepassing zijnde beperkte verstrekkingenregime waarborgt dat de gegevens niet voor andere doeleinden kunnen worden gebruikt.

Opmerkelijk is dat ook de gegevens behorende tot categorie *c* kunnen worden verwerkt in een tijdelijk politieregister. Een verstrekking van gegevens uit een register zware criminaliteit en de registratie daarvan in een tijdelijk politieregister leidt niet tot een ontoelaatbare inbreuk op de privacy vanwege het beperkte verstrekkingenregime in combinatie met het feit dat de gegevens, die geenszins zijn bestemd voor operationeel gebruik, na afloop van het gericht dataminingonderzoek worden vernietigd. Ook hier zij overigens opgemerkt dat dient te worden voorkomen dat gegevens uit een register zware criminaliteit die zijn opgenomen in een tijdelijk politieregister (dat als datawarehouse fungeert), middels registratie in een MRO-bestand voor operationeel gebruik beschikbaar komen. Voor die gegevens geldt dat zij ook op een andere wijze kunnen worden verkregen.

### *10.6.4 Weigering door de beheerder*

Een verstrekking aan een tijdelijk politieregister kan door de beheerder van een register zware criminaliteit worden geweigerd of aan beperkende voorwaarden worden gebonden,

---

57. Zie ook sectie 10.5.1.

indien dat noodzakelijk is voor een goede uitvoering van de politietaak<sup>58</sup>. Gezien echter de verstrekingsverplichting voor zover nodig voor de uitvoering van de politietaak<sup>59</sup>, is de betekenis van de weigeringsbevoegheid in de praktijk gering.

### Resumerend

In het kader van een gericht dataminingonderzoek kan gebruik worden gemaakt van gegevens in een register zware criminaliteit wanneer het doel van dat onderzoek samenhangt met de bestrijding van de zware criminaliteit. Dit geldt, afhankelijk van het doel van het dataminingonderzoek, voor alle drie gegevenscategorieën in een register zware criminaliteit.

### 10.7 Afsluitend

Een belangrijke conclusie uit dit hoofdstuk betreft de positie van het verkennend onderzoek als bedoeld in art. 126gg Sv. Volgens de wetgever is het verkennend onderzoek bij uitstek onderzoek naar gegevens uit bestaande persoonsregistraties. Alleen wanneer er ruimte is dergelijke gegevens te verkrijgen, kan het tot goede resultaten leiden. Nu de bedoelde ruimte op grond van de huidige wet- en regelgeving ontbreekt kan worden geconcludeerd, dat het verkennend onderzoek in de huidige vorm een onbruikbaar instrument is. Dit lijkt een gemiste kans, nu het verkennend onderzoek – mede gezien de plaats ervan binnen het proces van informatiegaring – een belangrijke bijdrage kan leveren aan een succesvolle uitvoering van de opsporingstaak. Daarbij is het, zoals de wetgever in beginsel onderkent, van belang dat kan worden beschikt over NAW-gegevens. Het op vrijwillige basis opvragen van deze gegevens is ongewenst en onrechtmatig. Gezien het doel van een verkennend onderzoek en het belang van de bestrijding van de zware criminaliteit in een vroegtijdig stadium, ligt een herziening van de reikwijdte en invulling van art. 126gg Sv dan ook in de rede. Ter afsluiting van dit hoofdstuk volgt een overzicht van de in het bovenstaande uiteengezette wijzen, waarop uitvoering kan worden gegeven aan een gericht dataminingonderzoek.

### Geen gebruik van externe gegevens

In het beginstadium van het onderzoek zijn nog geen gegevens in het tijdelijk register voorhanden om te kunnen analyseren. In een later stadium van het onderzoek ligt de nadruk meer op het analyseren van de reeds vergaarde gegevens. Voor de verwerking van externe gegevens zijn, naast de algemene voorwaarden die bij ieder dataminingonderzoek gelden, geen nadere beperkingen van toepassing.

---

58. Art. 13a lid onder 3 WPolr.

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

**Gebruik van gegevens die niet afkomstig zijn uit een politieregister**

De aard van de verdenking waarvan bij een gericht dataminingonderzoek sprake is rechtvaardigt, dat actief en gericht kan worden gezocht naar externe gegevens. Met betrekking tot het gebruik van gegevens van buiten de politieke sfeer dient onderscheid te worden gemaakt tussen persoonsgegevens en overige gegevens. In beginsel zijn de mogelijkheden om in het kader van een gericht dataminingonderzoek gebruik te maken van gegevens van buiten het politieke kader erg ruim, vooral wanneer het onderzoek samenhangt met de bestrijding van de zware criminaliteit. Wanneer daarbij tevens sprake is van de verwerking van persoonsgegevens dient daarvoor een wettelijke grondslag aanwezig te zijn.

**Gebruik van gegevens uit een gewoon politieregister**

In het kader van een gericht dataminingonderzoek kan in beginsel steeds gebruik worden gemaakt van de gegevens die zijn vastgelegd in gewone politieregisters indien dat noodzakelijk is voor het doel van het gerichte dataminingonderzoek. Daarbij is het mogelijk gebruik te maken van het register-MOT en het hulpverleningsregister.

**Gebruik van gegevens uit een bijzonder politieregister**

In beginsel is het in het kader van een gericht dataminingonderzoek wenselijk dat kan worden gekoppeld met (gegevens in) de drie bijzondere politieregisters. Op grond van de huidige wet- en regelgeving is die koppeling echter alleen mogelijk met een register zware criminaliteit. Het verstrekkingenregime, evenals het op een bijzonder politieregister betrekking hebbende modelreglement, staat een koppeling met een ander tijdelijk politieregister in de weg.

Gericht dataminingonderzoek	Koppeling	Beperkingen	Gebruik
<b>Geen gebruik externe gegevens</b>	Nee	Algemeen	Onbeperkt
<b>Gebruik externe gegevens*</b>	Ja**	Algemeen/koppeling	Beperkt
<b>Gegevens uit een gewoon politieregister</b>	Ja	Algemeen/koppeling	Beperkt
<b>Gegevens uit een bijzonder politieregister</b>	Ja	Algemeen/koppeling/specifiek	Alleen het register zware criminaliteit

\* Uitgezonderd de gegevens die in de politieregisters liggen opgeslagen.

\*\* Tenzij de externe gegevens niet tot enig zelfstandig register behoren.

*Schema 16 Toepassing gericht dataminingonderzoek (ter verbetering van de informatiepositie van een tijdelijk politieregister)*



---

## 11 Beantwoording van de onderzoeksvragen

### Conclusies en aanbevelingen

Centraal in dit onderzoek staat de toepassing van dataminingonderzoek bij het streven naar een optimale informatiepositie bij politie en justitie. Opsporing is bij uitstek een kennisintensieve activiteit. Informatie is vaak versnipperd aanwezig en bevat belangrijke (verborgen) kennis, die pas na een bewerking van de gegevens zichtbaar kan worden gemaakt. Bij het streven naar optimalisering van de informatiepositie speelt nieuwe informatie (van derden) van buitenaf een steeds prominentere rol. Naast de bestrijding van bijvoorbeeld de zware en georganiseerde criminaliteit in eigen land nopen ook ontwikkelingen als een 'uitdijend' Europa en de toenemende dreiging van het internationale terrorisme tot een herziening van informatieverwerking in het kader van de opsporing. Voor het verkrijgen en behouden van een goede informatiepositie dient informatie op een veel grotere schaal en (daardoor ook) efficiënter te worden verwerkt dan voorheen. Vanuit technisch oogpunt lijken hiervoor weinig obstakels te bestaan. Door de mogelijkheden tot digitale verwerking van gegevens en de voortschrijdende technologische ontwikkelingen op dat gebied kunnen de enorme hoeveelheden (potentieel) bruikbare gegevens op efficiënte wijze worden verwerkt. Hoewel het proces van datamining enerzijds een belangrijke bijdrage kan leveren aan de opsporing, dient anderzijds het belang van de burger bij de bescherming van diens persoonlijke levenssfeer niet uit het oog te worden verloren. Het recht heeft een dubbele functionaliteit. Het biedt de overheid de mogelijkheid inbreuk te maken op de rechten van de burger, maar beschermt diezelfde burger tegelijkertijd tegen te vergaande inbreuken door de overheid. De behoefte aan en de vraag naar het gebruik van het dataminingsproces creëert een confrontatie met het spanningsveld tussen de bescherming van de fundamentele rechten van de burger enerzijds en het belang van de overheid bij het in bepaalde gevallen maken van een inbreuk op die rechten anderzijds<sup>1</sup>. Dataminingonderzoek dient zodanig plaats te vinden dat opsporingsdiensten optimaal kunnen profiteren van de mogelijkheden die het dataminingspro-

---

1. *Kamerstukken II, 2000 /01, 27 613, nr. 1, p. 5.* Notitie over de vraag hoe kan worden gekomen tot maximale versterking van de effectiviteit van opsporing en toezicht, waarin nogmaals de afweging tussen enerzijds de effectiviteit van de opsporing en anderzijds de waarborging van het recht op de eerbiediging van de persoonlijke levenssfeer aan de orde wordt gesteld.

ces biedt, zonder dat daarbij de rechten van de burger al te zeer in het gedrang komen.<sup>2</sup> In dit hoofdstuk worden de volgende, in dit onderzoek behandelde overkoepelende onderzoeksvragen beantwoord:

*‘Wat is het strafvorderlijke en privacyrechtelijke kader voor de toepassing van dataminingonderzoek door de Nederlandse overheid ten behoeve van de opsporingstaak?’*

Deze vraag wordt beantwoord aan de hand van een verkenning van de privacyrechtelijke en strafvorderlijke grenzen die (dienen te) worden gesteld aan het gebruik van het dataminingsproces door opsporingsinstanties in het kader van de opsporingstaak. Nagegaan wordt onder meer wat precies onder dataminingonderzoek dient te worden verstaan en welke plaats het proces van datamining inneemt binnen het proces van informatiegaring. Een en ander resulteert in een beschrijving van het benodigde privacyrechtelijke en strafvorderlijke kader.

*‘Op welke wijze kan (en mag) de Nederlandse overheid gebruik maken van het proces van datamining ten behoeve van de opsporingstaak?’*

Aangegeven wordt in hoeverre het gebruik van dataminingonderzoek onder de bestaande wet- en regelgeving mogelijk is. Gelet op de huidige maatschappelijke situatie, de toegenomen mogelijkheden om gegevens te verwerken en de huidige (juridische) opvattingen met betrekking tot de bescherming van de privacy wordt beschreven, op welke punten een herziening van wet- en regelgeving wenselijk is.

### **11.1 Het strafvorderlijke kader voor dataminingonderzoek**

Teneinde het strafvorderlijke kader voor de toepassing van datamining te kunnen schetsen wordt eerst vastgesteld wat onder ‘datamining’ dient te worden verstaan. Daarbij is van belang op welke wijze het dataminingsproces zich verhoudt tot het proces van informatiegaring. Onderzocht wordt of voor het dataminingsproces dient te worden voorzien in een wettelijke regeling, waarbij onder meer wordt bekeken of datamining als opsporingsmethode of opsporingsmiddel kan worden aangemerkt. Afgesloten wordt met conclusies en aanbevelingen inzake het strafvorderlijke kader voor de toepassing van dataminingonderzoek door de Nederlandse overheid ten behoeve van de opsporingstaak.

#### *11.1.1 Datamining en het proces van informatiegaring*

Hoewel een eenduidige definitie van het dataminingsproces ontbreekt<sup>3</sup> kan het worden gekenmerkt als: een deels of volledig geautomatiseerde analyse die betrekking heeft op

---

2. Ministerie van Justitie 1998, p. 5.

3. Zie sectie 1.3.

één of meer gegevensbestanden en gericht is op het ontdekken van nieuwe informatie (anomalieën, bepaalde kenmerken of verbanden) welke niet (of slechts met veel grotere inspanning) op een andere wijze kan worden verkregen. Aan het dataminingsproces kan op tal van manieren uitvoering worden gegeven. Teneinde die methoden te vatten in een werkbaar regeling, maakt dit onderzoek een onderscheid naar ongericht en gericht dataminingsonderzoek. Daardoor is voor een complex technologisch proces als datamining een juridisch werkbaar kader gecreëerd en uitgewerkt.

In hoofdstuk twee werd onderzocht hoe het dataminingsproces zich verhoudt tot het proces van informatiegaring ofwel de opsporing. Hierdoor werd duidelijk wanneer en op welke wijze het dataminingsproces gedurende het proces van informatiegaring kan worden ingezet. Dit proces valt uiteen in drie fasen, te weten het opsporingsonderzoek, het verkennend onderzoek en het opbouwen en in stand houden van een zekere informatiepositie hetgeen kan worden gerealiseerd door het opslaan, bewerken, gebruiken en analyseren van gegevens dan wel het vergaren van gegevens door de toepassing van niet-ingrijpende middelen. Toepassing van dataminingsonderzoek is mogelijk gedurende het gehele proces van informatiegaring. Indien de afzonderlijke toepassingsvarianten van het dataminingsproces worden afgezet tegen het proces van informatiegaring, geeft de verhouding tussen deze dataminingsvarianten en de opsporingsfasen het volgende beeld:

	Ontdekken		Toetsing
<b>Toepassingsvarianten dataminingsproces</b>	Onggericht dataminingsonderzoek	Gericht dataminingsonderzoek	Verificatie
<b>Het proces van informatiegaring</b>	Opbouwen en instandhouden van de informatiepositie	Het verkennend onderzoek	Het opsporingsonderzoek
<b>Aanknopingspunten</b>	Geen verdenking	← Overgang ⇒	Verdachte

*Schema 17 De relatie tussen de drie dataminingsvarianten en de stadia van het proces van informatiegaring*

### Onggericht dataminingsonderzoek

Onggericht dataminingsonderzoek kan worden gebruikt ter verbetering van de (algemene) informatiepositie van een politieregister, een politiekorps of het Nederlandse politieapparaat als geheel. Binnen het proces van informatiegaring gaat het om de fase van opbouwen en in stand houden van een zekere informatiepositie, waarbij in beginsel niet gericht wordt gezocht naar aanleiding van een bepaalde aanwijzing, zaak of gedraging. In het kader van een ongericht dataminingsonderzoek zal slechts in beperkte mate een inbreuk op de persoonlijke levenssfeer plaatsvinden. Toepassing van ongericht dataminingsonder-

zoek dient te kunnen worden aangemerkt als een niet-ingrijpend middel. Verwerking van gegevens omtrent onverdachte personen is onwenselijk, aangezien in dat geval sprake is van een ingrijpend middel waarvoor een nadere legitimatie aanwezig dient te zijn in de vorm van een wettelijke regeling. Een algemene bevoegdheid als die van art. 2 Politiewet 1993 volstaat dan niet meer. Een ongericht dataminingonderzoek dat betrekking heeft op gegevens die reeds bij opsporingsinstanties aanwezig zijn is mogelijk, voor zover dat plaatsvindt in overeenstemming met de WPolr en het BPolr. Voor een verbetering van de informatiepositie van een politieregister met behulp van ongericht dataminingonderzoek door de beheerder van het register, is in beginsel geen aanvullende wettelijke grondslag vereist wanneer geen gebruik wordt gemaakt van externe gegevens die een inbreuk op de privacy met zich meebrengen<sup>4</sup>. Wanneer gebruik wordt gemaakt van externe gegevens uit andere politieregisters of van buiten de politieke sfeer gelden op grond van onder meer de WPolr en het BPolr nadere beperkingen. Voor een verwerking van persoonsgegevens van buiten de politieke sfeer is steeds een wettelijke grondslag benodigd.

#### **Gericht dataminingonderzoek**

De gerichte dataminingsvariant kan worden ingezet ter verbetering van de informatiepositie in een bepaald geval. Dit heeft betrekking op de informatiepositie van een tijdelijk politieregister dat kan worden aangelegd in het kader van de politietaken in een specifiek geval of een verkennend onderzoek van art. 126gg Sv. Een gericht onderzoek is mogelijk naar aanleiding van een aanwijzing of verdenking van het plegen dan wel beramen van strafbare feiten. Nu bij aanvang van een gericht dataminingonderzoek al sprake is van een bepaalde mate van verdenking, is dat onderzoek qua reikwijdte beperkter dan de ongerichte dataminingsvariant. Dit betreft met name het doel (de aard van de strafbare feiten) en de groep van personen waarop het onderzoek betrekking heeft. De ingrijpende aard van deze dataminingsvariant wordt gerechtvaardigd door de striktere voorwaarden voor het verrichten van een gericht dataminingonderzoek. Gezien het voorgaande vindt een gericht dataminingonderzoek plaats in de latere stadia van het proces van informatiegaring: het verkennend onderzoek of het opsporingsonderzoek.

Het verkennend onderzoek gaat normaliter aan het opsporingsonderzoek vooraf en kan zich tevens richten op personen die (nog) niet als verdachte kunnen worden aangemerkt. Daarom heeft het verkennend onderzoek een wettelijke grondslag; gebruik van opsporingsbevoegdheden of dwangmiddelen waarmee inbreuken op de rechten van burgers kunnen worden gemaakt is niet toegestaan. Wanneer uit het verkennend onderzoek een verdenking voortvloeit die de behoefte doet ontstaan aan de inzet van dergelijke middelen, dient het verkennend onderzoek (tenminste voor zover dat betrekking heeft

---

4. Gegevens die gedurende een lopend ongericht dataminingonderzoek via de daarvoor bestaande wettelijke wegen in een politieregister worden opgenomen, worden niet aangemerkt als zijnde externe gegevens.

op de betreffende verdenking) te eindigen en neemt het opsporingsonderzoek een aanvang. In het kader van een gericht dataminingonderzoek worden vrijwel steeds gegevens verwerkt die nog niet bij de politie aanwezig waren. Waar voor een verwerking van reeds aanwezige gegevens vooral dient te worden gekeken naar de WPolr en het BPolr, is een verwerking van persoonsgegevens van buiten de politieke sfeer slechts mogelijk indien daarvoor een wettelijke grondslag bestaat. Hoewel de WPolr en het BPolr de registratie van gegevens regelen, voorzien zij slechts summier in de verwerking ervan<sup>5</sup>.

### Verificatie

Bij verificatie is, strikt genomen, geen sprake meer van dataminingonderzoek. Bij verificatie staat niet het zoeken naar nieuwe kennis, maar het verifiëren van al gevonden kennis centraal. Of in een bepaald geval sprake is van gericht dataminingonderzoek of van verificatie hangt van de mate van verdenking af. Wanneer er een afdoende onderbouwde verdenking is zal niet langer naar nieuwe gegevens worden gezocht, maar vindt verificatie dan wel toetsing van het behaalde resultaat plaats. Verificatie gebeurt gedurende het opsporingsonderzoek, het laatste stadium van het proces van informatiegaring. Kenmerkend is dat een informatief karakter ontbreekt en dat de focus ligt op een strafvorderlijke afdoening. Er wordt gericht gezocht op één of meer personen. Aangezien er sprake is van een zwaardere verdenking en de verdengkingscriteria van de art. 27 en/of 132a Sv vervuld zijn, kunnen – afhankelijk van de aard van de criminele gedraging(en) waarop de verdenking betrekking heeft – mogelijk bijzondere opsporingsbevoegdheden en dwangmiddelen worden toegepast.

### Resumerend

De wijze waarop de verschillende toepassingsvarianten van het dataminingsproces zich verhouden tot het proces van informatiegaring is bepalend voor de grenzen van de toepassing van dataminingonderzoek ten behoeve van de opsporingstaak. Hoewel het dataminingsproces tal van toepassingsmogelijkheden biedt, mogen deze niet op elk willekeurig moment gedurende de opsporing worden ingezet. Aan de hand van de onderverdeling binnen het dataminingsproces wordt duidelijk, op welke manier een legitieme toepassing van de verschillende dataminingsvarianten binnen het proces van informatiegaring kan worden gerealiseerd. De beperkingen die dit onderzoek daarbij stelt aan de toepassing van dataminingonderzoek sluiten aan bij het regeringsstandpunt daaromtrent in de Nota WES; daar wordt aangegeven dat bij dataminingonderzoek ten aanzien van een op voorhand onbepaalde groep van personen veel verdergaander beperkingen aan het zoeken dienen te worden gesteld, dan wanneer het een enkele persoon betreft.<sup>6</sup>

5. Vanwege het doel van een gericht dataminingonderzoek zal de bedoelde grondslag bij die dataminingsvariant eerder aanwezig zijn dan bij een ongericht dataminingonderzoek.

6. *Kamerstukken II, 1997/98, 25 880, nrs. 1-2, p. 83.*

Door de inzet van datamining in verband te brengen met een bepaalde mate van verdenking worden de rechten van de burger gewaarborgd. Hoe ernstiger de aard van het strafbare feit en/of hoe sterker de verdenking, hoe groter de eventuele inbreuk op de persoonlijke levenssfeer mag zijn die met een onderzoek naar dat feit gepaard gaat. Voor een verwerking van personen in politieregisters is met name het bepaalde in de WPolr en het BPolr van belang. Indien sprake is van een verwerking van (informatie waarbij het onder meer gaat om) gegevens omtrent onverdachte personen, is in alle gevallen een aparte wettelijke grondslag noodzakelijk, temeer daar die gegevens vaak voor andere doeleinden zijn verzameld dan waarvoor ze vervolgens zouden worden verwerkt. De wetgever geeft aan dat dergelijke gegevens bij verwerking dienen te worden afgeschermd, niet voor andere onderzoeken mogen worden gebruikt en zodra mogelijk dienen te worden vernietigd.

#### *11.1.2 Wettelijke inkadering datamining*

In deze sectie wordt onderzocht of, en zo ja op welke wijze voor het dataminingsproces dient te worden voorzien in een wettelijke regeling.

##### *11.1.2.1 Datamining als opsporingsmiddel*

Opsporingsbevoegdheden dienen zowel naar inhoud als procedure en controle goed te worden geregeld. Wanneer met een opsporingsmethode inbreuk wordt gemaakt op een door de Grondwet, het EVRM of het IVBP beschermd grondrecht is een wettelijke regeling in beginsel noodzakelijk.<sup>7</sup> Bij de toepassing van datamining in het kader van de opsporingstaak is vooral de bescherming van de persoonlijke levenssfeer in het geding. In dat geval stellen de Grondwet en de genoemde verdragen eisen aan de wijze van normering van die bevoegdheden en is een wettelijke basis vereist in bijvoorbeeld het Wetboek van Strafvordering of middels bijzondere wetgeving. De opdracht om regelingen te treffen die in het bijzonder betrekking hebben op registraties van persoonsgegevens en het gebruik daarvan, is sinds 1983 verankerd in art. 10 lid 1 en 2 Gw<sup>8</sup>. Hieraan is (uitgaande van de strekking van dit onderzoek) nader invulling gegeven met de Wpr, de WPolr en het bijbehorende Bpolr.<sup>9</sup>

Het rapport ‘Opsporing gezocht’<sup>10</sup> maakt verschil tussen de begrippen opsporingsmethode en opsporingsmiddel, als aanduiding van een concrete opsporingsactiviteit. Het rapport onderscheidt vier opsporingsmethoden: observatie, het gebruik maken van informanten, infiltratie en het verrichten van andere vormen van informatiewinning. Dataminingonderzoek kan op de categorie van overige informatie-inwinning worden

---

7. *Kamerstukken II*, 1996/97, 25 403, nr. 3, p. 9.

8. Zie Van Ruth & Schreuders 2000.

9. *Kamerstukken II*, 1997/98, 25 880, nrs. 1-2, p. 82.

10. *Rapport Opsporing gezocht* 1994

toegepast. Aan die categorie worden voorts de opsporingsmiddelen van informatie-inwinning bij derden, misdaadanalyse, fenomeenonderzoek en financieel rechercheren toegekend. Het principe van het dataminingonderzoek komt deels overeen met dat van misdaadanalyse. De definitie die de Nota WES geeft van misdaadanalyse:

*‘Het opsporen en inzichtelijk maken van verbanden tussen criminaliteitsgegevens onderling en andere mogelijk relevante gegevens met het oog op de praktijk van politie en justitie. Dit wordt gerealiseerd door het verzamelen, evalueren en analyseren van de beschikbare informatie en vervolgens (intern) verstrekken van de bevindingen’.*<sup>11</sup>

sluit aan op die van het dataminingonderzoek voor zover het de ongerichte dataminingsvariant betreft:

*‘Het geautomatiseerd doorzoeken van grote gegevensbestanden en het combineren van gegevens die verspreid in bestanden liggen opgeslagen waarna met behulp van speciale programmatuur in deze gegevens wordt gezocht naar anomalieën, trends of bepaalde kenmerken’.*<sup>12</sup>

De klassieke misdaadanalyse is beperkt tot niet-ingrijpende middelen terwijl dataminingonderzoek, vanwege het flexibele karakter ervan, zowel ingrijpend als niet-ingrijpend van aard kan zijn.<sup>13</sup> In de Nota WES<sup>14</sup> wordt aangegeven dat bevoegdheden die inbreuk maken op de privacy zo nauwkeurig mogelijk omschreven dienen te worden. Er moet onderzoek worden verricht naar de noodzaak en de wenselijkheid van het gebruik van datamining als opsporingsmiddel, waarbij de volgende uitgangspunten gehanteerd dienen te worden.

- Opsporingsonderzoek naar en verwerken van gegevens is slechts toelaatbaar bij verdenking of bij een verkennend onderzoek, dan wel in verband met een onderzoek naar georganiseerde criminaliteit, zonder dat er sprake is van een concrete verdenking.
- Het verwerken van gegevens en de daarbij te gebruiken technieken kan een forse inbreuk op het recht op privacy opleveren. Een nauwkeurige afweging tussen het opsporingsbelang en het belang van de privacybescherming is nodig.

Het eerste uitgangspunt ziet met name op de gerichte dataminingsvariant, het tweede meer algemeen op het dataminingsproces. Dat ook de ongerichte dataminingsvariant tot

11. *Rapport werkgroep Misdaadanalyse* 1991.

12. *Kamerstukken II, 1997/98, 25 880, nrs. 1-2, p. 30 en 42.*

13. De moderne misdaadanalyse heeft niet steeds als niet-ingrijpend middel te kunnen worden aangemerkt en sluit daardoor beter aan op het dataminingsproces als geheel.

14. *Kamerstukken II, 1997/98, 25 880, nrs. 1-2, p. 161.*

dat proces wordt gerekend blijkt uit het feit, dat wordt gesproken over technieken die een forse inbreuk op het recht op privacy *kunnen* opleveren. Voorts zij erop gewezen dat hier in het kader van datamining wordt gesproken over het *verwerken* van gegevens.

#### 11.1.2.2 *Het belang van wettelijke regeling van het dataminingsproces*

Wanneer datamining wordt aangemerkt als een opsporingsmethode dient deze een expliciete wettelijke basis te krijgen. De wet definieert limitatief de opsporingsmethoden die een inbreuk op de fundamentele rechten van de burger inhouden. Analoge methoden mogen niet worden toegepast zonder wettelijke basis. Wanneer de weg wordt gevolgd die met de wet BOB is ingeslagen, ligt het in de rede dat ook voor de toepassing van dataminingonderzoek een wettelijke basis wordt gecreëerd. Hiermee kan worden voorzien in voldoende waarborgen voor een garantie van de bescherming van de rechten van de burger<sup>15</sup>. De Nota WES behandelt het dataminingsvraagstuk ook als onderdeel van het thema privacy (deel IIIC). Een wettelijke basis voorziet tevens in de behoefte om bevoegdheden van opsporingsambtenaren expliciet in de wet te regelen. De wetgever dient erop bedacht te zijn bevoegdheden duidelijk te omschrijven, teneinde verschillende interpretaties te voorkomen.<sup>16</sup> Opsporingsambtenaren hebben het recht precies te weten over welke bevoegdheden zij kunnen beschikken.<sup>17</sup> Politie en justitie dienen overigens voldoende beleidsvrijheid te behouden bij de afweging, of van bepaalde methoden gebruik zal worden gemaakt.

Dankzij relatief techniekonafhankelijke wet- en regelgeving is er, wanneer het gaat om de toepassing van dataminingonderzoek, geen sprake van een volledig juridisch vacuüm. Uit dit onderzoek komt echter ook naar voren dat de bestaande wetgeving overwegend indirect van toepassing is op het dataminingsproces en onvoldoende recht doet aan de hedendaagse maatschappelijke werkelijkheid en de veranderde opvattingen inzake onder meer de bescherming van de persoonlijke levenssfeer. Van laatstgenoemde ontwikkeling zijn de verschillen tussen de Wpr en de Wbp een goed voorbeeld. Een extensieve interpretatie, dan wel een interpretatie naar analogie van bestaande wet- en regelgeving, teneinde het dataminingsproces als geheel toch onder de werking van die wet- en regelgeving te brengen resulteert in een kortstondige en onbevredigende oplossing. De nu van toepassing zijnde wetgeving als de WPolr en het BPolr gaan uit van verouderde opvat-

---

15. *Kamerstukken II*, 2000 /01, 27 613, nr. 1, p. 6.

16. *Kamerstukken II*, 2004 /05, 30 001, nr. 1.

17. Er kunnen nog andere redenen bestaan om opsporingsmethoden te normeren, welke nu worden samengevat onder de noemer van het belang van de integriteit van de strafrechtspleging. Daarbij valt bovenal te denken aan de wens om de verantwoordelijkheden voor het gebruik van bepaalde bevoegdheden daar te leggen waar zij horen, de kans op misbruik van bepaalde methoden te verkleinen en in verband daarmee het gevaar van corruptiepeerbaarheid van de politie tegen te gaan. *Kamerstukken II*, 1995 /96, 24 072, nr. 14, p. 16.

tingen aangaande de bescherming van de privacy. De bestaande wet- en regelgeving kan daarom weliswaar richtinggevend zijn voor de toepassing van datamining, maar niet richtingbepalend. Het belang van een specifieke wettelijke regeling met betrekking tot het gebruik van complexe technologische ontwikkelingen wordt zowel door de HR als de regering onderschreven. Met het oog op het voorgaande is het wenselijk de bestaande wetgeving kritisch te toetsen aan de hedendaagse wensen en belangen van burger en overheid. In veel gevallen zal een nadere nuancering van bestaande wetgeving noodzakelijk blijken of zal het zelfs voorkeur verdienen bestaande regelingen volledig terzijde te schuiven en zonodig te vervangen.

#### *11.1.2.3 Reikwijdte van de bestaande wettelijke grondslag*

Uitgaande van de bestaande wettelijke kaders wordt ingegaan op de vraag, hoe een passend juridisch kader voor het dataminingsproces kan worden gerealiseerd.

#### **Plaats van een wettelijke regeling**

In beginsel kan het dataminingsproces worden gerekend tot de activiteiten waarop de WPoI ziet. Het uitputtende karakter van de WPoI nodigt uit om ook het dataminingsproces onder deze bijzondere regeling te brengen. Daartoe zal herziening van de bestaande WPoI noodzakelijk zijn. Op de verwerking van persoonsgegevens in het kader van de politietoek is niet de Wbp, maar de WPoI van toepassing<sup>18</sup>. De WPoI ziet op alle persoonsregistraties die worden bijgehouden in het kader van de uitvoering van de politietoek in de zin van art. 2 Politiewet 1993. De keuze voor een aparte wettelijke regeling met betrekking tot de verwerking van persoonsgegevens door de politie<sup>19</sup> hangt met name samen met het vertrouwelijke en gevoelige karakter van die gegevens. Het regime van de WPoI staat echter niet geheel los van de Wbp. De MvT bij de Wbp stelt nadrukkelijk dat bijzondere wetten als de WPoI formeel-juridisch weliswaar naast de privacywetgeving staan, maar zich wel bevinden binnen de grenzen die de normen van de Wbp voorstaan<sup>20</sup>. Omdat de Wbp, in tegenstelling tot de WPoI, reeds voorziet in de huidige opvattingen op het gebied van privacy speelt de Wbp op dat punt een belangrijke rol bij het creëren van een juridisch kader voor de toepassing van dataminingonderzoek.

#### **Ongericht dataminingonderzoek**

In beginsel wordt uitgegaan van het standpunt dat voor het opslaan, bewerken en analyseren van gegevens door toepassing van niet-ingrijpende middelen niet per definitie een wettelijke grondslag vereist is. Niet-ingrijpende middelen worden niet in de wet geregeld, omdat deze geen inbreuk op de privacy met zich zouden meebrengen. Het gebruik

18. Art. 2 lid 2 onder c Wbp.

19. In het kader van de strafrechtelijke handhaving van de rechtsorde.

20. *Kamerstukken II, 1997/98, 25 892, nr. 3, p. 12.*

ervan is toegestaan wanneer dat past binnen en dient ter uitvoering van de politietaak, met betrekking tot de strafrechtelijke handhaving van de rechtsorde. Voorts moet worden voldaan aan de eisen van proportionaliteit en subsidiariteit<sup>21</sup>. In de praktijk zal slechts sprake zijn van een niet-ingrijpend middel wanneer geen persoonsgegevens worden verwerkt. Dit is bijvoorbeeld het geval wanneer met behulp van dataminingonderzoek bepaalde profielen worden opgesteld, waarbij het niet noodzakelijk is dat het resultaat in enig stadium herleidbaar is tot een individu. Dergelijk fenomeenonderzoek wordt echter niet tot de taak van de politie gerekend. Een verwerking van persoonsgegevens in het kader van de opsporingstaak zal met het oog op de Wbp in beginsel steeds gepaard gaan met een inbreuk op de persoonlijke levenssfeer<sup>22</sup>. Daarvoor is een wettelijke grondslag vereist.

Het verwerken van gegevens in het kader van een ongericht dataminingonderzoek is algemeen en ongericht van aard en kan worden gerekend tot de taakstelling van art. 2 Politiewet 1993. De wettelijke regeling voor het vastleggen, verstrekken en koppelen van gegevens in het kader van de politietaak is de WPolr en het bijbehorende BPolr. Wanneer gegevens rechtmatig zijn verkregen en noodzakelijk zijn voor het doel waarvoor zij zijn vastgelegd, kunnen zij (in beperkte zin) worden verwerkt op grond van de WPolr. Aangezien de WPolr en het BPolr het benodigde wettelijk kader vormen voor het doen van een zodanige (klassieke) misdaadanalyse, is voor die verwerking in beginsel geen aanvullende wettelijke regeling nodig.

De verwerking van de gegevens in de politieregisters vindt plaats in het kader van een algemene verbetering van de politieke informatiepositie. Dergelijk ongericht dataminingonderzoek kan worden gerekend tot de algemene zorgplicht van de beheerder van een politieregisters, als vastgelegd in art. 7 WPolr. Hoewel ook bij een ongericht onderzoek sprake is van een inbreuk op de privacy, wordt deze binnen het kader van de WPolr niet als ontoelaatbaar bestempeld. Van een ontoelaatbare inbreuk op de persoonlijke levenssfeer kan wel sprake zijn wanneer in het kader van een ongericht dataminingonderzoek tevens (externe) gegevens worden verwerkt die afkomstig zijn van buiten de politieke sfeer. Indien het daarbij persoonsgegevens betreft, is daarvoor in beginsel steeds een aanvullende wettelijke grondslag vereist.<sup>23</sup>

---

21. *Kamerstukken II*, 1996/197, 25 403, nr. 3, p. 8-9.

22. Voor een situatie waarbij geen sprake is van een inbreuk op de privacy, kan worden gedacht aan de situatie waarbij datamining niet wordt gebruikt ten behoeve van de opsporing, maar voor het doen van fenomeenonderzoek. Daarbij is het niet noodzakelijk dat het resultaat in enig stadium herleidbaar is tot een individueel persoon.

23. Hiermee wordt voorkomen dat onverdachte burgers onderwerp gaan vormen van ongericht onderzoek, zonder dat zij daartoe enige aanleiding hebben gegeven.

### Resumerend

Gesteld kan worden dat het wettelijk kader voor ongericht dataminingonderzoek wordt gevormd door de WPolr en het BPolr, indien dat onderzoek zich beperkt tot gegevens die reeds binnen de politieregisters aanwezig zijn en/of externe gegevens, niet zijnde persoonsgegevens.

### Gericht dataminingonderzoek

Ook voor een verwerking van gegevens in het kader van een gericht dataminingonderzoek kan aansluiting worden gezocht bij de WPolr en het BPolr. Een gericht dataminingonderzoek ziet op een specifieke verbetering van de informatiepositie. Met het oog op het doel van dergelijk onderzoek en de aard van de gegevens die hierbij kunnen worden verwerkt, volstaan de WPolr en de Politiewet 1993 echter niet als wettelijke grondslag. De wetgever geeft aan dat hier in beginsel een specifieke en aanvullende wettelijke grondslag noodzakelijk is.<sup>24</sup> De aanleg van een nieuw tijdelijk politieregister in het kader van een gericht dataminingonderzoek kan niet meer tot het algemeen beheer van de politieregisters worden gerekend. Voorts speelt bij een gericht dataminingonderzoek vooral het gebruik van externe gegevens, met name die welke afkomstig zijn van buiten de politieke sfeer, een essentiële rol. Ook het feit dat onschuldige burgers onderdeel van een gericht dataminingonderzoek kunnen uitmaken noopt tot een aanvullende wettelijke regeling.

Een gericht dataminingonderzoek kan plaatsvinden in het tweede en/of derde stadium van het proces van informatiegaring<sup>25</sup>. Beide stadia kennen een wettelijke grondslag, respectievelijk art. 126gg en 132a Sv. De keuze voor de ene of de andere vorm van onderzoek hangt af van de aard, de omvang en de kwaliteit van de beschikbare informatie. Indien aanwijzingen bestaan dat binnen een groep van personen strafbare feiten worden beraamd of gepleegd die een ernstige inbreuk op de rechtsorde opleveren, kan een verkennend onderzoek aan een strafrechtelijk opsporingsonderzoek voorafgaan. Indien uit de verkregen informatie voldoende concrete aanwijzingen volgen met betrekking tot het plegen of beramen van strafbare feiten als beschreven in art. 132a Sv, kan tot een opsporingsonderzoek worden overgegaan. De genoemde wetsartikelen kunnen dienen als grondslag voor het doen van gericht dataminingonderzoek. De waarborgen die gelden bij het verkennend- en het opsporingsonderzoek gelden dan eveneens voor dat dataminingonderzoek. Dit rechtvaardigt tevens de ruime mogelijkheden tot gegevensverwerking in het kader van een gericht dataminingonderzoek.

---

24. *Kamerstukken II*, 1997/98, 25 880, nrs. 1-2, p. 83.

25. Op het terrein van de strafrechtelijke handhaving kan het vervolg dat aan de informatievergaring wordt gegeven bestaan uit een verkennend onderzoek of een opsporingsonderzoek. Zie sectie 2.3 en *Handboek voor de opsporingspraktijk* 2000, Model Verkennend onderzoek, sectie 1.2.3.

Voor het starten van een gericht dataminingonderzoek vormen de art. 126gg en 132a Sv steeds het uitgangspunt. De WPolr vormt hierbij het wettelijk kader voor de verwerking van gegevens die al aanwezig zijn in de politieregisters. Ook bij een gericht onderzoek is de verwerking van externe persoonsgegevens van buiten de politieke sfeer niet zonder meer mogelijk. De WPolr vormt geen grondslag voor het vergaren van gegevens; de art. 126gg en 132a Sv geven weliswaar een wettelijk kader voor het doen van gericht dataminingonderzoek, maar behelzen geen specifieke regeling voor de verwerking van externe persoonsgegevens. Een aanvullende wettelijke regeling is daarom noodzakelijk. Opgemerkt zij dat onderzoek dat is gebaseerd op de art. 126gg en art. 132a Sv een vergaande inbreuk op de privacy legitimeert, waardoor in de praktijk zeer wel kan worden voorzien in een wettelijke grondslag voor de verwerking van externe persoonsgegevens, voor zover dat nog niet het geval mocht zijn. De criteria die gelden voor een wettelijke regeling voor de verwerking van externe persoonsgegevens zullen in beginsel aansluiten op die voor de toepassing van deze twee stadia van het proces van informatiegaring.

#### *11.1.2.4 Uitgangspunten van de wettelijke regeling*

Met het vastleggen, verstrekken en koppelen van gegevens voorziet de huidige WPolr slechts gedeeltelijk in het verwerken van persoonsgegevens in het kader van de politietak. De bescherming van de persoonlijke levenssfeer dient echter niet alleen te worden gewaarborgd op het moment waarop een registratie van gegevens plaatsvindt, maar ook gedurende de verdere verwerking van die gegevens. Het is onvoldoende wanneer er, weliswaar strikte, regels gelden voor de doeleinden waarvoor en de omstandigheden waaronder gegevens mogen worden vastgelegd, maar vervolgens niet wordt voorzien in de wijze waarop die gegevens na registratie binnen de politie mogen worden verwerkt. Ook de wetgever spreekt in het kader van datamining als opsporingsmiddel over 'het verwerken van gegevens'<sup>26</sup>. Vooral op dit punt schiet de huidige wet- en regelgeving tekort. Met het oog op de spilfunctie van de WPolr bij de verwerking van gegevens in het kader van opsporingstaak, is een herziening op dit punt noodzakelijk.

Een dergelijke benadering is ook van belang met het oog op de duidelijkheid en techniekafhankelijkheid van de wet. Wanneer het dataminingsproces als geheel binnen de reikwijdte van de WPolr wordt gebracht, kan het onderscheid dat de WPolr momenteel maakt naar het vastleggen, verstrekken en koppelen van gegevens worden losgelaten. Dat onderscheid is niet alleen ontoereikend met het oog op de technologische mogelijkheden van datamining, maar het maakt de regeling van de verwerking van politiegegevens ook onnodig complex. Zoals beschreven ziet 'het eigenlijke datamining' op het moment, waarop de gegevens in een datawarehouse met behulp van een technologisch procédé worden verwerkt. Met een (geavanceerd) computerprogramma worden de in het data-

---

26. Sectie 11.1.2.1.

warehouse opgeslagen gegevens op een zodanige manier bewerkt, dat mogelijk aanwezige nieuwe kennis kan worden ontdekt. De exacte technische methode of onderliggende werking van dat computerprogramma is, juridisch gezien, van ondergeschikt belang. Wel van belang is de vraag of een bewerking is toegestaan. Het antwoord op die vraag hangt samen met de gegevensverwerking als geheel. Een wettelijke regeling dient zich daarom zoveel mogelijk te concentreren op het dataminingsproces als geheel.

Voor het vaststellen van het juridische kader voor de toepassing van een technologisch procédé als datamining is in dit onderzoek aansluiting gezocht op de met dat proces samenhangende technische terminologie. Nu het juridisch kader vaststaat is, het voor een wettelijke regeling van het dataminingsproces onwenselijk om hieraan vast te houden. Vanwege het belang van een techniekonafhankelijke regeling zal, in aansluiting op de terminologie van de Wbp, worden uitgegaan van ‘de verwerking van politiegegevens’ om de toepassing van (onder meer) het dataminingsproces wettelijk te regelen. In het verlengde daarvan dienen misdaadanalyse en dataminingonderzoek niet langer als twee naast elkaar staande opsporingsmethoden te worden aangemerkt, maar kan worden gekozen voor een centrale benadering: de verwerking van gegevens in het kader van de politietask.

### *11.1.3 Conclusies en aanbevelingen met betrekking tot het strafvorderlijke kader voor dataminingonderzoek*

#### **Conclusies**

Uit het voorgaande wordt een beeld verkregen van het strafvorderlijke kader voor de toepassing van dataminingonderzoek door de Nederlandse overheid ten behoeve van de opsporingstaak. De bestaande wet- en regelgeving vormt reeds een belangrijk deel van het benodigde wettelijke kader voor de toepassing van datamining. Een ongericht dataminingonderzoek waarbij geen gebruik wordt gemaakt van externe persoonsgegevens, komt sterk overeen met de klassieke misdaadanalyse. Voor de toepassing van deze dataminingsvariant volstaan in beginsel art. 2 Politiewet 1993 en de WPolr als algemene wettelijke grondslag. Wanneer tevens gebruik wordt gemaakt van externe persoonsgegevens van buiten de politieke sfeer kan zowel bij de ongerichte als de gerichte dataminingsvariant sprake zijn van de moderne misdaadanalyse. In dat geval is voor de verwerking van die externe persoonsgegevens een aanvullende wettelijke regeling noodzakelijk. Bovendien kent een gericht dataminingonderzoek een afzonderlijke wettelijke grondslag in de vorm van art. 126gg of 132a Sv. Noch de moderne misdaadanalyse, noch het dataminingonderzoek kennen momenteel een eigen wettelijke regeling. Met het oog op de bescherming van de persoonlijke levenssfeer en het belang van techniekonafhankelijke en duidelijke regelgeving is het wenselijk, beide opsporingsmiddelen onder te brengen in één wettelijke regeling. Dit kan worden gerealiseerd door de hiervoor beschreven aanpassing van de WPolr. Wanneer de WPolr uitgaat van de verwerking van gegevens, wordt

voorzien in een techniekonafhankelijke regeling van bestaande en toekomstige handelingen met betrekking tot politiegegevens in het kader van de politietaak, waarbij de bescherming van de persoonlijke levenssfeer op iedere verwerking van toepassing is. Een en ander komt de duidelijkheid, de rechtszekerheid en de rechtsbescherming ten goede.

### **Aanbevelingen**

Met het oog op de in sectie 10.2.1.1 besproken beperkingen van het verkennend onderzoek verdient het aanbeveling, de reikwijdte en de betekenis van art. 126gg Sv te evalueren. Wellicht vragen de huidige inzichten inzake de verwerking van persoonsgegevens ten behoeve van de opsporing om een ruimere wettelijke basis voor het doen van gericht dataminingsonderzoek dan die, welke art. 126gg Sv thans biedt. Verder dient te worden voorzien in een duidelijke wettelijke regeling van het dataminingsproces (en aanverwante opsporingsmiddelen) teneinde de mogelijkheden van dit proces beter te benutten en tegelijkertijd de bescherming van de persoonlijke levenssfeer voldoende te kunnen waarborgen. Hiertoe dient de WPolr te worden herzien in die zin dat het huidige onderscheid naar de verschillende handelingen met betrekking tot persoonsgegevens wordt losgelaten en wordt uitgegaan van een centrale regeling voor de verwerking van politiegegevens.<sup>27</sup>

## **11.2 Het privacyrechtelijk kader voor de toepassing van dataminingsonderzoek**

In deze sectie staat het privacyrechtelijke kader voor de toepassing van dataminingsonderzoek centraal. Na een algemene uiteenzetting van internationale en nationale uitgangspunten en uitwerking van de privacyregels voor de verwerking van (persoons)gegevens in het kader van de politietaak, wordt ingegaan op de vraag in hoeverre en op welke wijze de huidige wet- en regelgeving daarin voorziet (voor het dataminingsproces) en op welke punten eventueel nog verbetering nodig is.

### **Uitgangspunten privacy internationaal**

Bij een verwerking van gegevens in het kader van de politietaak is in beginsel steeds sprake van een inbreuk op de persoonlijke levenssfeer. Op grond van de internationale wet- en regelgeving dient daarvoor een wettelijke grondslag te zijn, die voor de burger voldoende toegankelijk en voorzienbaar is. Indien de regeling is gebaseerd op een wet in formele zin (zoals art. 10 Gw verlangt) is hieraan voldaan. Van belang is dat de regeling voldoende exact geformuleerd is, zodat de burger vooraf kan weten onder welke omstandigheden en voorwaarden de bevoegdheid mag worden toegepast. De regeling moet voorts waarborgen bieden tegen willekeurige inmenging van de overheid in het persoon-

---

27. Hiermee wordt het huidig regelgevend kader, in overeenstemming met de aanbevelingen in de evaluatie van de wet bijzondere politieregisters, vereenvoudigd. *Rapport Evaluatie wet bijzondere politieregisters 2004*, p. 183-187.

lijke leven van de burger en misbruik van bevoegdheid<sup>28</sup>. Met het oog hierop dient het verwerken van gegevens omtrent onverdachte personen slechts in uitzonderlijke gevallen mogelijk te zijn. Ook voor de verwerking van persoonsgegevens voor een ander doel dan waarvoor zij zijn vastgelegd is een wettelijke regeling van belang. Het uitgangspunt dat gegevens in beginsel niet worden gebruikt voor een ander doel dan waarvoor zij zijn vastgelegd is uitgewerkt in de Wbp.

### **Uitwerking privacy nationaal**

In Nederland is met de WPolr gekozen voor een aparte wettelijke regeling voor de ‘verwerking’<sup>29</sup> van persoonsgegevens in het kader van de politietaak. Als ‘lex specialis’ van de Nederlandse privacywetgeving (Wbp) zijn de WPolr en het BPolr bepalend voor de wijze waarop die verwerking plaatsvindt. Het feit dat de WPolr inmiddels sterk is verouderd heeft negatieve consequenties voor de bescherming van de persoonlijke levenssfeer. Bij de totstandkoming van de WPolr en het bijbehorende BPolr is logischerwijs enkel rekening gehouden met de regels, die het internationale en nationale recht op dat moment stelden aan de registratie van persoonsgegevens. De WPolr richt zich vooral op de registratie van gegevens in het kader van de politietaak en voorziet niet of nauwelijks in de vraag, wat er verder met de geregistreerde gegevens mag gebeuren. Inmiddels is de toenmalige van kracht zijnde privacywetgeving in de vorm van de Wpr echter vervangen door de Wbp, en zijn nationale en internationale opvattingen betreffende de bescherming van de persoonlijke levenssfeer gewijzigd. Met betrekking tot het voortgangstraject na de registratie van gegevens gaat het Wbp uit van de verwerking van persoonsgegevens in al haar stadia<sup>30</sup>, waartoe iedere handeling met betrekking tot persoonsgegevens wordt gerekend. Ook verwerkingen die niet zijn gericht op individuele personen waarbij gebruik wordt gemaakt van persoonsgegevens, vallen onder de begripsomschrijving<sup>31</sup>. In het navolgende wordt uiteengezet, op welke wijze de WPolr en het BPolr momenteel plegen te voorzien in de benodigde privacywaarborgen bij de verwerking van persoonsgegevens in het kader van de politietaak.

#### *11.2.1 Uitwerking privacybescherming in de WPolr en het BPolr*

De bescherming van de persoonlijke levenssfeer wordt in de WPolr en het bijbehorende BPolr binnen het gesloten systeem van de politieregisters op verschillende manieren gewaarborgd. Enerzijds wordt aangegeven wanneer en onder welke voorwaarden gegevens mogen worden vastgelegd, anderzijds waarborgt het verstrekkingenregime dat de vastgelegde gegevens op een verantwoorde wijze verder worden verwerkt. De WPolr maakt onderscheid tussen gewone en bijzondere politieregisters. De bijzondere politie-

28. Kruslin & Huvig, EHRM 24 april 1990, NJ 1991, nr. 523.

29. Niet iedere vorm van verwerken wordt nog door de WPolr geregeld.

30. *Kamerstukken II*, 1997/98, 25 892, nr. 3, p. 16.

31. *Kamerstukken II*, 1997/98, 25 892, nr. 3, p. 51.

registers kenmerken zich in beginsel door een beperkt verstrekkingenregime. Hoewel een register zware criminaliteit is bestemd voor operationeel gebruik, is in de praktijk sprake van een beperkt verstrekkingenregime. Van de gewone politieregisters kennen alleen het hulpverleningsregister en het register-MOT een beperkt verstrekkingenregime. In de registers waarop een beperkt verstrekkingenregime van toepassing is, kan ook zachte opsporingsinformatie worden vastgelegd. De registratie en verstrekking daarvan is slechts beperkt mogelijk met het oog op de bescherming van de persoonlijke levenssfeer. De handhaving van het originele verstrekkingenregime is daarom van essentieel belang. Het gevaar van een doorbreking van de verstrekkingenregimes die (oorspronkelijk) op de gegevens in die verwijsindex van toepassing zijn is in het bijzonder aanwezig, wanneer gebruik wordt gemaakt van een verwijsindex. Bij het vastleggen en verstrekken van gegevens spelen de aard van de gegevens, het doelbindings- en het noodzakelijkheidsbeginsel, de reglementen en de naleving van de privacywaarborgen een rol. Hierna wordt ingegaan op de wijze waarop de genoemde factoren bijdragen aan een verantwoorde verwerking van gegevens in het kader van de opsporing.

#### *11.2.1.1 Beperkte verwerking van gevoelige en zachte gegevens*

De verwerking van gevoelige gegevens is slechts beperkt mogelijk. In art. 5 WPolr is geregeld welke persoonsgegevens onder welke omstandigheden kunnen worden geregistreerd. Dit heeft met name betrekking op gegevens aangaande godsdienst, ras, politieke gezindheid en seksualiteit en medische of psychologische kenmerken. Op grond van art. 5a WPolr kunnen gegevens over onverdachte personen ook niet zonder meer in een politieregister worden vastgelegd. Langdurige opslag van dergelijke gegevens is alleen mogelijk in de bijzondere politieregisters, doch gedurende een termijn van vier maanden mogen zij ook worden vastgelegd in een gewoon politieregister. In de praktijk betekent dit, dat die gegevens gedurende die termijn onbeperkt binnen het politieapparaat kunnen worden gebruikt, ongeacht de vraag voor welk doel dit gebeurt. Met het oog op de persoonlijke levenssfeer kunnen vraagtekens worden geplaatst bij de wenselijkheid en noodzaak van een dergelijke ruime verwerking van gevoelige gegevens.

#### *11.2.1.2 Het doelbindingsbeginsel*

De doelbinding is van invloed op zowel het registratie- als het verstrekkingenregime van de WPolr en vormt hierdoor een belangrijk aspect van de privacybescherming. Noch de WPolr, noch het BPolr bevat een spiegelbepaling van art. 9 Wbp, op grond waarvan persoonsgegevens niet verder mogen worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor zij zijn verkregen. Middels de verstrekkingenregimes en de reglementen wordt met de WPolr echter indirect toch in de doelbinding voorzien, zoals uit het onderstaande duidelijk moge worden.

### De registratie van gegevens

Toetsing van het doelbindingsbeginsel vindt plaats wanneer gegevens voor een ander doel worden verwerkt dan waarvoor zij zijn vastgelegd. Op grond van art. 4 lid 1 WPolr wordt een politieregister steeds aangelegd voor een bepaald doel. Een registratie van persoonsgegevens in een politieregister is slechts mogelijk voor het doel van dat register<sup>32</sup>. Dat doel dient een bepaalde registratie te rechtvaardigen en maakt een toetsing aan het doelbindingsbeginsel mogelijk. Indien het doel van een politieregister de bestrijding van de zware criminaliteit betreft zal niet snel sprake zijn van strijdigheid met het doelbindingsbeginsel. Er kunnen ook gegevens worden gebruikt die voor een ander doel zijn verzameld. Naarmate het doel van een politieregister echter algemener van aard is, neemt de beperkende werking van de doelbinding navenant toe. In par. 3a WPolr is voor elk van de bijzondere politieregisters een afzonderlijke regeling getroffen voor de registratie van persoonsgegevens. Is de opname van persoonsgegevens in een tijdelijk of een voorlopig politieregister slechts mogelijk met het oog op het doel van die registers, de registratie in een register zware criminaliteit dient samen te hangen met de bestrijding van de zware criminaliteit.

### De verstrekking van gegevens

Voor de gegevens die al in de politieregisters aanwezig zijn komt de vraag naar de doelbinding ter sprake op het moment waarop die gegevens worden verstrekt. Voor het hulpverleningsregister en het register-MOT zijn in het BPolr afzonderlijke doelbindingsbepalingen opgenomen; op grond daarvan worden gegevens uit die registers in beginsel alleen verstrekt voor het doel waarvoor die registers zijn ingesteld. Hetzelfde geldt voor voorlopige politieregister en het tijdelijke politieregister. Wanneer de verstrekking plaatsvindt in het kader van een koppeling met een ander register bepaalt art. 4 lid 2 BPolr voor een tijdelijk politieregister, dat die koppeling voor dat register noodzakelijk moet zijn. Voor een voorlopig politieregister en een register zware criminaliteit is een doelbindingsregeling opgenomen in de modelreglementen van die registers<sup>33</sup>. Hoewel een register zware criminaliteit, evenals de gewone politieregisters, geen specifieke doelbindingsbepaling kent, blijken de gegevens in dat register in de praktijk alleen te worden verstrekt in het kader van de bestrijding van de zware criminaliteit. Dit betekent dat in beginsel enkel de gegevens in de gewone politieregisters<sup>34</sup> binnen de politietaak voor elk doel kunnen worden verwerkt. Hoewel art. 4 lid 2 WPolr in eerste instantie ziet op de registratie van gegevens in een politieregister, heeft het ook betekenis voor de verstrekking ervan; in het

32. Art. 4 lid 2 WPolr.

33. Voor gegevens die uit een voorlopig politieregister worden verstrekt geldt, dat deze niet elders mogen worden vastgelegd. Daarmee wordt voorkomen dat gegevens na de verstrekking alsnog voor een ander doel kunnen worden verwerkt. Dit gevaar bestaat in beginsel wel bij een verstrekking uit een tijdelijk politieregister, nu de WPolr geen nadere beperkingen stelt aan een zodanige verstrekking.

34. Uitzonderd het hulpverleningsregister en het register-MOT.

kader van een koppeling is immers sprake van een verstrekking aan en registratie in een bepaald politieregister (datawarehouse). Volgens genoemd artikel dient een registratie in het kader van een koppeling noodzakelijk te zijn voor het doel van het register waaraan de verstrekking plaatsvindt.

### **De verwerking van gegevens**

Om te komen tot een regeling die afdoende privacywaarborgen biedt voor de verwerking van gegevens in het kader van de opsporing behoeft het doelbindingsbeginsel, evenals het hierna te bespreken noodzakelijkheidsbeginsel, nadere invulling. Zo dient het steeds duidelijk te zijn onder welke omstandigheden wel of niet aan het doelbindingsbeginsel is voldaan. Dat is momenteel bijvoorbeeld niet het geval waar het gaat om de vraag of gegevens die worden vastgelegd in, en voor het specifieke doel van, een voorlopig politieregister ook mogen worden verwerkt in het kader van de bestrijding van de zware criminaliteit in het algemeen. Registratie in een voorlopig politieregister vindt plaats voor een 'eigen' specifiek omschreven doel, dat weliswaar is gerelateerd aan de zware criminaliteit maar daarmee niet volledig overeenkomt. Het is ongewenst dat bepaalde zachte gegevens, die slechts voor specifieke doeleinden mogen worden vastgelegd, middels een ruime interpretatie van de doelbinding alsnog voor een breder gebruik beschikbaar kunnen komen. Het doelbindingsbeginsel vormt dus een belangrijke graadmeter bij de bepaling in hoeverre een verwerking in het kader van de WPolr mogelijk is. Dat geldt voor iedere registratie, verstrekking of andere handeling met betrekking tot gegevens. Dergelijke fundamentele afwegingen dienen in eerste instantie te worden gestuurd door de wetgevende macht en kunnen niet worden overgelaten aan de individuele opsporingsambtenaren.

#### *11.2.1.3 Het noodzakelijkheidsbeginsel*

Naast de doelbinding speelt het noodzakelijkheidsbeginsel een belangrijke rol in de WPolr bij de bescherming van de persoonlijke levenssfeer. Op grond van art. 4 lid 1 WPolr dient de aanleg van een politieregister noodzakelijk te zijn voor een goede uitvoering van de politietaak en op grond van art. 4 lid 2 WPolr dienen de gegevens in een politieregister noodzakelijk te zijn voor het doel waarvoor het register is aangelegd. Voorts is op grond van art. 6 lid 1 een koppeling slechts mogelijk, indien dat noodzakelijk is voor een goede uitvoering van de politietaak. Het noodzakelijkheidsbeginsel beperkt onder meer de mogelijkheid om zachte gegevens voor operationeel gebruik vast te leggen in andere dan de bijzondere registers. Een verwerking van persoonsgegevens is enkel mogelijk wanneer daarvoor een daadwerkelijke noodzaak bestaat. Hiermee moet worden voorkomen, dat opsporingsautoriteiten zonder een aanwijsbare reden (zachte) persoonsgegevens verwerken. Het is de vraag in hoeverre dit criterium voldoende is voor een zo precies geformuleerde wettelijke regeling, dat volledig duidelijk wordt gemaakt onder welke omstandigheden en voorwaarden een bevoegdheid mag worden toegepast. Het noodzakelijkheids criterium lijkt namelijk nauwelijks een beperkende werking te

hebben op het handelen van opsporingsautoriteiten. Het begrip ‘noodzakelijk voor de politietaak’ of ‘noodzakelijk voor het doel van het register’ is voor verschillende interpretaties vatbaar. Hoe rekbaar dit begrip is blijkt bij de totstandkoming van de wet ‘Vorderen gegevens telecommunicatie’<sup>35</sup>. Hier lijkt bij de wetgever zelf ook geen eenduidigheid te bestaan omtrent de precieze invulling van het noodzakelijkheids criterium. In eerste instantie verklaart de wetgever de bevoegdheid tot het verwerken van NAW-gegevens van toepassing op elk strafbaar feit<sup>36</sup> omdat het belang van de opsporing zwaarder weegt dan het belang van de bescherming van persoonsgegevens<sup>37</sup>; met andere woorden: de toekenning van de bevoegdheid wordt als noodzakelijk voor de opsporing beschouwd. Vervolgens wordt in het gewijzigde wetsvoorstel<sup>38</sup> blijk gegeven van een andere visie door te stellen, dat de toepassing van de bevoegdheid (tot het verwerken van NAW-gegevens) voor elk strafbaar feit niet voldoet aan het noodzakelijkheids criterium, en de bevoegdheid vervolgens tot misdrijven te beperken. De motivering is dat het individuele belang van de burger bij de bescherming van zijn persoonsgegevens, voor zover het gaat om strafbare feiten die geen misdrijven zijn, zwaarder dient te wegen dan het algemene belang van de opsporing, ook al zijn die gegevens op zichzelf niet ingrijpend voor de persoonlijke levenssfeer. Hieruit blijkt dat een fundamentele waarborg als het noodzakelijkheidsbeginsel op zichzelf geen waarde heeft wanneer aan de uitleg van dit beginsel geen regels zijn verbonden. Gezien de huidige maatschappelijke situatie is het standpunt verdedigbaar dat het voor de politietaak noodzakelijk is om, met het oog op de dreiging van terrorisme, elke mogelijke gegevensverwerking toe te staan. Aangezien het noodzakelijkheids criterium hierdoor op gespannen voet raakt met het legaliteitsbeginsel<sup>39</sup> is het van belang, om in de WPoI aan dit beginsel een concrete invulling te geven. Vastgehouden kan worden aan het uitgangspunt, dat een verwerking van gegevens noodzakelijk dient te zijn voor een goede uitvoering van de politietaak (voor zover deze de strafrechtelijke handhaving van de rechtsorde betreft). Voor een antwoord op de vraag wanneer dat het geval zal zijn kan aansluiting worden gezocht bij het doelbindingsbeginsel. Een registratie van gegevens is slechts noodzakelijk voor de politietaak wanneer het doel van de registratie die registratie kan rechtvaardigen. Zowel de verstrekking aan een ander register enerzijds, als de verwerking van die verstrekte gegevens anderzijds dienen noodzakelijk te zijn voor het doel waarvoor de informatie wordt verstrekt/verwerkt. Wanneer informatie is verkregen in het kader van een andere politietaak dan waarvoor deze wordt verwerkt zal in beginsel minder snel aan het doelbindingsbeginsel zijn voldaan, waardoor wellicht geen sprake is van een noodzakelijke verwerking in het kader van de politietaak. Op deze

35. *Kamerstukken I*, 2002 /03, 28 059, nr. 187. Inmiddels is deze regeling in het *Staatsblad* verschenen (*Stb.* 2004, 105).

36. *Kamerstukken II*, 2001 /02, 28 059, nr. 3, p. 4.

37. *Kamerstukken II*, 2001 /02, 28 059, nr. 3, p. 11-12 en 20.

38. *Kamerstukken II*, 2001 /02, 28 059, nr. 5, p. 21.

39. Deze kritiek geldt niet alleen voor de toepassing van het noodzakelijkheidsbeginsel in het kader van de WPoI.

wijze wordt middels het doelbindingsbeginsel nader invulling gegeven aan het uitgangspunt dat een verwerking noodzakelijk dient te zijn voor de politietaak.

#### 11.2.1.4 *Het reglement*

Ieder politieregister bevat in beginsel een reglement waarin regels worden gesteld met betrekking tot het doel van het register, de categorie van persoonsgegevens die erin mogen worden opgenomen en de wijze waarop met die gegevens dient te worden omgegaan. Hiermee vormt het reglement een belangrijke uitwerking van de privacywaarborgen in de WPolr en het BPolr<sup>40</sup>. Het heeft een wettelijke grondslag in de WPolr. Daarnaast vormt de betrokkenheid van het CBP bij de totstandkoming van een reglement een extra waarborg voor de persoonlijke levenssfeer. Een reglement biedt voorts de mogelijkheid om de wijze waarop gegevens in een register worden verwerkt aan te passen, zonder dat daarvoor een wetwijziging nodig is. Verder kan in het reglement nader invulling worden gegeven aan het doelbindings- en noodzakelijkheidsbeginsel. Gezien de rol die een reglement kan vervullen binnen de systematiek van de WPolr bij de bescherming van de privacy, kunnen vraagtekens worden geplaatst bij het (tijdelijk) ontbreken van een reglementsplicht voor het tijdelijke politieregister. Omdat toepassing van de huidige reglementsplicht voor een tijdelijk politieregister in beginsel inefficiënt is kan worden overwogen, gebruik te maken van een modelreglement (indien dat tijdelijke register is aangelegd in het kader van een gericht dataminingonderzoek).

#### 11.2.1.5 *Handhaving privacywaarborgen in wet- en regelgeving*

De privacywaarborgen in de WPolr en het BPolr zullen alleen dan effect resulteren, wanneer zij naar behoren kunnen en worden gehandhaafd. De kwaliteit van het beheer van de politieregisters en het toezicht op de naleving van de wettelijke regelingen vormen het sluitstuk op de waarborgen ter bescherming van de persoonlijke levenssfeer. Het CBP onderstreept het belang van een duidelijke wettelijke regeling op dit punt<sup>41</sup>, nu de WPolr momenteel een 'open' beveiligingsreis kent die door iedere beheerder naar eigen inzicht kan worden ingevuld. In dit verband zij gewezen op de Regeling Informatiebeveiliging Politie (RIP)<sup>42</sup>, op grond waarvan een korpsbeheerder<sup>43</sup> een informatiebeveiligingsbeleid dient vast te stellen. Dat beleid dient ertoe te leiden, c.q. ervoor te zorgen dat de omvangrijke gegevensverzamelingen die de politie heeft over natuurlijke personen beveilig-

40. Zo dient op grond van art. 3 BPolr in een reglement uitdrukkelijk toestemming te worden gegeven voor de opname van gevoelige persoonsgegevens en worden beperkingen gesteld aan het gebruik van persoonsgegevens met betrekking tot raseigenschappen. Voor iedere opname van een gegeven als bedoeld in art. 5 WPolr dient een aanduiding betreffende de betrouwbaarheid daarvan te worden opgenomen.

41. CBP 2001.

42. Regeling van 1 april 1997.

43. Voor zover het betreft het KLPD en de ITO; de Minister van Binnenlandse Zaken en Koninkrijksrelaties.

ligd zijn. Daarbij gelden gemeenschappelijke betrouwbaarheidseisen en worden per informatiesysteem of IT-dienst afhankelijkheids- en kwetsbaarheidsanalyses toegepast, die tot maatregelen leiden die in beveiligingsplannen worden vastgelegd<sup>44</sup>. De toelichting op de regeling bevat de volgende alinea:

*‘De complexiteit van het beveiligingsvraagstuk zal nog toenemen naarmate de technologie meer mogelijkheden biedt tot directe communicatie op elk gewenst moment en elke gewenste plaats. In de praktijk zal van deze mogelijkheden gebruik worden gemaakt. Het is daarom noodzakelijk voor de politie aandacht te besteden aan de beveiliging van de informatievoorziening en om de informatiebeveiliging aan te pakken op een gemeenschappelijke basis.’*

Een duidelijke regeling die voorziet in de situatie waarin onheus gebruik van politieke informatie wordt gemaakt, zal reeds een belangrijke preventieve waarborg tegen misbruik vormen. Afgezien daarvan kan in de praktijk reeds gebruik worden gemaakt van Privacy-Enhancing Technologies (PET). Deze privacy-bevorderende technologieën vormen een samenhangend geheel van ICT maatregelen, dat de persoonlijke levenssfeer beschermt door het elimineren of verminderen van persoonsgegevens dan wel door het voorkomen van onnodige en ongewenste verwerking van persoonsgegevens, een en ander zonder verlies van de functionaliteit van het informatiesysteem<sup>45</sup>. Met behulp van ICT kan er onder meer voor worden gezorgd, dat opsporingsambtenaren alleen toegang hebben tot de informatie die zij daadwerkelijk nodig hebben voor een goede uitoefening van hun functie. Desondanks blijft misbruik van de informatiepositie mogelijk. De PEC concludeerde al dat in de praktijk geen inzicht bestaat in de mate waarin koppeling tussen registers plaatsvindt. Het gevoelige karakter van de informatie en het verschil in doelstellingen waarvoor de registers zijn aangelegd vragen om een betere regeling ten aanzien van de toegankelijkheid, die thans bijzonder groot is. Deze problematiek komt ook aan de orde in de studie<sup>46</sup> naar de ‘integriteit in het dagelijks politiewerk’. Hoewel een positief beeld wordt gegeven van de integriteit van de Nederlandse politie in het algemeen, blijkt het misbruik van informatiesystemen voor privégebruik binnen de politie een geaccepteerd verschijnsel. De techniek biedt de mogelijkheden om dergelijk misbruik van de politieke informatiepositie te voorkomen; zo is het mogelijk het gebruik van informatiesystemen bij te houden en te controleren op misbruik.<sup>47</sup>

44. Middelkoop 2002.

45. Zie ook Hes & Borking 1998 en Van Blarckom & Borking 2001.

46. Naeyé e.a. 2004.

47. Zie ook *Rapport Evaluatie wet bijzondere politieregisters* 2004, p. 185.

### *11.2.2 Conclusies en aanbevelingen met betrekking tot het privacyrechtelijke kader voor dataminingonderzoek*

#### **Conclusies**

Het privacyrechtelijk kader voor de toepassing van dataminingonderzoek door de Nederlandse overheid ten behoeve van de opsporingstaak wordt in eerste instantie gevormd door de internationale wet- en regelgeving op dit punt. Op grond daarvan is ten minste een wettelijke regeling vereist die voldoet aan een aantal voorwaarden, die voornamelijk dienen te voorkomen dat ontoelaatbare inbreuken worden gepleegd op de persoonlijke levenssfeer van de burger. In sectie 11.1.3 bleek, dat voor de verwerking van externe gegevens van buiten de politieke sfeer steeds een specifieke wettelijke grondslag is vereist wanneer daarmee inbreuk wordt gemaakt op die persoonlijke levenssfeer. Voor de verwerking van gegevens binnen het politieapparaat is dit niet het geval. De juridische kaders van de WPolr en het BPolr bieden onvoldoende waarborgen ter bescherming van de privacy. De huidige WPolr is gebaseerd op de oude Wpr in plaats van op de Wbp, en richt zich voornamelijk op de registratie in plaats van op de verwerking van gegevens. Maar ook wanneer de wettelijke waarborgen in overeenstemming worden gebracht met de huidige inzichten inzake de privacybescherming dient men zich bewust te blijven van het feit, dat de kwaliteit van het beheer van de politieregisters en het toezicht op de naleving van wettelijke bepalingen een even belangrijke rol spelen bij de privacybescherming.

#### **Aanbevelingen**

##### *a. In het kader van beperkte verwerking van gevoelige en zachte gegevens*

Met het oog op de persoonlijke levenssfeer dient een registratie op grond van bepaalde kenmerken alleen plaats te vinden in aanvulling op andere gegevens en voor zover dat noodzakelijk is voor het doel van het register. In beginsel is hiervan ten minste sprake bij de bestrijding van de zware criminaliteit. Voor een goede uitvoering van de politietak is het noodzakelijk om zachte gegevens op enigerlei wijze voor evaluatiedoeleinden te kunnen vastleggen. Dit dient echter wel op een verantwoorde wijze te gebeuren; aangezien een gewoon politieregister daarvoor onvoldoende waarborgen biedt verdient het aanbeveling, gebruik te maken van een bijzonder politieregister, of ten minste een register met een beperkt verstrekkingenregime. Een bijkomstig voordeel daarvan is dat de gegevens langer dan vier maanden bewaard kunnen worden, ook wanneer deze nog niet als zelfstandig subject in één van de bestaande bijzondere politieregisters kunnen worden opgenomen.

##### *b. In het kader van het doelbindingsbeginsel*

Momenteel voorzien de WPolr en het BPolr in aparte doelbindingsbepalingen voor verschillende handelingen en voor de afzonderlijke registers met betrekking waartoe die handelingen plaatsvinden. Een dergelijke versnipperde (en incomplete) regeling is ineffi-

ciënt en leidt tot onduidelijkheid over de vraag, wanneer precies sprake is van doelbinding.<sup>48</sup> Een regeling in de WPolr moet waarborgen dat de doelbinding van toepassing is op ieder gebruik van gegevens in het kader van de politietaak, waarbij naar een meer directe aansluiting wordt gezocht op art. 9 Wbp. Een dergelijke algemene doelbindingsbepaling zou als volgt kunnen worden geformuleerd:

*‘Een verwerking van gegevens in het kader van de politietaak vindt slechts plaats in overeenstemming met het doel waarvoor de gegevens zijn verkregen.’*

Hiermee worden de afzonderlijke, her en der in de WPolr en het BPolr voorkomende, doelbindingsbepalingen overbodig. In aansluiting daarop kan worden voorzien in een uitzondering op de hoofdregel, op grond waarvan bijvoorbeeld de OvJ kan bepalen dat deze buiten toepassing kan worden gelaten onder bepaalde omstandigheden en indien noodzakelijk voor de uitvoering van het onderzoek. Met het oog op de duidelijkheid en rechtszekerheid is een nadere invulling van het doelbindingsbeginsel noodzakelijk.

*c. In het kader van het noodzakelijkheidsbeginsel*

In principe zal het noodzakelijkheidsbeginsel alleen in samenhang met aanvullende waarborgen als het doelbindingsbeginsel kunnen voorzien in een afdoende bescherming van de persoonlijke levenssfeer. Wanneer de algemene regeling: ‘een verwerking van gegevens dient noodzakelijk te zijn voor een goede uitvoering van de politietaak’ wordt gecombineerd met de in sectie 11.2.1.2 voorgestelde algemene doelbindingsbepaling wordt het volgende resultaat verkregen:

*‘Een verwerking van gegevens dient noodzakelijk te zijn voor een goede uitvoering van de politietaak en vindt slechts plaats in overeenstemming met het doel waarvoor de gegevens zijn verkregen.’*

*d. In het kader van het reglement*

Met het oog op de toegevoegde waarde van een reglement kan worden overwogen, om ten aanzien van een tijdelijk politieregister dat is aangelegd in het kader van een gericht onderzoek, gebruik te maken van het bestaande modelreglement tijdelijke politieregisters. Dit werkt efficiënt en zorgt voor meer eenheid in de wijze waarop gegevens worden verwerkt.

---

48. Zo gaat de WPolr met betrekking tot de gegevens in een register zware criminaliteit ervan uit dat deze zijn bestemd voor operationeel gebruik, terwijl in de praktijk het doelbindingsbeginsel wordt gehanteerd.

*e. In het kader van handhaving privacywaarborgen in wet- en regelgeving*

De bescherming van de privacy dient zich uit te strekken tot iedere verwerking van gegevens. Vanuit dat standpunt bieden de bestaande waarborgen in de WPolr voldoende garantie voor een rechtmatige verwerking van gegevens. Het is evenwel van belang om waarborgen als het doelbindings- en het noodzakelijkheidsbeginsel nader uit te werken, bijvoorbeeld middels de reglementen. Bij een aanpassing van de WPolr dient rekening te worden gehouden met het feit, dat de huidige waarborgen ter bescherming van de privacy<sup>49</sup> de mogelijkheden tot verwerking van gegevens binnen het politieapparaat (in het kader van een dataminingonderzoek) vaak onnodig beperken. Deze gegevens kunnen effectiever worden ingezet, zonder daarmee afbreuk te doen aan de bescherming van de privacy. Een algemene, op iedere vorm van gegevensverwerking van toepassing zijnde, regeling is te verkiezen boven de huidige situatie, waarin voor iedere verwerking een afzonderlijke (waarborg)regeling is vereist. Aanvullend dient, waar nodig, te worden voorzien in een (wettelijke) regeling aangaande de beveiliging van de politieke informatiepositie.

**11.3 Toepassing van dataminingonderzoek ten behoeve van de opsporingstaak**

De WPolr en het BPolr reguleren drie functies die een politieregister kan vervullen, te weten de registratie, de analyse en de raadpleging van gegevens. De wijze waarop de politieregisters in één of meer van deze functies voorzien is onder de huidige wet- en regelgeving in sterke mate bepalend voor de toepassingsmogelijkheden van dataminingonderzoek<sup>50</sup>. Aan de hand van de genoemde functies is onderzocht, op welke wijze de Nederlandse overheid gebruik kan (en mag) maken van het proces van datamining ten behoeve van de opsporingstaak. Daarbij worden aanbevelingen gedaan voor het elimineren van de knelpunten van de bestaande wet- en regelgeving op dit punt.

*11.3.1 Registratie*

In het kader van de registratiefunctie van politieregisters bieden de WPolr en het BPolr geen zelfstandige grondslag voor het vergaren van gegevens.<sup>51</sup> Teneinde in het kader van een dataminingonderzoek gebruik te kunnen maken van externe, buiten de politieke sfeer afkomstige, persoonsgegevens is in beginsel steeds een aanvullende wettelijke grondslag

---

49. Zie hiervoor onder meer sectie 9.2 over de functieverdeling van de bijzondere politieregisters.

50. De functie van registratie ziet op het datawarehouse dat in het kader van een dataminingonderzoek of verwerking tot stand komt. De analysefunctie wordt beïnvloed door de functies van registratie en raadpleging. Hierbij gaat het voornamelijk om het 'eigenlijke datamining' of bewerken van gegevens. Bij raadpleging staat de functie van de politieregisters als informatiebron centraal. De functie van raadpleging hangt ook samen met de vraag, of gegevens in het kader van een dataminingonderzoek mogen worden verstrekt dan wel ontvangen.

51. Aldus ook Corstens 2002, p. 281

vereist<sup>52</sup>. In deze sectie ligt de nadruk op de manier waarop de WPolr en het BPolr voorzien in de registratie van gegevens en de gevolgen daarvan voor de toepassing van dataminingonderzoek. De registratie van gegevens vormt een wezenlijk onderdeel van het proces van datamining. In het kader van een dataminingonderzoek worden gegevens vastgelegd teneinde deze op een bepaald moment te kunnen bewerken. Het geheel van gegevens waarop de bewerking betrekking heeft, wordt in het kader van het dataminingsproces aangeduid als: het datawarehouse. Aangezien een datawarehouse in beginsel kan worden aangemerkt als een politieregister, dient voor de registratie van gegevens in het kader van een dataminingonderzoek aansluiting te worden gezocht bij hetgeen de WPolr bepaalt omtrent de registratie van gegevens. Het is van belang dat de gegevens in een datawarehouse op een verantwoorde wijze worden vastgelegd, daarbij ten minste rekening houdende met de bestaande verstrekkingenregimes.

#### *11.3.1.1 Kwalificatie datawarehouse*

Om te kunnen bepalen welke regels de WPolr en het BPolr precies stellen aan de registratie van gegevens in een datawarehouse, dient dat warehouse te worden gekwalificeerd op basis van het daaraan gelieerde politieregister. Daarbij wordt onderscheid gemaakt tussen een datawarehouse dat tot stand komt in het kader van een ongericht en dat van een gericht dataminingonderzoek.

#### **Ongericht dataminingonderzoek**

Het is niet noodzakelijk om voor ieder dataminingonderzoek ter kwalificatie van het bijbehorende datawarehouse steeds een nieuw politieregister aan te leggen. Voor kwalificatie van het datawarehouse in het geval van een ongericht dataminingonderzoek kan aansluiting worden gezocht bij het politieregister dat het onderwerp vormt van dat onderzoek: het zogenaamde basisregister. Wanneer wordt gestreefd naar een verbetering van de informatiepositie van een bepaald (basis)register middels datamining, biedt dat register in beginsel zelf reeds de benodigde waarborgen voor een legitieme gegevensverwerking. Indien geen gebruik wordt gemaakt van externe gegevens zal de inhoud van het datawarehouse exact overeenkomen met de gegevens in het basisregister, hetgeen de aanleg van een apart datawarehouse overbodig maakt.

Een basisregister volstaat niet meer als kwalificatie van het datawarehouse wanneer zich in het datawarehouse gegevens bevinden, waarop een ander (lees: strikter) verstrekk-

---

52. Naar aanleiding van de bevindingen van de Commissie Mevis 2001 voorziet de wetgever momenteel in de behoefte van opsporingsautoriteiten om op grotere schaal gebruik te kunnen maken van in het bijzonder externe informatiebronnen (*Kamerstukken II*, 29 441, 28 353 en 28 059). In samenhang met deze uitbreiding van bevoegdheden tot gegevensvergaring in het kader van de opsporing en de toenemende bewustwording van de reeds bestaande verwerkingsmogelijkheden, dient een rechtmatige en verantwoorde verwerking van die gegevens middels regelgeving te worden gegarandeerd.

kingenregime van toepassing is. In dat geval zal het basisregister niet meer voorzien in de waarborgen voor een verantwoorde verwerking van de gegevens in het datawarehouse.

Bij een ongericht dataminingonderzoek ter verbetering van de informatiepositie van een bijzonder politieregister of het register-MOT is het mogelijk dat een datawarehouse tot stand komt, dat gegevens bevat waarop afwijkende verstrekkingenregimes van toepassing zijn. Desondanks kan het basisregister dienst doen als datawarehouse, aangezien op deze specifieke politieregisters (basisregisters) een beperkt verstrekkingenregime van toepassing is. De wijze waarop van een basisregister gebruik wordt gemaakt laat de mogelijkheid toe tot verbetering van de informatiepositie van bestaande politieregisters, zonder dat daarvoor ingrijpende aanpassingen noodzakelijk zijn. Daarbij blijven de bestaande verstrekkingenregimes en de daarmee samenhangende privacybescherming gewaarborgd<sup>53</sup>.

### **Gericht dataminingonderzoek**

Bij een gericht dataminingonderzoek is nog geen basisregister aanwezig. Voor een verantwoorde opslag van de gegevens die in het kader van dat onderzoek worden verwerkt dient daarom te worden voorzien in een nieuw register dat dienst doet als datawarehouse. Hiervoor bleek het tijdelijke politieregister de meest voor de hand liggende optie te zijn. Het beperkte verstrekkingenregime van dit bijzondere politieregister maakt het mogelijk dat het (als datawarehouse) gegevens bevat, waarop verschillende verstrekkingenregimes van toepassing zijn. Een punt van aandacht is het ontbreken van een wettelijke reglementsplicht voor een tijdelijk register. Hoewel een reglement op vrijwillige basis kan worden opgesteld, heeft een wettelijke regeling de voorkeur.

#### *11.3.1.2 Beperkende werking functies politieregisters*

De voor de registratie van (politie)gegevens geldende regels werken, onder meer middels het datawarehouse, door op het proces van datamining. De mogelijkheden van een ongericht dataminingonderzoek worden afgebakend door de voor het basisregister geldende regels, die van een gericht dataminingonderzoek voor de regels van een tijdelijk politieregister. In principe wordt hiermee de bescherming van de persoonlijke levenssfeer ook tijdens een dataminingonderzoek gewaarborgd.

Gezien de nauwe samenhang tussen de functies van registratie, analyse en raadpleging binnen de systematiek van de WPolr gelden voor de verwerking van gegevens in het kader van de politietaak niet alleen dezelfde waarborgen, maar ook dezelfde beperkingen.

---

53. Bij een ongericht dataminingonderzoek is de aanleg van een apart datawarehouse vanuit juridisch oogpunt niet noodzakelijk. In beginsel kan dit onderzoek plaatsvinden binnen de kaders van de bestaande politieregisters. De aanleg van een datawarehouse kan evenwel op praktische gronden wenselijk zijn; alvorens toepassing van datamining mogelijk is dient namelijk steeds een kopie (mirror) van het oorspronkelijke register te worden gemaakt.

De keuze voor de wijze van registreren (of kwalificeren van het datawarehouse) is bepalend voor een aantal andere zaken, waaronder het doel van het dataminingonderzoek, de gegevens die in het kader van dat onderzoek verwerkt kunnen worden, het doel waarvoor en de wijze waarop een verstrekking van gegevens mogelijk is en de mogelijkheid om te koppelen met andere gegevens(verzamelingen). Dit zal in het algemeen geen probleem opleveren. In het kader van een ongericht dataminingonderzoek, bijvoorbeeld, worden ter verbetering van de informatiepositie van een gewoon politieregister in beginsel geen gevoelige gegevens verwerkt en zal het open verstrekkingenregime van de gewone politieregisters derhalve geen obstakel vormen voor de toepassing van datamining. De inbreukmakende verwerking van zachte gegevens ten behoeve van de bijzondere politieregisters en het register-MOT wordt gecompenseerd door het beperkte verstrekkingenregime dat op deze registers van toepassing is.

Ten slotte zal de beperking van de analysefunctie, ofwel de mogelijke toepassing van dataminingonderzoek, door de functies van registratie en raadpleging waarin deze registers eveneens voorzien, niet leiden tot een onwenselijke inperking van de mogelijkheid tot het verrichten van dataminingonderzoek. In de bestaande opvattingen omtrent de balans die aanwezig moet zijn tussen de opsporing en de bescherming van de privacy wordt namelijk voorzien door de wisselwerking van de verschillende functies.

De verwevenheid van functies kan echter ook nadelig uitpakken voor de toepassingsmogelijkheden van dataminingonderzoek. De keuze voor een bepaald register ter kwalificatie van het datawarehouse kan bijvoorbeeld een bepaalde analysemogelijkheid in de weg staan die, met het oog op de huidige inzichten inzake opsporing en privacy, wenselijk of zelfs noodzakelijk wordt geacht. De verschillende verstrekkingenregimes van de bijzondere politieregisters staan in beginsel een onderlinge uitwisseling van gegevens tussen deze registers niet toe. Voor de politieke informatiepositie kan een onderlinge vergelijking van de gegevens in deze registers evenwel wenselijk zijn.<sup>54</sup> Hoewel de wetgever positief staat tegenover een koppeling van gegevens in bijzondere politieregisters, blijkt dat in de praktijk slechts beperkt mogelijk te zijn (schema 18).

---

54. Aldus ook *Rapport Evaluatie wet bijzondere politieregisters 2004*, p. 185.

	Tijdelijk politieregister		Voorlopig-politie-register	Register zware criminaliteit	
	Overig	Onverdacht		Overig	Onverdacht
<b>Gegevens omtrent onverdachte personen in tijdelijk politieregister</b>	Doel-binding	Nee	Nee	Doel-binding	Nee
<b>Gegevens omtrent onverdachte personen in register zware criminaliteit*</b>	<b>A</b>	Nee	Nee	Nee	Ja
	<b>B</b>	Doel-binding	Nee	Nee	Ja
<b>Voorlopige politieregister</b>	Doel-binding	Nee	Ja	Ja	Nee

\* Uitgaande van de situaties waarbij deze verwerking niet (A)/wel (B) mogelijk is.

*Schema 18 Koppeling van gegevens omtrent onverdachte personen in bijzondere politieregisters met andere bijzondere politieregisters*

De beperkende werking van de functies van politieregisters doet zich ook gevoelen ten aanzien van het BPS, een gewoon politieregister dat de mogelijkheid biedt om zachte gegevens die nieuw bij de politie binnenkomen ter analyse gedurende een termijn van vier maanden vast te leggen.<sup>55</sup> Ook de functies van het register zware criminaliteit, dat zich bij uitstek leent voor het uitvoeren van uitvoerige analyses ter verbetering van de informatiepositie inzake (met name) de zware criminaliteit, hebben een vergaande beperkende invloed op de toepassingsmogelijkheden van het dataminingsproces. Die invloed gaat met name uit van de strikte registratievoorwaarden en het open verstrekkingenregime. Voor een efficiëntere gegevensverwerking kan een herziening worden overwogen van de wijze waarop de verwerking van gegevens in een register zware criminaliteit en het BPS thans door de WPoI en het BPOI worden geregeld.

### Register zware criminaliteit en het BPS

De stringente regels die van toepassing zijn op het register zware criminaliteit kunnen worden toegeschreven aan de, uit de IRT-affaire gebleken, wildgroei in gegevensverwerking. Sindsdien is de maatschappelijke situatie echter sterk veranderd en worden de bestrijding van de zware criminaliteit en het (inter)nationale terrorisme steeds belangrijker. Was matiging voorheen het uitgangspunt, tegenwoordig is er sprake van een toenemende behoefte en noodzaak om zachte informatie langer te bewaren en (efficiënter) te gebruiken. In dit verband zij ook gewezen op het rapport ‘Gegevensuitwisseling en Ter-

55. Dit wordt voornamelijk veroorzaakt door het open verstrekkingenregime.

rorismebestrijding<sup>56</sup>. Kritische evaluatie van de bestaande regeling van de registers zware criminaliteit is derhalve wenselijk. Ter verbetering van de informatiepositie van een register zware criminaliteit (door middel van ongericht dataminingonderzoek) kan bijvoorbeeld gebruik van gegevens uit het BPS worden overwogen. Onder de huidige wet- en regelgeving is dat uitgesloten en is men voor een analyse van nieuwe gegevens (omtrent onverdachte personen) in het BPS aangewezen op het BPS zelf<sup>57</sup>. Nadeel hiervan is, dat de voor de registratie van gegevens in het BPS geldende termijn van vier maanden onvoldoende kan blijken voor het verrichten van een goede analyse<sup>58</sup>. Een termijnbepaling is evenwel noodzakelijk ter bescherming van de persoonlijke levenssfeer. Overwogen kan worden om op het BPS een beperkt verstrekkingenregime van toepassing te verklaren, waardoor zachte gegevens langer in dit register kunnen worden vastgelegd. Daarmee wordt evenwel het bepaalde in art. 5a lid 1 onder a WPolr doorkruist, dat ziet op het vastleggen van gegevens omtrent onverdachte personen overeenkomstig par. 3a WPolr. Wanneer voor een kortstondige registratie van zachte gegevens wordt gekozen voor een register als bedoeld in par. 3a WPolr, wordt het bepaalde in art. 5a lid 1 onder c WPolr overbodig. Daarbij is het verder de vraag in hoeverre het BPS als bijzonder politieregister nog kan voldoen aan het doel waarvoor het is aangelegd. Met een beperkt verstrekkingenregime worden ook de mogelijkheden om de gegevens in dit register operationeel te checken in vergaande mate beperkt. Dit is onwenselijk aangezien het BPS, naast zachte gegevens, gegevens bevat die steeds voor algemeen gebruik binnen de politie in aanmerking (dienen te) komen. Daarom kan ook een uitbreiding van de analysemogelijkheden van het register zware criminaliteit worden overwogen, in plaats van die van het BPS. Daardoor wordt niet alleen een verbetering van de informatiepositie van dat register bereikt, maar wordt tevens gezorgd voor een efficiëntere verwerking van de gegevens in het BPS.

Een uitbreiding van de analysefunctie is slechts mogelijk, wanneer de functies van raadpleging en registratie van een register zware criminaliteit worden herzien. Een (langere/voortgezette) registratie van gegevens uit het BPS in een register zware criminaliteit is denkbaar, wanneer operationeel gebruik daarvan wordt uitgesloten. Voor de gegevens (uit het BPS) als bedoeld in art. 13a lid 1 onder a, b en d WPolr kan het huidige verstrekkingenregime van een register zware criminaliteit worden gehandhaafd. Voor gegevens die worden vastgelegd in het kader van de bestrijding van de zware criminaliteit maar die (nog) niet in aanmerking komen om als zelfstandig subject in dat register te worden vastgelegd, kan aansluiting worden gezocht op het verstrekkingenregime dat van toepassing is op de gegevens als bedoeld in art. 13a lid 1 onder c WPolr. Door op zachte

56. *Rapport Gegevensuitwisseling en Terrorismebestrijding* 2003.

57. Door middel van een ongericht dataminingonderzoek ter verbetering van de informatiepositie van het BPS.

58. Zie ook Van Bommel 2003.

gegevens in het BPS. het verstrekkingenregime van het voorlopige politieregister van toepassing te verklaren is het mogelijk, deze gedurende een termijn van zes maanden<sup>59</sup> te bewaren in een register zware criminaliteit<sup>60</sup>. Rechtvaardiging van een langere registratieperiode dan de voor het BPS geldende vier maanden kan gevonden worden in het beperkte verstrekkingenregime.

Teneinde gebruik te kunnen maken van gegevens uit het BPS is voorts uitbreiding van de mogelijkheid tot registratie van gegevens in een register zware criminaliteit noodzakelijk. Daartoe kan aansluiting worden gezocht op art. 13 lid 1 en art. 13*b* lid 1 WPolr door te bepalen, dat opname van persoonsgegevens in een register zware criminaliteit plaatsvindt voor het doel waarvoor dat register is aangelegd<sup>61</sup>. Daarbij dient ten aanzien van het register zware criminaliteit onderscheid te worden gemaakt tussen enerzijds de gegevens in dat register die enkel in het kader van een analyse worden vastgelegd (het register zware criminaliteit als datawarehouse) en anderzijds de gegevens die ook voor operationeel gebruik bestemd dienen te blijven (het huidige register zware criminaliteit), beschreven in art. 13*a* lid 1 onder *a*, *b* en *d* WPolr. Hoewel de CIE is belast met de 'informatievoorziening in het kader van de uitvoering van de politietaak voor zover het betreft misdrijven als omschreven in art. 1, lid 1 onder *k* WPolr', sluit dit de (incidentele) verwerking van bedoelde informatie door andere onderdelen binnen de politieorganisatie niet uit; die kunnen daarmee immers ook in aanraking komen en in die gevallen dienen ook zij ervoor te zorgen, dat dergelijke informatie te bestemder plaatse komt. Het is bijvoorbeeld denkbaar, dat de beheerder van het BPS zal zijn betrokken bij de verwerking van aan de bestrijding van de zware criminaliteit gelieerde gegevens.

#### *11.3.1.3 Beperkingen van het reglement*

In sectie 11.2.1.4 is ingegaan op de rol van het reglement binnen de WPolr. In het kader van de registratiefunctie van een politieregister zal het reglement van invloed zijn op het datawarehouse. Het vormt immers een nadere uitwerking van de regels van de WPolr en het BPolr en biedt waarborgen voor een zorgvuldige omgang met persoonsgegevens. Daarmee is het reglement ook in vergaande mate bepalend voor de mogelijkheden van het dataminingonderzoek in het kader waarvan het datawarehouse is aangelegd. Zo wordt de mogelijkheid van een koppeling in art. 6 WPolr afhankelijk gesteld van hetgeen het reglement daaromtrent bepaalt.

---

59. De genoemde termijn van zes maanden geldt voor de registratie van gegevens in een voorlopig politieregister. In de praktijk kan worden geopteerd voor een afwijkende termijn.

60. Overeenkomstig de termijn van het voorlopige politieregister (art. 13*b* lid 5 WPolr).

61. Zie hiervoor art. 1 lid 1 onder *k* WPolr.

Uit dit onderzoek komt naar voren dat (model)reglementen vaak zijn verouderd en niet, of in onvoldoende mate, voorzien in de mogelijkheden van datamining. Bij een eventuele herziening van de bestaande reglementen kan tevens worden gedacht aan specifieke bepalingen inzake de verwerking van de gegevens in een register middels datamining. In het geval (nog) geen sprake is van een reglement, zoals bij een gericht dataminingonderzoek, kan ten behoeve van factoren als uniformiteit, zorgvuldigheid en het toezicht van het CBP, herziening van de regeling inzake het opstellen van een reglement voor een tijdelijk politieregister worden overwogen<sup>62</sup>. De redenen voor het ontbreken van een onmiddellijke verplichting tot het opstellen van een reglement bij een tijdelijk politieregister zijn niet per definitie aanwezig in het geval van aanleg van een register in het kader van een gericht dataminingonderzoek.

#### *11.3.1.4 Raadplegen van het datawarehouse*

Voor de volledigheid wordt in deze sectie ingegaan op het gebruik van de gegevens in een (politieregister dat wordt gebruikt als) datawarehouse. Zoals in het voorgaande reeds werd gesteld, wordt met betrekking tot de gegevens in een politieregister een onderscheid gemaakt naar gegevens die als zelfstandig subject worden geregistreerd en gegevens die worden vastgelegd in het kader van een dataminingonderzoek. Voor de eerste categorie geldt, dat een verwerking daarvan wordt bepaald door de regels die gelden voor dat register. Ten aanzien van de tweede categorie gegevens (welke (nog) niet in aanmerking komen om als zelfstandig subject in het register te worden opgenomen) kan een andere regeling worden gehanteerd. Die opslag dient te worden aangemerkt als het voorbereidend stadium van het verdere dataminingsproces. Het is niet gericht op een directe verstrekking van de daarin opgeslagen gegevens aan derden maar dient slechts het doel van het datawarehouse, het dataminingonderzoek. Een verstrekking van gegevens uit een datawarehouse, afkomstig uit andere politieregisters, is in principe ook niet noodzakelijk. Indien men daarover wil beschikken kan een verzoek worden ingediend tot verstrekking uit het politieregister waaruit zij afkomstig zijn. Aan de hand van het verstrekkingenregime van dat register dient te worden bepaald of een verstrekking mogelijk is. Dit ligt anders wanneer het gaat om gegevens die afkomstig zijn van buiten de politieke sfeer. Die kunnen niet op andere wijze dan middels een verstrekking uit het datawarehouse worden verkregen. Gezien hun ruime registratiefunctie kunnen dergelijke gegevens worden verstrekt aan het register-MOT, of aan een in het kader van een gericht dataminingonderzoek aangelegd tijdelijk politieregister. Beide politieregisters hebben in beginsel enkel een analyserende functie op zowel gegevens die daarin als zelfstandig subject zijn opgenomen, als die welke werden vastgelegd in het kader van een verbetering van de informatiepositie (middels datamining). Gezien de sterke samenhang tussen de analysefunctie en de registratiefunctie van deze registers, is een aanvullende beperking van de verwerking van de gegevens in

---

62. Hierbij kan worden gedacht aan een wettelijke verplichting tot het opstellen van een reglement, waarbij een modelreglement de voorkeur heeft.

beginsel niet noodzakelijk. Het verstrekkingenregime van beide registers – er wordt alleen verstrekt voor het doel van het register – werkt ook door op de gegevens in het datawarehouse, waardoor deze niet zonder meer kunnen worden geraadpleegd. Daarmee worden de waarborgen die de WPolr gehandhaafd. Het kan evenwel het in het kader van de bestrijding van de zware criminaliteit noodzakelijk worden geacht, op ruimere schaal te kunnen beschikken over gegevens (van buiten de politieke sfeer) die in het kader van gericht dataminingonderzoek zijn vastgelegd in een tijdelijk politieregister. In dat geval kan worden overwogen deze gegevens, met inachtneming van de benodigde waarborgen, beschikbaar te stellen middels een verwijzindex.

### *11.3.2 Analysefunctie in de koppelingsregeling van artikel 6 WPolr*

De analysefunctie van een politieregister is mede bepalend voor de wijze, waarop politiegegevens kunnen worden verwerkt. Deze functie is uitgewerkt in de koppelingsregeling van art. 6 WPolr. In deze sectie wordt ingegaan op de reikwijdte van de koppeling en de beperkingen die de regeling ervan stelt aan de toepassing van dataminingonderzoek. Onderzocht is op welke wijze de bestaande koppelingsregeling kan en dient te worden aangepast aan de huidige opvattingen aangaande privacy en opsporing.

#### *11.3.2.1 De koppeling*

De koppelingsregeling vormt een essentieel onderdeel van de bescherming van de persoonlijke levenssfeer binnen de WPolr. Het regelt onder meer of, en zo ja op welke wijze, gegevens die voor een bepaald doel zijn vastgelegd (voor een ander doel) gebruikt kunnen worden; daarmee wordt de vraag beantwoord of verschillende gegevensverzamelingen met elkaar in verband mogen worden gebracht. Het gaat daarbij niet alleen om de onderlinge koppeling van politieregisters, maar ook om de – voor de opsporingspraktijk steeds belangrijker wordende – vergelijking van politiegegevens met gegevens van buiten de politieke sfeer. Ondanks het (toenemende) belang van de koppeling voor de opsporingspraktijk, is de koppelingsregeling nauwelijks uit de verf gekomen omdat nog steeds onduidelijkheid bestaat omtrent de exacte invulling van de regeling. Het begrip ‘koppeling’ wordt op verschillende manieren uitgelegd en ook de wetgever meent, dat het niet om een eenduidig begrip gaat. Dit onderzoek wil aan de hand van de uitwerking van de koppelingsregeling daarover meer duidelijkheid verschaffen, en met name wanneer deze wordt toegepast in het kader van het dataminingsproces. De wettelijke koppelingsregeling van art. 6 WPolr sluit niet aan op de verschillende manieren waarop informatie kan worden bewerkt. Binnen het dataminingsproces ziet koppeling op de fase van de datawarehousing die dient ter voorbereiding van de daaropvolgende vergelijking of bewerking. Onderscheid dient te worden gemaakt tussen bewerken en selecteren; de koppeling in de zin van art. 6 WPolr ziet evenwel uitsluitend op het selecteren van gegevens<sup>63</sup>.

---

63. Art. 1 onder d WPolr.

Voorts is ingegaan op het onderscheid tussen koppeling en raadpleging. Een onderzoek waarbij een bepaalde gedraging centraal staat of zich richt op meerdere personen (waartegen nog geen concrete verdenking bestaat), kan worden aangemerkt als dataminingonderzoek. Een verwerking van externe gegevens vindt daarbij in beginsel plaats in het kader van een koppeling, waarbij het niet alleen kan gaan om een vergelijking van gehele gegevensverzamelingen, maar ook om delen daarvan. Een dataminingonderzoek kan geen betrekking hebben op één enkele persoon. Wanneer een onderzoek uiteindelijk heeft geleid tot een bepaalde naam, zal er in beginsel een verdenking zijn jegens tegen die persoon. Vanaf dat moment verlegt het zwaartepunt van het onderzoek zich van het verzamelen van nieuwe informatie naar het verifiëren van de gevonden informatie. Daarmee is het dataminingonderzoek beëindigd en valt het gebruik van aanvullende gegevens ter verificatie van het gevonden resultaat (de verdenking) onder de noemer raadpleging. Hoewel ervan wordt uitgegaan dat een koppeling steeds betrekking heeft op een onbepaalde groep van personen is onduidelijk, wanneer daarvan precies sprake is. Een gericht dataminingonderzoek in het kader van een verkennend onderzoek in het kader van art. 126gg Sv heeft bijvoorbeeld uitdrukkelijk betrekking op een ‘bepaalde groep van personen’, terwijl daarbij nog steeds sprake kan zijn van koppeling. Het begrip ‘onbepaald’ verdient nadere uitwerking. Als algemene regel kan worden aangehouden dat een verwerking betrekking heeft op een onbepaalde groep van personen, tenzij sprake is van verificatie/raadpleging. Voor een verduidelijking van de koppelingsregeling kan ook aansluiting worden gezocht bij art. 6 lid 2 WPolr; dat bepaalt, dat het reglement dient te voorzien in de mogelijkheid van koppeling. Een ander punt van aandacht is dat de bestaande koppelingsregeling uitgaat van persoonsregistraties, terwijl datamining ziet op een verwerking van persoonsgegevens. Een verruiming van de reikwijdte van de koppelingsregeling op dit punt is daarom gewenst<sup>64</sup>.

#### **Uitwerking doelbindings- en noodzakelijkheidsbeginsel**

Het combineren van gegevens vormt een essentieel onderdeel van de gegevensverwerking in het kader van de politietoek. De koppelingsregeling is bepalend voor de vraag, of verschillende gegevens(verzamelingen) met elkaar in verband mogen worden gebracht. De huidige regeling gaat uit van het noodzakelijkheidsbeginsel door te stellen, dat een koppeling noodzakelijk dient te zijn voor een goede uitvoering van de politietoek. Dit uitgangspunt is voor het tijdelijke politieregister verder uitgewerkt middels een doelbindingsbepaling<sup>65</sup>. Gegevens worden verwerkt voor een bepaald doel. Gegevens die voor eenzelfde doel zijn verzameld kunnen in beginsel in hetzelfde register worden vastgelegd. Koppeling ziet vooral op de situatie waarin gegevens die voor verschillende doeleinden zijn verwerkt met elkaar in verband worden gebracht. Vanuit die optiek kan het bepaalde

64. Zie sectie 11.3.2.2.

65. Art. 4 lid 2 BPolr.

in art. 6 WPolr onder meer worden aangemerkt als een nadere uitwerking van het doelbindingsbeginsel. Het artikel bepaalt wanneer verschillende gegevens(verzamelingen) met ieder een eigen doelstelling (voor een afwijkend doel) gekoppeld mogen worden. Bij een eventuele herziening van het huidige art. 6 WPolr op het punt van verwerking van gegevens<sup>66</sup> dient met deze functie van de koppelingsregeling rekening te worden gehouden. Verder dient te worden gestreefd naar een regeling die duidelijkheid verschaft over de reikwijdte en de toepassing van een dergelijke regeling. Een techniekafhankelijke benadering met voor elke koppelingsvorm een afzonderlijke regeling is, gezien de beperkte houdbaarheid<sup>67</sup> daarvan, ongewenst. Er kunnen zich ook combinaties van koppelingsvormen voordoen, waardoor onduidelijkheid ontstaat over de aard van de koppeling en of in juridische zin wel sprake is van een koppeling. Gezocht moet worden naar een eenduidige, techniekafhankelijke regeling die voorziet in zowel de huidige als de toekomstige toepassingsvormen van koppeling. In de volgende sectie is uiteengezet op welke wijze dit kan worden gerealiseerd.

#### *11.3.2.2 Herziening van de koppelingsregeling*

De bestaande koppelingsregeling dient zodanig te worden verruimd dat deze steeds voorziet in een verantwoorde gegevensverwerking, terwijl de functie die de koppeling vervult als uitwerking van het doelbindingsbeginsel gehandhaafd blijft. In deze sectie wordt voor de afzonderlijke artikelen die op de koppeling betrekking hebben uitgewerkt, hoe dit streven kan worden gerealiseerd. Daarbij gaat het met name om de art. 1 lid 1 sub *d* en 6 WPolr en art. 4 lid 1 BPolr.

#### **Artikel 1 lid 1 sub *d* WPolr**

De WPolr definieert koppeling in art. 1 lid 1 sub *d* als: het treffen van technische of organisatorische voorzieningen waardoor verschillende verzamelingen van persoonsgegevens systematisch met elkaar kunnen worden vergeleken. Het oogmerk van een koppeling is in de regel het verkrijgen van nieuwe informatie over een in beginsel onbepaalde groep van personen, welke informatie niet kan worden ontleend aan één van de betrokken registers afzonderlijk<sup>68</sup>. Onderzoek, waarbij uit verschillende registers gegevens worden verzameld ter verkrijging van nieuwe informatie omtrent een bepaald persoon of een bepaalde groep van personen, is geen koppeling als bedoeld in art. 6 WPolr<sup>69</sup>. In dat geval is sprake van raadpleging, en niet van verstrekking in het kader van een koppeling. Aangezien het begrip ‘koppeling’ in het dagelijks taalgebruik ruim kan worden geïnterpreteerd kan die term, ten behoeve van een betere aansluiting van de bestaande koppe-

---

66. Zie sectie 11.2.1.6.

67. In verband met de technologische turbulentie.

68. *Kamerstukken II*, 1988/89, 19 589, nr. 3, p. 16.

69. *Kamerstukken II*, 1988/89, 19 589, nr. 6, p. 10.

lingsregeling op de opsporingspraktijk en de gegevensverwerking die in het kader daarvan plaatsvindt, in art. 1 lid 1 sub *d* WPoIz beter als volgt worden gedefinieerd:

*‘Het combineren van verschillende (verzamelingen van) persoonsgegevens teneinde een bewerking in het kader van de politietaak mogelijk te maken voor een ander doel dan waarvoor de betreffende gegevens zijn verkregen’.*

Deze formulering maakt een verwerking van gegevens mogelijk die kan leiden tot informatie die zonder de bedoelde combinatie niet aan de betrokken gegevens afzonderlijk kan worden ontleend. Gegevens(verzamelingen) die voor een bepaald doel zijn verzameld kunnen in het aan dat doel gelieerde register worden vastgelegd, waarmee wordt voldaan aan de in sectie 11.2.1.3 beschreven algemene regeling op grond waarvan een verwerking van gegevens noodzakelijk dient te zijn voor een goede uitvoering van de politietaak en slechts plaatsvindt in overeenstemming met het doel waarvoor de gegevens zijn verkregen. Het ‘combineren van persoonsgegevens’ dient te worden onderscheiden van ‘het raadplegen of bevragen van verschillende gegevens of gegevensverzamelingen’. Raadplegen kan worden gedefinieerd als:

*‘Het bevragen van één of meer verschillende (verzamelingen van) persoonsgegevens in het kader van de politietaak voor een ander doel dan waarvoor de betreffende gegevens zijn verkregen’.*

#### **Artikel 6 lid 1 WPoIz**

De wijze waarop koppeling dient plaats te vinden is geregeld in art. 6 WPoIz. Op grond van het eerste lid kan een politieregister alleen worden gekoppeld met een ander politieregister of met een andere verzameling van persoonsgegevens, wanneer dat noodzakelijk is voor een goede uitvoering van de politietaak. Hiermee wordt enkel uitgegaan van een koppeling van een politieregister. In de praktijk behoeft dit echter niet per definitie het geval te zijn. Ter verduidelijking een theoretisch voorbeeld. In het kader van een onderzoek naar de illegale teelt van softdrugs kan een lijst van huishoudens met extreem hoog watergebruik worden vergeleken met een lijst van huishoudens met een zeer hoog stroomverbruik. Adressen die op beide lijsten voorkomen kunnen vervolgens nader worden onderzocht. De lijsten, of externe gegevensverzamelingen, die worden vergeleken zijn geen politieregisters. De gegevens kunnen in het kader van een vergelijking echter wel worden vastgelegd in een tijdelijk politieregister. Er is dan sprake van een koppeling van gegevensverzamelingen waarbij niet wordt uitgegaan van een reeds bestaand politieregister. Van een koppeling als bedoeld in art. 6 lid 1 WPoIz zou sprake zijn wanneer het tijdelijke politieregister al gegevens zou bevatten, bijvoorbeeld een lijst van mensen die eerder in verband met softdrugs met justitie in aanraking zijn geweest. Wanneer een dergelijke lijst van antecedenten wordt vergeleken met de bovengenoemde lijsten is er sprake van een koppeling uitgaande van een politieregister. Voorbijgaande aan de vraag

of een koppeling die niet uitgaat van een bestaand politieregister steeds wenselijk zal zijn, kan worden geopteerd voor een aanpassing van art. 6 lid 1 WPolr die in beide vormen van koppeling voorziet:

*‘Een combinatie van verschillende (verzamelingen van) (persoons)gegevens in het kader van de politietaak (die voor één of meer van de betrokken gegevens leidt tot een verwerking van de betreffende gegevens) voor een ander doel dan waarvoor zij zijn verkregen, is slechts mogelijk indien dit noodzakelijk is voor een goede uitvoering van de politietaak’.*

Deze formulering vormt een bevestiging (herhaling) van het noodzakelijkheidsbeginsel van art. 4 WPolr, zoals uiteengezet in sectie 11.2.1. De term ‘combinatie’ impliceert dat ook delen van gegevensverzamelingen kunnen worden gekoppeld.<sup>70</sup>

#### **Artikel 6 lid 2 WPolr**

Op grond van art. 9 WPolr kan een politieregister, en daarmee een datawarehouse, slechts in werking treden wanneer in een reglement is voorzien. Hierbij is steeds sprake van betrokkenheid van het CBP. In art. 6 lid 2 WPolr wordt de mogelijkheid tot koppeling afhankelijk gesteld van hetgeen daaromtrent in het reglement is bepaald. Daarmee speelt het reglement een belangrijke rol bij de verwerking van gegevens in het kader van de opsporing. Middels het reglement kan voor ieder register afzonderlijk worden aangegeven, op welke wijze de gegevens in het bijbehorende register mogen worden verwerkt. Afhankelijk van de omstandigheden kan worden vastgesteld voor welke doeleinden en met welke andere gegevens(verzamelingen) mag worden gecombineerd en vergeleken. Terwijl het eerste lid van art. 6 WPolr ziet op het noodzakelijkheidsbeginsel (dat middels de doelbinding verder kan worden uitgewerkt), vormt het tweede lid van art. 6 WPolr een directere uitwerking van het doelbindingsbeginsel. Het reglement is immers in grote mate bepalend voor de vraag wanneer verschillende gegevens met elkaar in verband kunnen worden gebracht.

Tijdens dit onderzoek kwam de vraag naar voren of de verplichting om de mogelijkheid van koppeling met een ander register in een reglement vast te leggen alleen geldt voor politieregisters, of ook voor andere registers. Van een koppeling is namelijk slechts sprake wanneer wordt gekoppeld met een andere gegevensverzameling of een deel daarvan; bij een verwerking van gegevens die niet tot enige gegevensverzameling behoren is geen sprake van een koppeling in de zin van art. 6 WPolr<sup>71</sup>. In beginsel kan worden

---

70. Zie ook Verbeek e.a. 1999.

71. Hoewel in dat geval geen sprake is van een koppeling, zal het gebruik van deze persoonsgegevens in beginsel slechts mogelijk zijn op basis van een wettelijke grondslag.

gesteld, dat bij een combinatie van een politieregister met een ander register ten minste het reglement van het politieregister in een koppeling moet voorzien. De WPolr voorziet evenwel niet in een koppeling van (delen van) externe verzamelingen van persoonsgegevens van buiten de politieke sfeer; er zal immers steeds sprake zijn van een verwerking van persoonsgegevens voor een ander doel dan waarvoor zij zijn vastgelegd. Pas wanneer is vastgesteld dat voor een zodanige koppeling een wettelijke grondslag aanwezig is komt de vraag aan de orde, of het reglement van het politieregister waarin de externe gegevens worden vastgelegd in een koppeling, en een verdere verwerking van de gegevens, voorziet. Resumerend kan derhalve worden gesteld, dat op grond van art. 6 lid 2 WPolr de reglementen van de politieregisters dienen te voorzien in de mogelijkheid om te koppelen. De mogelijkheid tot koppeling van een politieregister met een externe gegevensverzameling of een ander politieregister wordt bepaald aan de hand van het reglement. Van welke externe gegevensverzamelingen precies gebruik kan worden gemaakt hangt af van de wettelijke bevoegdheden tot gegevensgaring. Overwogen kan worden, het tweede lid van art. 6 WPolr als volgt aan te passen:

*‘Een combinatie van verschillende (verzamelingen van) persoonsgegevens in het kader van de politietask (die leidt tot een verwerking van de betreffende gegevens) voor een ander doel dan waarvoor zij zijn verkregen, vindt plaats overeenkomstig hetgeen de reglementen van de betrokken politieregisters daaromtrent bepalen. Over die bepalingen wordt het College bescherming persoonsgegevens vooraf gehoord’.*

#### **Artikel 6 lid 3 en 4 WPolr**

Het derde lid van art. 6 WPolr bepaalt dat bij AMvB nadere regels omtrent koppeling worden gesteld ter bescherming van de persoonlijke levenssfeer. Overwogen kan worden de term ‘koppeling’ te vervangen door ‘combinatie’. Hetzelfde geldt voor art. 6 lid 4 WPolr, dat de mogelijkheid openlaat voor de MvJ om in bijzondere omstandigheden af te wijken van het tweede en derde lid van art. 6 WPolr. Een combinatie van gegevensbestanden dient in dat geval plaats te vinden voor de opsporing van een misdrijf waardoor de rechtsorde ernstig is geschokt. Het CBP wordt hierbij eveneens betrokken.

##### *11.3.2.3 Proces-verbaal koppeling*

Op grond van art. 5 BPolr dient van elke koppeling proces-verbaal te worden opge maakt. Daarin moet onder meer zo nauwkeurig mogelijk worden vermeld welke registraties zijn gekoppeld, of de koppeling geleid heeft tot nieuwe persoonsgegevens en zo ja, welke en of die gegevens zijn opgenomen in een register. Teneinde achteraf te kunnen reconstrueren welke handelingen zijn verricht lijkt het wenselijk, om ook met betrekking tot een technisch complex proces als datamining proces-verbaal op te maken. Een dergelijke regeling moet echter wel werkbaar blijven. De wenselijkheid van een proces-verbaal kan worden afgewogen aan de hand van de schaal waarop een koppeling met het oog op de politieke informatiepositie noodzakelijk wordt geacht. Dagelijkse, geautomatiseerde

koppelingen, bijvoorbeeld, zouden kunnen worden uitgezonderd van de plicht van art. 5 BPolr, terwijl complexe en vergaande koppelingen uitgebreid zouden dienen te worden gedocumenteerd.

#### *11.3.2.4 Het reglement*

De reglementen vormen in beginsel een ‘condicio sine qua non’ voor de aanleg van een datawarehouse en de daaropvolgende bewerking. Zij vervullen een belangrijke rol bij de koppeling van gegevens en de bescherming van de persoonlijke levenssfeer. Het belang van een (model)reglement wordt onderstreept door de onderstaande daaraan verbonden essentiële functies.

- Het (model)reglement kan op flexibele wijze voorzien in de specifieke kenmerken van het dataminingsproces als geheel en de verschillende dataminingsvarianten afzonderlijk.
- Het biedt een uitgebreide waarborgfunctie ten aanzien van de persoonlijke levenssfeer, (onder meer) door een uitwerking van het noodzakelijkheids- en het doelbindingsbeginsel.
- Het kan een uniforme gegevensverwerking in het algemeen en de aanleg van een datawarehouse in het bijzonder bevorderen.
- Het werkt tijdsbesparend; met name het modelreglement maakt een efficiënte toepassing van het dataminingsproces mogelijk, hetgeen bij de dataminingsvarianten met een hoge gebruiksfrequentie essentieel is.
- Het CBP is direct betrokken bij de totstandkoming van een modelreglement.

Wanneer een datawarehouse kan worden aangemerkt als een politieregister dient daarvoor, alvorens het in werking kan treden, een reglement aanwezig te zijn. Indien in het kader van het dataminingsonderzoek sprake is van een koppeling in de zin van art. 6 WPolr, wordt daarmee een tweede noodzaak gevormd om in een reglement te voorzien. Naast art. 9 lid 5 WPolr moet dan namelijk ook rekening worden gehouden met art. 6 lid 2 WPolr, dat bepaalt dat het reglement van een register dient te voorzien in de mogelijkheid tot koppeling. Bij het opstellen van de reglementen is uitgegaan van het principe dat een koppeling per definitie een verstrekking met zich meebrengt. Uit dit onderzoek blijkt dat echter per definitie niet het geval te hoeven zijn; door de bestaande (model)reglementen worden de mogelijkheden tot de verwerking van de gegevens in de registers waarop zij betrekking hebben dus onnodig beperkt. De mogelijkheden van een koppeling kunnen worden uitgebreid, zonder dat daarmee afbreuk wordt gedaan aan de verstrekkingenregimes van de verschillende politieregisters. Een herziening van de reglementen op dit punt ligt in het verlengde van de voorgestelde aanpassing van de huidige koppelingsregeling. Met de reglementen wordt voor een belangrijk deel invulling gegeven aan de waarborgen van het daarin opgenomen algemene artikel, dat ziet op de verwerking van gegevens in het kader van de politietaak. Per register, en daarmee ook per

doel waarvoor gegevens zijn vastgelegd, dient het reglement te bepalen of de gegevens in dat register mogen worden gekoppeld. Zo wordt tegelijkertijd geregeld voor welke andere doeleinden de gegevens gebruikt mogen worden.

### *11.3.3 Raadplegen en het (doen) verwerken van gegevens*

Politierregisters vervullen als informatiebron een spilfunctie binnen de opsporing; de mate waarin gegevens mogen worden geraadpleegd hangt onlosmakelijk samen met de verwerkingsmogelijkheden. De raadpleegfunctie van een politieregister is, behalve voor de vraag óf kan worden verstrekt (teneinde de verstrekte gegevens te verwerken) binnen de politie, ook bepalend voor de vraag wie voor het uitvoeren van een verwerking in aanmerking komt.

#### *11.3.3.1 Onderscheid raadplegen en analyseren*

Gegevens worden vastgelegd voor een bepaald doel, en kunnen vervolgens voor dat doel worden geraadpleegd. Regel is dat het doel van een verwerking de daarmee gepaard gaande inbreuk op de persoonlijke levenssfeer rechtvaardigt. Onder bepaalde omstandigheden is het wenselijk dat gegevens in het kader van de opsporing voor een ander doel worden verwerkt dan waarvoor zij zijn vastgelegd. De mogelijkheden daartoe zijn op dit moment beperkt, aangezien het raadplegen van gegevens onlosmakelijk is verbonden aan het doel waarvoor die zijn vastgelegd. In het kader van een koppeling kan dit betekenen dat een verwerking niet mogelijk is. Om een efficiëntere gegevensverwerking door opsporingsdiensten mogelijk te maken, kan een onderscheid worden gemaakt tussen een meer algemeen te raadplegen en een ter analysering dienende registratie. In het laatste geval kan, mits de gegevens niet voor andere doeleinden worden gebruikt, worden uitgegaan van een beperkt(er) verstrekkingenregime. In sectie 11.3.1.2 is aangegeven op welke manier dit kan worden gerealiseerd ten behoeve van het register zware criminaliteit. Het doelbindings- en het noodzakelijkheidsbeginsel zijn in sterke mate bepalend voor de vraag welke gegevens ter registratie en welke ter analyse kunnen worden vastgelegd. Een registratie in het kader van een analyse dient te kunnen worden gerechtvaardigd door het doel van, en noodzakelijk te zijn voor, die analyse. In het kader van de opsporingstaak hangt de hoeveelheid van de in het kader van de opsporingstaak te analyseren gegevens af van de aard van het delict op grond waarvan de analyse plaatsvindt. Bij de bestrijding van de zware criminaliteit is het denkbaar dat alle binnen de politie aanwezige gegevens gebruikt kunnen worden, hetgeen nimmer het geval kan zijn met betrekking tot bijvoorbeeld een fietsendiefstal.

#### *11.3.3.2 Het spanningsveld tussen voor- en nadelen van algemene beschikbaarheid binnen het politieapparaat*

Ten behoeve van de algemene politieke informatiepositie kan het wenselijk worden geacht dat (gevoelige) gegevens die in beginsel zijn vastgelegd voor specifieke doeleinden als de bestrijding van de zware criminaliteit toch algemeen beschikbaar zijn binnen het

politieapparaat. Mogelijk versnipperde informatie kan zo worden samengebracht, waardoor deze efficiënter benut kan worden. Tegenover de voordelen van een ruime beschikbaarheid staat het nadeel van de inbreuk die deze meebrengt op de persoonlijke levenssfeer. Gegevens over een in een voorlopig politieregister geregistreerde persoon zijn onderhevig aan strikte beschikbaarheidsbeperkingen. Om het spanningsveld tussen een ruime(re) beschikbaarheid en de bescherming van de privacy te verkleinen kan worden geopteerd voor een tussenoplossing.

#### *11.3.3.3 Het (doen) uitvoeren van een analyse*

Momenteel is het niet steeds duidelijk wie verantwoordelijk is voor het bereiken van een zo optimaal mogelijke informatiepositie binnen het politieapparaat. In deze sectie wordt nagegaan, op welke wijzen een verbetering van de informatiepositie kan worden nagestreefd.

#### **De gewone politieregisters**

De beheerder van een gewoon politieregister is verantwoordelijk voor het goed functioneren van dat register. Een goede informatiepositie maakt daarvan onderdeel uit en kan worden bereikt door met behulp van ongericht dataminingonderzoek naar mogelijkheden te zoeken voor optimaal gebruik van die gegevens in dat register. Het is echter ook mogelijk, en efficiënter, om in het kader van het dataminingonderzoek aansluiting te zoeken bij andere (soort)gelijke registers binnen de politie, waardoor het resultaat ten goede zal komen aan alle betrokken registers. Vastgesteld moet worden wie of welke instantie een dergelijk overkoepelend onderzoek ter verbetering van de algemene informatiepositie logischerwijze zou dienen uit te voeren.

#### **Het tijdelijke politieregister**

Bij gericht dataminingonderzoek wordt gestreefd naar de verbetering van de informatiepositie in een bepaald geval. De beheerder van een tijdelijk politieregister (dat in het kader van het gericht dataminingonderzoek is aangelegd) is in beginsel verantwoordelijk voor het welslagen van dat onderzoek. Het resultaat van een gericht onderzoek komt ten goede aan dat specifieke onderzoek, waarbij de verkregen kennis – indien van toepassing – in de daarvoor bestemde politieregisters kan worden vastgelegd<sup>72</sup>. Het onderzoek wordt in principe uitgevoerd door gewone opsporingsambtenaren. Een beperking van het verstrekkingenregime is, gezien de aard van de gegevens, niet noodzakelijk. Wanneer een, in het kader van een (datamining)onderzoek aangelegd, tijdelijk politieregister evenwel raakvlakken heeft met de bestrijding van de zware criminaliteit, is de CIE de eerst-aangewezen instantie voor het verrichten van dat onderzoek. Gericht dataminingonder-

---

72. Het tijdelijke register zelf wordt na afloop van het onderzoek vernietigd en is niet bedoeld voor langdurige opslag van verkregen resultaten.

zoek is in beginsel ingrijpender van aard dan ongericht onderzoek. Voor het datawarehouse betekent dit dat er voor het eerstgenoemde onderzoek op ruimere schaal gebruik kan worden gemaakt van bijvoorbeeld gegevens in andere politieregisters. Vooral in geval een onderzoek raakt aan de zware criminaliteit en wordt uitgevoerd door de CIE dient de binnen het politieapparaat aanwezige informatie optimaal te kunnen worden verwerkt. Bij gericht onderzoek is de reikwijdte van de analyse die plaatsvindt in beginsel beperkt tot het doel van dat onderzoek. Het beperkte verstrekkingenregime van een tijdelijk politieregister is met name doeltreffend wanneer het register is aangelegd ter bestrijding van de zware criminaliteit. Bij andere politietaken in een bepaald geval waarvan onder meer sprake kan zijn bij de bestrijding van de kleine criminaliteit, is een beperkt verstrekkingenregime niet noodzakelijk.

#### **Overige bijzondere politieregisters**

Ten slotte kan ook voor de bijzondere politieregisters een verbetering van de informatiepositie worden nagestreefd. Met uitzondering van het tijdelijke register zullen bijzondere registers uitsluitend zijn aangelegd met het oog op de bestrijding van de zware criminaliteit. Voor dat doel kan het noodzakelijk en toelaatbaar worden geacht dat op grote schaal zowel harde als zachte gegevens worden verwerkt. De CIE is verantwoordelijk voor de uitvoering hiervan. Uitgaande van een situatie waarin de gegevens worden vastgelegd in het kader van een analyse (en slechts kunnen worden geraadpleegd in het kader van die analyse) kan worden overwogen, de verschillende bijzondere en overige registers onderling met elkaar in verband te brengen. Een dergelijke verwerking van gegevens in de ruimste zin zal zijn gerechtvaardigd door het daarmee beoogde doel. Het resultaat van een zodanige analyse kan bijvoorbeeld leiden tot een zelfstandige registratie in een register zware criminaliteit en/of aanleiding vormen voor gericht dataminingonderzoek. Op deze wijze vervult de CIE eveneens een coördinerende rol door te zorgen dat informatie (voortkomend uit de beschreven analyse in het kader van de bestrijding van de zware criminaliteit) die voor ander onderzoek of politieregister van belang is, ter bestemde plaats komt.

#### *11.3.4 Conclusies en aanbevelingen in het kader van toepassing van dataminingonderzoek ten behoeve van de opsporingstaak*

##### *11.3.4.1 Conclusies en aanbevelingen in het kader van de registratie*

#### **Conclusies**

De manier waarop de WPolr voorziet in de registratie van politiegegevens beperkt de mogelijkheden voor het verwerken daarvan in het kader van dataminingonderzoek. Bij de regeling van de registratie van gegevens in de politieregisters, die nauw samenhangt met de verschillende functies van die registers, is indertijd aansluiting gezocht op de uitgangspunten van de Wpr en de toenmalige stand van de techniek. Hoewel thans mogelijkheden openstaan om (tegenwoordig vaak essentieel geachte) analyses te verrichten

zonder dat daarbij de privacy in het gedrang komt, worden bepaalde vormen van gegevensanalyse, juist met het oog op het waarborgen van die privacy, door de WPolr en het BPolr uitgesloten.

### **Aanbevelingen**

Door de analysefunctie deels los te koppelen van de functies van registratie en raadpleging, kan in het datawarehouse zodanig onderscheid worden gemaakt tussen een (zelfstandige) registratie ten behoeve van raadpleging en een registratie ten behoeve van analyse, dat geen afbreuk wordt gedaan aan de bestaande privacywaarborgen. In beginsel dienen de gegevens in een datawarehouse alleen te worden verwerkt voor het dataminingonderzoek in het kader waarvan het is aangelegd. Het verdient daarom aanbeveling om voor een datawarehouse uit te gaan van een beperkt verstrekkingenregime.

Ten slotte is het, gezien de rol van het tijdelijke politieregister in het kader van gericht dataminingonderzoek, wenselijk dat ook met betrekking tot dit register wordt voorzien in een bijbehorend reglement.

#### *11.3.4.2 Conclusies en aanbevelingen in het kader van de analysefunctie in de koppelingsregeling van art. 6 WPolr*

### **Conclusies**

Bij het streven naar een zo efficiënt mogelijk gebruik van beschikbare gegevens speelt de koppeling van gegevens(bestanden) een belangrijke rol. De bestaande koppelingsregeling is sterk verouderd en sluit (mede daardoor) veel vormen van gegevensverwerking uit; herziening is dus noodzakelijk.

### **Aanbevelingen**

Een centrale, techniekonafhankelijke regeling moet voorkomen, dat voor iedere denkbare koppelingsvorm een aparte wettelijke voorziening dient te worden gecreëerd. De koppeling dient in hogere mate afhankelijk te worden gesteld van het doelbindings- en het noodzakelijkheidsbeginsel. Deze beginselen kunnen daartoe in de reglementen nader worden uitgewerkt. De voorgestelde herformulering van het begrip koppeling en de daaraan gelieerde wet- en regelgeving biedt enerzijds uitbreiding van de mogelijkheden tot verwerking van gegevens in het kader van de politietaak en garandeert anderzijds dat die verwerking op rechtmatige wijze plaatsvindt.

#### **a. Conclusie en aanbevelingen in het kader van artikel 6 WPolr**

##### *Conclusie*

Hoewel in het vorengaande een aanpassing van het bestaande art. 6 WPolr wordt aanbevolen is het de vraag of en in hoeverre het noodzakelijk is, de koppeling van gegevens in het kader van de politietaak in een afzonderlijk artikel te regelen.

*Aanbevelingen*

Teneinde te voorzien in de benodigde waarborgen die samenhangen met het doelbindings- en noodzakelijkheidbeginsel kan worden volstaan met de in sectie 11.2.1.3 voorgestelde, algemene regeling die bepaalt, dat een verwerking van gegevens noodzakelijk dient te zijn voor een goede uitvoering van de politietaak en slechts plaatsvindt in overeenstemming met het doel waarvoor de gegevens zijn verkregen. Die waarborgen maken de regeling van art. 6 lid 1 WPolr in beginsel overbodig. Desondanks blijft het van belang, de koppeling van gegevens binnen de WPolr apart te benoemen. Hoewel bij zowel raadplegen als bij koppelen een gegevensverwerking plaatsvindt, verschilt de mate waarin daarbij inbreuk wordt gemaakt op de persoonlijke levenssfeer. Het raadplegen van gegevens is in beginsel minder bezwaarlijk dan een koppeling van gegevens. Raadpleging (of verstrekking) kan bij reglement worden geregeld, voor de koppeling geniet een aparte wettelijke benoeming de voorkeur. De voorgestelde, herziene definitie van koppeling<sup>73</sup> vormt een uitzondering op het eerder geformuleerde algemene artikel voor zover dat laatste artikel bepaalt dat een verwerking slechts plaatsvindt in overeenstemming met het doel waarvoor de gegevens zijn verkregen. Een koppeling betekent in beginsel dat gegevens worden gecombineerd (verwerkt) voor een ander doel dan waarvoor zij zijn verkregen. Op grond hiervan kan worden overwogen om de koppeling te regelen in het voorgestelde algemene art. 4 WPolr<sup>74</sup> als uitzondering op de daarin verwoorde hoofdregel. Die uitzondering kan als volgt luiden:

*‘In afwijking van het eerste lid kan worden besloten tot een koppeling (combinatie) van gegevens (voorzover dit noodzakelijk is om een bewerking in het kader van de politietaak mogelijk te maken<sup>75</sup>) als bedoeld in (het aangepaste<sup>76</sup>) art. 1 lid 1 sub d WPolr. Koppeling vindt slechts plaats overeenkomstig hetgeen de reglementen van de betrokken politieregisters daaromtrent bepalen. Over die bepalingen wordt het College bescherming persoonsgegevens vooraf gehoord.’*

Ten aanzien van het derde lid van art. 6 WPolr kan worden overwogen om de daarin neergelegde waarborg ruimer te formuleren. Zo kan worden bepaald dat voor de ver-

73. ‘Het combineren van verschillende (verzamelingen van) persoonsgegevens teneinde een bewerking mogelijk te maken in het kader van de politietaak voor een ander doel dan waarvoor de betreffende gegevens zijn verkregen.’

74. Inhoudende dat een verwerking van gegevens noodzakelijk dient te zijn voor een goede uitvoering van de politietaak en slechts plaatsvindt in overeenstemming met het doel waarvoor de gegevens zijn verkregen.

75. Deze voorwaarde vloeit reeds voort uit de algemene regeling die bepaalt dat een verwerking van gegevens noodzakelijk dient te zijn voor een goede uitvoering van de politietaak en uit de herziene definitie van koppeling.

76. ‘Het combineren van verschillende (verzamelingen van) persoonsgegevens teneinde een bewerking in het kader van de politietaak mogelijk te maken voor een ander doel dan waarvoor de betreffende gegevens zijn verkregen.’

werking van gegevens in het algemeen bij AMvB nadere regels worden gesteld ter bescherming van de persoonlijke levenssfeer. In art. 6 lid 4 WPolr zou kunnen worden vastgelegd, dat de daarin geregelde uitzondering die de MvJ kan maken op de koppelingsregeling betrekking krijgt op hetgeen daaromtrent in de reglementen wordt bepaald.

#### **b. Conclusies en aanbevelingen in het kader van artikel 4 BPolr**

##### *Conclusies*

In het kader van een herziening van de koppelingsregeling verdient ook art. 4 BPolr de aandacht. Dit artikel is op nogal wat punten verouderd en het blijkt de mogelijkheden die dataminingonderzoek biedt onnodig te beperken. Om te beginnen wordt in art. 4 BPolr verwezen naar de Wpr, die al geruime tijd geleden is vervangen door de Wbp en dus niet meer bestaat. Zo is art. 4 lid 1 WPolr is opgebouwd rond het begrip ‘persoonsregistratie’, een begrip dat in de Wbp niet meer wordt gehanteerd. Herziening op dat punt ligt derhalve voor de hand. Voorts worden de mogelijkheden tot gegevensverwerking in vergaande mate beperkt door de uitwerking van de koppelingsregeling in art. 4 lid 1 BPolr: een politieregister mag slechts worden gekoppeld met een ander politieregister of persoonsregistraties van het Rijk, provincies, gemeenten en andere openbare lichamen met inbegrip van de daaronder ressorterende diensten, instellingen en bedrijven<sup>77</sup>. Door deze bepaling wordt de mogelijkheid uitgesloten om twee externe gegevensverzamelingen van buiten de politieke sfeer onderling met elkaar in verband te brengen in het kader van de politietoek. Een koppeling dient immers altijd uit te gaan van een bestaand politieregister. Ook maakt de regeling het onmogelijk om te koppelen met gegevensverzamelingen (of delen daarvan) die niet in art. 4 lid 1 BPolr worden genoemd, terwijl de huidige ontwikkeling in wet- en regelgeving juist tendert in de richting van een veelvuldiger en optimaler gebruik van gegevensverzamelingen die bij derden als verzekeringsmaatschappijen, banken en internetproviders aanwezig zijn. Zelfs wanneer een wettelijke grondslag aanwezig is voor de beschikking over dergelijke externe gegevens, wordt de reikwijdte van die bevoegdheid beperkt tot een raadplegen; een koppeling van of met die gegevens zal op grond van art. 4 lid 1 BPolr ook dan zijn uitgesloten. Met het oog op de huidige privacywetgeving is het maken van onderscheid tussen de verwerking van publieke en niet-publieke gegevensverzamelingen niet langer een vereiste, temeer daar de verwerking van de ene gegevensverzameling niet per definitie meer of minder bezwaarlijk zal blijken te zijn dan een verwerking van de andere. Herziening van art. 4 lid 1 BPolr is derhalve noodzakelijk.

---

77. Een persoonsregistratie als bedoeld in art. 17, aanhef en onder a Wpr.

*Aanbevelingen*

Nu het huidige art. 4 lid 1 BPolr een koppeling met politieregisters zonder meer toestaat kan worden gesteld, dat het artikel met name de koppeling met gegevens(verzamelingen) van buiten de politieke sfeer reguleert. De vigerende beperkingen op dat terrein zijn in het licht van de maatschappelijke en juridische ontwikkelingen onwenselijk. Gestreefd dient te worden naar een regeling die voorziet in de mogelijkheid om (beperkt) gebruik te maken van (koppeling met) gegevens uit zowel de publieke als uit de niet-publieke sector. Tevens dient te worden onderkend dat in het kader van de opsporing ook een combinatie van twee externe gegevensverzamelingen kan plaatsvinden. De vraag naar de mogelijkheid van een koppeling dient zich pas aan wanneer duidelijk is, dat ook daadwerkelijk van de externe gegevens (waarmee wordt gekoppeld) gebruik kan worden gemaakt. Voor een verwerking van de gegevens dient in beginsel een wettelijke grondslag aanwezig te zijn. Voor een verkennend onderzoek, bijvoorbeeld, is in art. 126gg Sv vastgelegd dat de OvJ, indien dat noodzakelijk is voor de uitvoering van het onderzoek, kan bepalen dat de doelbinding (Wbp) met betrekking tot het verkennend onderzoek niet van toepassing is op daarbij nader aan te geven openbare registers die bij wet zijn ingesteld. Vervolgens voorziet de WPolr in de mogelijkheid om die externe gegevens verder te verwerken. Voor de vraag of een koppeling al dan niet is toegestaan kan dus eenvoudig aansluiting worden gezocht op de voorgestelde herziene koppelingsregeling; daarmee wordt de regeling van art. 4 lid 1 BPolr (waarin de mogelijkheid van een koppeling afhankelijk wordt gesteld van de vraag of die koppeling noodzakelijk is in het kader van de politietask en (cumulatief) of de inbreuk die met de koppeling wordt gemaakt opweegt tegen het belang ervan) overbodig. Voor een nadere uitwerking van een dergelijke regeling ter bescherming van de persoonlijke levenssfeer kan, zoals in het kader van de herziening van art. 6 lid 3 WPolr ter sprake kwam, gebruik worden gemaakt van een AMvB.

**c. Conclusies en aanbevelingen Artikel 4 lid 2 BPolr***Conclusies*

Op grond van art. 4 lid 2 BPolr kan een tijdelijk politieregister alleen met een ander register worden gekoppeld indien dat noodzakelijk is voor het doel van het tijdelijke politieregister. Dit betekent dat een eventuele koppeling steeds dient uit te gaan van het tijdelijke politieregister, hetgeen de mogelijkheid van een verwerking van de gegevens in dit register beperkt. Daarom kan worden overwogen de voorwaarde van noodzakelijkheid uit de formulering van art. 4 lid 2 BPolr te schrappen en het artikel als volgt aan te passen:

*‘Koppeling van een tijdelijk register met een ander register vindt slechts plaats in overeenstemming (of voor zover dit niet in strijd is) met het doel waarvoor het eerstbedoelde register is aangelegd.’*

*Aanbevelingen*

Overigens lijkt een aparte regeling voor de verwerking van gegevens in een tijdelijk politieregister, gezien de strekking ervan, overbodig. Het in art. 4 lid 2 BPolr tot uitdrukking gebrachte doelbindingsbeginsel is al geregeld in het voorgestelde algemene artikel inzake de verwerking van gegevens<sup>78</sup>, op grond waarvan een verwerking van gegevens slechts plaatsvindt in overeenstemming met het doel waarvoor de gegevens zijn verkregen. Hierop kon een uitzondering worden gemaakt om een koppeling, welke noodzakelijk is om een bewerking in het kader van de politietaak, mogelijk te maken. De noodzaak kan worden vastgesteld aan de hand van de doelbinding.

*Aanbeveling in het kader van proces-verbaal koppeling*

Teneinde een toetsing achteraf mogelijk te maken kan proces-verbaal worden opgemaakt van een koppeling in die gevallen waarin dat opportuun wordt geacht. Daarbij dient het proces-verbaal betrekking te hebben op de verwerking als geheel en niet, zoals nu het geval is, op de koppeling alleen.

*Aanbevelingen in het kader van het reglement*

Aan de reglementsverplichting kan worden voldaan door voor elk datawarehouse afzonderlijk een reglement vast te stellen, of door gebruik te maken van een modelreglement<sup>79</sup>. Het modelreglement verdient de voorkeur aangezien daarmee op efficiënte wijze kan worden voorzien in de benodigde waarborgen ter voorkoming van ontoelaatbare inbreuken op de persoonlijke levenssfeer van de burger. Het instellen van een directe wettelijke reglementsverplichting is wenselijk ten aanzien van een (in het kader van gericht dataminingonderzoek tot stand gekomen) tijdelijk politieregister. Een dergelijke verplichting zou toegepast moeten worden op ieder tijdelijk politieregister, aangezien een koppeling daarmee altijd afhankelijk is van hetgeen het reglement van dat register daaromtrent bepaalt.

*11.3.4.3 Conclusies en aanbevelingen in het kader van raadplegen en het (doen) verwerken van gegevens***a. Het spanningsveld tussen voor- en nadelen van algemene beschikbaarheid binnen het politieapparaat***Aanbevelingen*

Een tussenoplossing kan worden gevormd door de mogelijkheid, slechts een zeer beperkt aantal gegevens als een naam of enkele zaakskenmerken voor algemeen gebruik beschikbaar te stellen. Wanneer elders binnen het politieapparaat aanvullende informatie blijkt

---

78. Zie sectie 11.2.1.3.

79. Zie art. 12 WPolr.

te zijn geregistreerd in een register zware criminaliteit, dan kan deze vervolgens automatisch beschikbaar worden gesteld aan, in dit geval, de beheerder van het laatstgenoemde register. Op deze wijze kan de aanwezige informatie effectiever worden verwerkt en wordt tevens voorkomen, dat gevoelige informatie voor algemeen gebruik beschikbaar komt. Voor een optimale waarborging van de privacy kan een geautomatiseerd systeem zodanig worden ingericht dat de opsporingsambtenaar daarin slechts melding hoeft te maken van een bepaald gebeuren, waarna het systeem controleert of die melding een match oplevert met bijvoorbeeld een persoon in het register zware criminaliteit en dat vervolgens kenbaar maakt aan de beheerder van het register zware criminaliteit. Hoewel een dergelijk systeem slechts naar één kant werkt kan per geval worden bepaald of, en zo ja op welke wijze, eventuele feedback moet plaatsvinden naar de opsporingsambtenaar. Dat kan bijvoorbeeld van belang zijn wanneer een gesignaleerd persoon vuurwapengevaarlijk is.

#### **b. Analyseactiviteiten met betrekking tot de gewone politieregisters**

##### *Conclusie*

Er moeten regels worden gesteld aangaande de verantwoordelijkheid voor de informatievoorziening binnen de politie voor zover het gaat om de gegevens in de gewone politieregisters. De voorkeur gaat daarbij uit naar een regeling die voorziet in een verplichte, centrale verwerking van gegevens en verspreiding van resultaten.

##### *Aanbevelingen*

Lokale registers kunnen door nationale registers worden vervangen. Het KLPD zou kunnen worden aangewezen voor het analyseren van de gegevens en er tevens op kunnen toezien dat het resultaat, indien van toepassing, in de daartoe aangewezen registers wordt vastgelegd.

#### **c. Analyseactiviteiten met betrekking tot de bijzondere politieregisters**

##### *Conclusie*

Ten behoeve van onder meer een efficiënte bestrijding van de zware criminaliteit dient te worden gestreefd naar een verwerking van gegevens (door de CIE) op centraal niveau. Daarbij kan worden gedacht aan een systeem dat zorg draagt voor directe overheveling van ingevoerde gegevens naar een nationale database.

### *Aanbevelingen*

Een dergelijk systeem kan zo worden ingericht dat gegevens zowel op lokaal als op landelijk niveau geselecteerd c.q. geraadpleegd kunnen worden. In de praktijk betekent dit dat de (lokale) beheerders van de verschillende registers zware criminaliteit niet langer zelfstandig een verbetering van de eigen informatiepositie behoeven na te streven; dit kan dan immers op veel efficiëntere wijze op nationaal niveau door de CIE worden gedaan<sup>80</sup>.

---

80. Dit ligt in de lijn van het streven om de oude Criminele inlichtingendienst (CID) terug te brengen naar zijn oorspronkelijke functie: het verzamelen, bewerken, veredelen en analyseren van criminele informatie en het opslaan en beheren daarvan.

---

## 12 Eindconclusies en aanbevelingen

In dit hoofdstuk zijn de belangrijkste bevindingen van dit onderzoek gerubriceerd. Daarnaast wordt een overzicht gegeven van de meest essentiële aandachtspunten ten behoeve van de verwerking van gegevens in het kader van de opsporing.

### Conclusies

#### a. Privacy

In dit onderzoek naar de toepassing van datamining komt veelvuldig het spanningsveld ter sprake tussen het belang van de opsporing enerzijds en de bescherming van de persoonlijke levenssfeer van de burger anderzijds. Met het oog hierop dient te worden voorzien in een juridisch kader waarbinnen de mogelijkheden van de opsporing ten volle kunnen worden benut en tegelijkertijd waarborgen zijn opgenomen ter bescherming van de privacy. De huidige privacyregels zijn in sterke mate bepalend voor de kaders waarbinnen het dataminingsproces, ofwel de verwerking van gegevens in het kader van de opsporing, dient plaats te vinden. Aangezien de opvattingen inzake opsporing en privacy sedert de totstandkoming van de WPolr en het BPolr sterk zijn verschoven is voor een efficiënte opsporing een ingrijpende aanpassing van die regelingen noodzakelijk.

#### b. Juridisch kader

Een aanpassing van de huidige wet- en regelgeving is niet alleen noodzakelijk met het oog op een afdoende bescherming van de persoonlijke levenssfeer, maar moet ook zorgen voor een betere benutting van de mogelijkheden die de huidige techniek biedt op het vlak van gegevensverwerking. Het ontbreken van specifiek op het dataminingsproces gerichte regelgeving bleek de beperkingen voor de toepassing ervan door opsporingsinstanties niet te verruimen. De bestaande nationale en internationale wet- en regelgeving vormt een juridisch uitgangskader voor de verwerking van gegevens op het vlak van de opsporing, dat afwisselend richtinggevend en richtingbepalend blijkt. Hoewel geen sprake is van een volledig juridisch vacuüm op dit punt noopt het grotendeels verouderde karakter van dit uitgangskader, mede gezien de toegenomen mogelijkheden van en behoefte aan gegevensverwerking in combinatie met de maatschappelijk heersende opvattingen omtrent privacy en veiligheid, tot een aanpassing ervan. Daarbij dient te worden gestreefd naar een zo eenvoudig mogelijke en techniekonafhankelijk geformuleerde regeling, die voorziet in zowel de verwerking van gegevens in het kader van de

opsporing als in de bescherming van de daarmee in het geding gebrachte persoonlijke levenssfeer.

Een verwerking van gegevens in het kader van de politietaak is niet zonder meer mogelijk. Indien de verwerking als niet-ingrijpend wordt aangemerkt, volstaat het algemene art. 2 Politiewet 1993. Wanneer met het gebruik echter een inbreuk op de privacy wordt gemaakt dient daarvoor een specifieke wettelijke grondslag aanwezig te zijn. Hoe groter de inbreuk, hoe strenger de voorwaarden die daaraan worden gesteld. De WPolr is bepalend voor de wijze waarop eenmaal verkregen gegevens verder mogen worden verwerkt. Het juridisch kader daarvoor wordt onder meer gevormd door het doelbindingsbeginsel. Met het oog op de privacybescherming dient steeds rekening te worden gehouden met de doeleinden waarvoor gegevens in eerste instantie zijn verkregen. Daarmee wordt een evenwicht bereikt in het spanningsveld tussen de twee belangen. In dit verband zij ten slotte opgemerkt dat gegevens omtrent onverdachte personen, die zijn verkregen uit onderzoek ten behoeve van de bestrijding van de zware criminaliteit, nu (in beginsel nog) niet onbeperkt kunnen worden verwerkt voor allerlei doeleinden binnen de politie. Die doeleinden zullen immers niet steeds een rechtvaardiging vormen voor de, met de verwerking van de gegevens gepaard gaande, inbreuk op de privacy.

#### **c. Taakverdeling**

Voor een optimaal gebruik van informatie in het kader van de opsporingstaak dient duidelijk te zijn, wie verantwoordelijk is voor welke informatieposities. Het is van belang om informatie zoveel mogelijk op centraal c.q. nationaal niveau te verwerken. De intake van informatie kan hierbij plaatsvinden op lokaal /regionaal niveau terwijl een verdere verwerking (analyse), zeker wanneer deze regio overschrijdend is, plaatsvindt op nationaal niveau. Dit maakt een eenduidige en effectieve verwerking van gegevens mogelijk en voorkomt versnippering van informatie. Het uiteindelijke doel is het bereiken van een centrale informatiepositie binnen de politiekorpsen/opsporingsinstanties/(inlichtingendiensten) ten behoeve van de individuele informatievragers.

#### **d. Techniek**

Ook de techniek kan een sleutelrol vervullen bij het streven naar een rechtmatige en optimale gegevensverwerking. Wanneer gegevens uniform worden verwerkt en onderling uitwisselbaar zijn, kunnen zij ten volle worden benut. Daartoe kan één flexibel systeem zodanig worden ingericht, dat het in zowel de bestaande als de toekomstige behoeften kan voorzien en informatie alleen beschikbaar stelt aan diegenen die daartoe bevoegd zijn. Door verdeling van de bevoegdheden zullen bepaalde gegevens, bijvoorbeeld voor CIE-onderzoek, snel en op eenvoudige wijze beschikbaar komen. De koppeling van bevoegdheden aan de beschikbaarheid van gegevens vormt tevens een waarborg voor een rechtmatige verwerking, waarmee eventuele inbreuken op de privacy tot een minimum

beperkt worden. Controle op de naleving van de wettelijke geregelde waarborgen kan eveneens plaatsvinden met behulp van de techniek.

### **Aanbevelingen**

Onderstaande opsomming behelst de belangrijkste aandachtspunten voor een optimale verwerking van gegevens in het kader van respectievelijk de privacy, de opsporing en de uitvoering van de opsporingstaak. Uitgangspunt hierbij is het streven naar een evenwichtssituatie tussen het recht als instrument voor de overheid en het recht als bescherming van de privacy voor de burger.

#### **a. Privacy**

- Aanpassing van met name de WPolr en BPolr aan de huidige (herziene) opvattingen inzake privacy.
- Uitgaan van de ‘verwerking’ van gegevens.
- Een uitwerking van het doelbindings- en het noodzakelijkheidsbeginsel.
- Inzetten van technologische hulpmiddelen ter waarborging van de privacy en realisatie van bevoegdheden in de praktijk.

#### **b. Opsporing**

- Aanpassing van met name de WPolr en BPolr aan de huidige (herziene) opvattingen en wensen (terrorisme) inzake de mogelijk- en onmogelijkheden van gegevensverwerking.
- Vereenvoudiging van de regeling voor de verwerking van gegevens door te streven naar een algemeen geformuleerde en techniekonafhankelijke regeling.
- Maken van onderscheid tussen raadplegen en analyseren in het kader van het vastleggen van gegevens.

#### **c. Uitvoering**

- Streven naar een uniforme gegevensverwerking binnen de politie, door een wettelijke verplichting tot samenwerking en invoering (daartoe) van één systeem en/of het hanteren van een onderling eenvoudig uitwisselbaar bestandsformaat.
- Duidelijke (wettelijke) taakverdeling en regeling van verantwoordelijkheden.
- Verwerking primair op nationaal en secundair op lokaal niveau.



---

## 13 Beschouwing wetsvoorstel Wet Politiegegevens

Met waardering heb ik kennis genomen van de positieve reactie van de minister<sup>1</sup> op het rapport 'evaluatie wet bijzondere politieregisters'. De in deze evaluatie geconstateerde knelpunten en aanbevelingen stemmen in hoofdlijnen overeen met die welke in dit onderzoek zijn beschreven. De minister geeft aan in beginsel in te stemmen met de gedane aanbevelingen welke inmiddels zijn betrokken bij de totstandkoming van het hierna te bespreken wetsvoorstel Wet Politiegegevens.

Gedurende de afronding van dit onderzoek verscheen het wetsvoorstel Wet Politiegegevens<sup>2</sup>, dat strekt tot integrale herziening van de WPolr. Hierna zal dit wetsvoorstel worden aangeduid als de WPolg (Wet Politiegegevens). Uit de MvT<sup>3</sup> bij de WPolg blijkt dat de wetgever zich bewust is van bestaande knelpunten die uit dit onderzoek naar voren komen en de ontwikkelingen op verschillende terreinen, die een herziening van de huidige wet- en regelgeving op het gebied van de politieke gegevensverwerking wenselijk maken. Met de WPolg wordt beoogd om, zonder aantasting van de beginselen die de bescherming van de privacy ten doel hebben, meer ruimte te bieden aan de verwerking van gegevens ten behoeve van een zo optimaal mogelijke uitvoering van de politietaken. Hiermee wordt volgens de wetgever voorzien in een nieuw evenwicht tussen de bescherming van de privacy van de burger enerzijds en het belang van de rechtshandhaving anderzijds. Hoewel het wetsvoorstel noodt tot een uitgebreide beschouwing, noopt het karakter van een naschrift tot beperkingen. In dit hoofdstuk wordt aandacht besteed aan de eerste twee paragrafen van de WPolg inzake respectievelijk de algemene bepalingen en de verwerking van politiegegevens met het oog op de uitvoering van de politietaken. Hierbij wordt ingegaan op de voor de vraagstelling van dit onderzoek relevante veranderingen die de WPolg ten opzichte van de WPolr met zich meebrengt. Onderzocht wordt of de WPolg oplossingen biedt voor de geconstateerde knelpunten en in hoeverre wordt

---

1. *Kamerstukken II*, 2004/05, 30 001, nr. 1.

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

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

voorzien in een efficiëntere gegevensverwerking door de politie waarbij de bescherming van de persoonlijke levenssfeer afdoende is gewaarborgd.

### 13.1 Algemeen

Deze sectie behelst een beknopte weergave van een aantal belangrijke verschillen tussen de WPolg en de WPolr. Verder wordt ingegaan op de algemene bepalingen als geregeld in de eerste sectie van de WPolg.

De wetgever houdt met de WPolg vast aan een aparte wettelijke regeling voor politiegegevens. Overeenkomstig de WPolr bevat de WPolg geen bevoegdheden tot het verkrijgen van politiegegevens. Het uitgangspunt is een efficiënte en effectieve verwerking van persoonsgegevens, waartoe aansluiting is gezocht op de systematiek van de Wbp. Dit betekent onder meer dat niet langer van het registerbegrip wordt uitgegaan maar van een verwerking van gegevens voor een bepaald doel. Met het vervallen van het registerbegrip verdwijnt het onderscheid tussen de verschillende soorten registers en wordt niet langer gesproken van politieregisters maar van politiegegevens.<sup>4</sup> Hieronder verstaat de wetgever elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon dat in het kader van de uitoefening van de politietaak wordt verwerkt. De vraag kan worden gesteld of de reikwijdte van de WPolg hiermee niet wordt beperkt. In het kader van de politietaak kunnen gegevensverwerkingen plaatsvinden die niet vallen onder het begrip politiegegevens terwijl de verwerking daarvan wel (een wettelijke) regeling behoeft. Het regime van het wetsvoorstel ziet daarmee niet op iedere gegevensverwerking in het kader van de politietaak. In het verlengde hiervan lijkt de definitie van het begrip politiegegevens zich niet te verhouden met het feit dat de wetgever aangeeft dat de politie er in de praktijk wellicht voor kiest om alle gegeven voor het gemak maar als politiegegevens te behandelen. Met de WPolg verdwijnt verder de verplichting om voor een register een reglement vast te stellen, waardoor veel gedetailleerde regelgeving kan komen te vervallen. Dit past volgens de wetgever binnen de stelling dat het wetsvoorstel bijdraagt aan de door het kabinet voorgestane vermindering van het aantal regels en het terugbrengen van de administratieve lasten.<sup>5</sup> De mogelijkheden tot gegevensverwerking worden aanzienlijk uitgebreid. Zo wordt het mogelijk om politiegegevens die voor verschillende doeleinden zijn verwerkt onder voorwaarden met elkaar in verband te brengen; daarbij wordt niet meer gesproken van ‘koppelen’ maar van ‘verwerken, combineren en vergelijken’<sup>6</sup>. De verwerkingsmogelijkheden zullen onder meer worden beperkt door een systeem van autorisaties (voorheen machtigingen) als geregeld in art. 6 WPolg. Met het oog op

---

4. Art. 1 onder *a* WPolg.

5. Het is de vraag in hoeverre dit inderdaad het geval is, aangezien in de (essentie van) de functies die een reglement vervult nu op een andere wijze dient te worden voorzien.

6. Hier zij verwezen naar de in sectie 11.3.2.2 voorgestelde herziening van de koppelingsregeling.

bepaalde maatschappelijke problemen van ernstige aard wordt voorzien in de mogelijkheid van een meer permanente gegevensverwerking. Hierbij kan worden gedacht aan de gegevens die relevant kunnen zijn voor het inzicht in terroristische activiteiten. Het hulpverleningsregister, dat op grond van het BPolr een beperkt verstrekkingenregime kent, krijgt onder de WPolg een open karakter waardoor de gegevens in dat register ook voor andere doeleinden dan de hulpverlening verwerkt mogen worden. Verder vervalt het bestaande onderscheid tussen gegevens aangaande verdachte en onverdachte personen<sup>7</sup>. Voorts wordt in de WPolg onderscheid aangebracht tussen het verwijderen en het vernietigen van gegevens hetgeen eisen stelt aan de praktische toepassing daarvan. Tevens wordt een onderscheid gemaakt tussen het verstrekken en het ter beschikking stellen van gegevens<sup>8</sup>. De hier ontbrekende eenduidigheid wordt wel bereikt waar het gaat om de, nu nog voor een belangrijk deel middels de reglementen geregelde termijn voor het verwerken van gegevens. Ten slotte wordt de naleving van de regels strikter gecontroleerd, enerzijds door middel van privacyfunctionarissen en anderzijds met behulp van de techniek. Het CBP is belast met het toezicht op de naleving van de wet.

In de algemene bepalingen in sectie 1 van de WPolg zijn de belangrijkste uitgangspunten neergelegd inzake de privacybescherming. Doordat deze bescherming zich uitstrekt tot de verwerking van politiegegevens wordt een zo ruim mogelijke bescherming van de persoonlijke levenssfeer gewaarborgd bij gegevensverwerkingen in het kader van de opsporing. De voorwaarden voor een verwerking komen grotendeels overeen met de uitgangspunten voor de ‘verwerking’ van gegevens als geregeld in de huidige WPolr en het BPolr. Een verwerking dient rechtmatig en noodzakelijk te zijn voor een goede uitvoering van de politietaak<sup>9</sup>. Het feit dat onjuiste gegevens worden gecorrigeerd of vernietigd duidt erop dat de beheerder van de gegevens hierin een actieve taak heeft<sup>10</sup>. De voorwaarde dat politiegegevens worden verwerkt voor welomschreven en gerechtvaardigde doelen en voor zover de verwerking van gegevens evenredig is aan het betreffende doel, sluit aan op het huidige art. 4 lid 1 WPolr. Doelafwijkend gebruik is slechts mogelijk voor zover de WPolg daar uitdrukkelijk in voorziet. Het wetsvoorstel bevat geen algemene norm voor doelafwijkend gebruik van politiegegevens. Bovenstaande zaken als noodzakelijkheid, rechtmatigheid en doelbinding zijn grotendeels vastgelegd in de algemene regeling van art. 3 WPolg. Deze regeling sluit goed aan op de in hoofdstuk 11 voorgestelde herziening van art. 4 WPolr. Op grond van dat voorstel dient een gegevensverwerking noodzakelijk te zijn voor een goede uitvoering van de politietaak en vindt deze slechts plaats in overeenstemming met het doel waarvoor de gegevens zijn verkregen. In de WPolg wordt spe-

7. Zie *Kamerstukken II*, 2005/06, 30 327, nr. 3, p. 2 en 10.

8. Art. 1 sub *d* en *e*.

9. Het huidige art. 4 lid 1 en 2 WPolr. Zie ook *Kamerstukken II*, 2005/06, 30 327, nr. 3, p. 3.

10. Het huidige art. 4 lid 3 WPolr.

cifiek aangegeven voor welke doeleinden gegevens in het kader van de politietaak mogen worden verwerkt. Uitgangspunt is dat een gegevensverwerking in overeenstemming dient te zijn met het doel waarvoor de gegevens zijn verkregen. Op die hoofdregel worden, indien noodzakelijk, wettelijk geregelde uitzonderingen toegestaan.<sup>11</sup>

### **13.2 De verwerking van politiegegevens**

Voor de verwerking van politiegegevens hanteert de WPolg niet langer de systematiek van de WPolr, die is gebaseerd op persoonsregistraties ofwel verschillende politieregisters waaraan regels inzake registratie, raadpleging en analyse zijn verbonden. Algemeen geldt dat een verwerking van politiegegevens slechts mogelijk is voor zover dit noodzakelijk is met het oog op een goede uitvoering van de politietaak. De politietaak ziet op het geheel van activiteiten van politieambtenaren. Binnen die overkoepelende taak heeft eenieder zijn of haar eigen deeltaken in het kader waarvan informatie wordt verwerkt voor bepaalde, aan de specifieke taken gerelateerde doeleinden. In beginsel dient iedere verwerking door een politieambtenaar noodzakelijk te zijn voor de specifieke politietaak die wordt vervuld. Het middel dient daarbij te voldoen aan de beginselen van proportionaliteit en subsidiariteit en de verwerkte informatie moet noodzakelijk zijn voor het doel van het onderzoek. Binnen de uitvoering van de politietaak maakt het wetsvoorstel een onderscheid tussen de uitvoering van de dagelijkse politietaak en de gerichte verwerking van politiegegevens. Voorts wordt voorzien in verwerkingsmogelijkheden binnen de politie, de verwerking met het oog op een aantal ondersteunende taken en de controle op en het beheer van informanten:

1. de uitvoering van de dagelijkse politietaak (art. 8);
2. gerichte verwerking van politiegegevens (art. 9 en 10);
  - onderzoek in verband met de handhaving van de rechtsorde in een bepaald geval (art. 9);
  - inzicht in de betrokkenheid van personen bij bepaalde ernstige bedreigingen van de rechtsorde (art. 10);
3. verdere verwerking binnen de politie/ondersteunende taken (art. 11 en 13);
4. het beheer van informanten (art. 12).

Deze doeleinden komen grotendeels overeen met die waarvoor op grond van de WPolr een politieregister kan worden aangelegd. Hierna wordt nader ingegaan op de eerste drie genoemde doeleinden waarvoor op grond van de WPolg een gegevensverwerking mogelijk is. De verwerking die betrekking heeft op het beheer van informanten is buiten beschouwing gelaten.<sup>12</sup>

---

11. Art. 3 lid 3 WPolg.

12. De regeling van het beheer van informanten(gegevens) valt buiten de reikwijdte van dit onderzoek.

### *13.2.1 De dagelijkse uitvoering van de politietaak*

De politie verwerkt gegevens in het kader van de dagelijkse uitvoering van de politiepraktijk, ook wel de basis-politiezorg genoemd. Het betreft gegevens die de politie ter kennis komen tijdens de dagelijkse werkzaamheden en welke voortkomen uit de verschillende onderdelen van de politietaak, zijnde de handhaving van de openbare orde, de strafrechtelijke handhaving van de rechtsorde en de hulpverlening.<sup>13</sup> Deze gegevens worden op dit moment vastgelegd in gewone politieregisters als het BPS. De in art. 8 WPolg geregelde gegevensverwerking in het kader van de dagelijkse uitvoering van de politietaak is vergelijkbaar met het in dit onderzoek beschreven ongericht dataminingonderzoek met betrekking tot gewone politieregisters.

#### **Gegevens omtrent onverdachte personen**

Het vastleggen van gegevens omtrent onverdachte personen geschiedt thans op tijdelijke basis in een gewoon politieregister, teneinde deze 'operationeel te checken'<sup>14</sup>; deze beperking is opgelegd met het oog op de bescherming van de persoonlijke levenssfeer. Onder de WPolg mogen alle gegevens die zijn verwerkt in het kader van art. 8 gedurende één jaar na de eerste verwerking, met inachtnaam van de algemene beperkingen, vrij binnen de politie worden verwerkt ten behoeve van de dagelijkse uitvoering van de politietaak. Hierbij worden geen beperkingen gesteld aan de wijze waarop de gegevens met elkaar in verband worden gebracht. Na een jaar blijven de gegevens nog vier jaar beschikbaar voor raadpleging. Indien dit noodzakelijk is kunnen zij geautomatiseerd worden vergeleken of onder voorwaarden met elkaar worden gecombineerd. Door het gedurende langere tijd vastleggen van deze basis politie-informatie kunnen soms verbanden worden gelegd tussen feiten en gebeurtenissen die tevoren niet helder waren en van groot belang kunnen zijn voor de taakuitvoering van de politie. Hoewel een dergelijke verruiming van de huidige termijn in het kader van een betere operationele controle in de rede lijkt te liggen is een kritische toetsing van de voorgestelde regeling aan de beginselen van proportionaliteit en subsidiariteit gewenst, evenals een duidelijke uitwerking van het doelbindings- en het noodzakelijkheidsbeginsel. Ten aanzien van de ruime mogelijkheden die art. 8 WPolg biedt voor de verwerking van gegevens omtrent onverdachte personen is het de vraag of deze worden gerechtvaardigd door het belang van de dagelijkse politietaak. Een langdurige en vergaande verwerking van gegevens lijkt eerder voorbehouden aan de bestrijding van de zwaardere criminaliteit. Het onderscheid tussen gegevens over verdachte en onverdachte personen, blijft vanuit privacyrechtelijk oogpunt een belangrijke rol spelen bij de afweging of een bepaalde verwerking al dan niet gerechtvaardigd is. De mogelijkheid om gegevens omtrent personen die daartoe geen enkele aanleiding hebben gegeven gedurende een jaar lang binnen de politie op zulk een ruime schaal te verwer-

13. Zie sectie 7.3.3.3.2.

14. Zie art. 5a WPolr.

ken, impliceert een vergaande inbreuk op de privacy van de burger. Dit kan deels worden ondervangen door de toegang tot deze gegevens reeds in een eerder stadium te beperken. Daarbij kan worden gedacht aan een methode waarbij gegevens omtrent onverdachte personen weliswaar langer (dan nu het geval is), maar op minder ingrijpende wijze (niet de basispolitiezorg) worden verwerkt. Een optie is de in dit onderzoek<sup>15</sup> voorgestelde regeling ten aanzien van gegevens als bedoeld in art. 5a WPolr, waarbij de betreffende gegevens gedurende een jaar beperkt kunnen worden verwerkt door deze beschikbaar te stellen voor analyse. Opgemerkt zij dat het niet is toegestaan om de gegevens die zijn verkregen in het kader van art. 8 WPolg te vergelijken met grote hoeveelheden openbare of andere externe bronnen. Dit is in strijd met het bepaalde in art. 3 WPolg. In dit onderzoek werd al eerder geconstateerd dat, gezien de algemene informatiepositie van gewone politieregisters, deze categorie gegevens niet mag worden verwerkt in het kader van een ongericht dataminingonderzoek, aangezien het doel van de verwerking de inbreuk die daarmee gepaard gaat niet rechtvaardigt. Voor een zodanige vergelijking is een wettelijke grondslag benodigd.

#### **Geautomatiseerd vergelijken**

Na verloop van een jaar worden de gegevens als bedoeld in art. 8 lid 1 WPolg ‘achter het schot geplaatst’, waardoor zij niet langer vrij binnen de politie beschikbaar zijn ten behoeve van de dagelijkse uitvoering van de politietaak. Op grond van het tweede lid van art. 8 kunnen deze gegevens nog wel geautomatiseerd worden vergeleken met de gegevens als bedoeld in art. 8 lid 1 WPolg om eventuele verbanden aan te tonen. In beginsel is deze verwerking niet aan beperkingen onderhevig. Het begrip ‘vergelijken’ is beperkter dan het begrip ‘verwerken’, waarmee wordt gewaarborgd dat de raadpleging van andere gegevens slechts plaatsvindt op basis van gegevens die in het oorspronkelijke onderzoek, van waaruit andere onderzoeken worden bevestigd, al zijn verkregen. De vergelijking vindt plaats op basis van hit/no hit. Verdergaande zoekmogelijkheden zijn niet toegestaan. De inbreuk op de privacy wordt hiermee zoveel mogelijk beperkt, terwijl een efficiënt gebruik van middelen is gewaarborgd. Bij of krachtens AMvB kunnen regels worden gesteld over de categorieën van gegevens op basis waarvan politiegegevens vergeleken kunnen worden. In de praktijk valt te bezien in hoeverre er van de voorwaarde dat een vergelijking noodzakelijk dient te zijn met het oog op de dagelijkse uitvoering van de politietaak beperkende werking zal uitgaan. Ten eerste is de doelomschrijving (evenals die onder het eerste lid) op zichzelf te ruim om een adequate normerende werking te kunnen hebben. Ten tweede kan worden gesteld dat de bedoelde vergelijking per definitie noodzakelijk is nu deze juist plaatsvindt om eventuele, op voorhand onbekende informatie of verbanden aan te tonen. Omdat de genoemde vergelijking past binnen het streven naar een optimale informatiepositie kan worden overwogen deze standaard te laten

---

15. Sectie 11.3.1.2.

plaatsvinden, zonder de afweging omtrent noodzakelijkheid (nogmaals)<sup>16</sup> te maken. Het resultaat kan worden verwerkt in het kader van de dagelijkse uitvoering van de politietoek. 427

#### Verwerken van gegevens in combinatie met elkaar

Het derde lid van art. 8 WPolg maakt het mogelijk dat gegevens als bedoeld in art. 8 lid 1 WPolg ook na een jaar nog in combinatie met elkaar kunnen worden verwerkt. Deze vorm van verwerken gaat verder dan het hierboven besproken vergelijken en zit dicht tegen analyse aan. Door middel van samengestelde zoekvragen wordt gezocht naar onderlinge verbanden die aanleiding kunnen vormen voor een verwerking op grond van art. 9 of 10 WPolg.

Ook de gegevens die zijn verwerkt in het kader van het hierna te bespreken art. 13 WPolg kunnen hierbij worden betrokken. Opgemerkt zij dat deze gegevens op grond van art. 8 lid 3 WPolg in beginsel niet mogen verwerkt in combinatie met andere gegevens dan die welke zijn verwerkt voor de dagelijkse uitvoering van de politietoek. 427

#### Doelafwijkende verwerking

In de WPolg wordt een doelafwijkende verwerking aangeduid met de term: ‘verdere verwerking’. Nu het begrip ‘verwerken’ ook een ‘verder verwerken’ impliceert<sup>18</sup>, kan dit tot verwarring leiden. Het verdient aanbeveling om in dit verband te spreken van een ‘verwerking voor een ander doel’, als uitzondering op een algemeen doelbindingsbeginsel op grond waarvan gegevens enkel worden verwerkt voor het doel waarvoor zij zijn vastgelegd. Gegevens die zijn verwerkt ten behoeve van de dagelijkse uitvoering van de politietoek. 427

16. Deze wordt ook reeds gemaakt op grond van art. 3 WPolg.

17. Ook de gegevens die zijn verwerkt in het kader van het nog te bespreken art. 13 WPolg kunnen hierbij worden betrokken.

18. De term ‘verwerken’ ziet op alle handelingen met betrekking tot gegevens, waaronder ook toekomstige.

### 13.2.2 *Gerichte verwerking van artikel 9*

Onder de WPolg kan voorts informatie worden verwerkt met als doel het streven naar een verbetering van de informatiepositie in een bepaald geval (gericht dataminingonderzoek), ofwel het gericht verwerken van gegevens. Volgens de MvT is hiervan sprake wanneer de politie overgaat tot gerichte en omvangrijke verzameling van gegevens ten behoeve van een onderzoek met het oog op de handhaving van de rechtsorde<sup>19</sup> in een bepaald geval<sup>20</sup>. Nu wordt gesproken van ‘verwerken’ zijn er geen beperkingen aan de wijze waarop gegevens worden bewerkt. Het moment waarop sprake is van gerichte verwerking in de zin van de WPolg zal veelal samengaan met dat waarop om opsporings-technische of tactische redenen aanleiding bestaat de gegevens binnen de politie af te schermen. Het gericht onderzoek betreft een naar tijd beperkte gebeurtenis of situatie dan wel een serie gebeurtenissen. Het kan gaan om een opsporingsonderzoek, een verkennend onderzoek of de aanpak van de overlast bij een school of een coffeeshop.<sup>21</sup> In beginsel gaat het om onderzoek in het kader waarvan onder de WPolg een tijdelijk politieregister kan worden aangelegd. De toepassing van een gericht onderzoek is onder de WPolg niet langer een keuze maar een verplichting. Dit kan als positief worden ervaren, aangezien hierdoor een beter gebruik zal worden gemaakt van de mogelijkheden die deze verwerkingsvorm biedt voor de opsporing. In het kader van art. 9 WPolg kan onderscheid worden gemaakt tussen twee typen van aan te leggen ad hoc bestanden, namelijk die ter opheldering van een gepleegde specifieke misdaad en die ter verkrijging van informatie over een specifiek criminaliteitsverschijnsel of fenomeen. Op basis van art. 9 WPolg kan de politie, evenals bij een tijdelijk politieregister, in het kader van een gerichte gegevensverwerking allerhande gegevens verzamelen, mits deze van belang zijn voor het onderzoek. De omvang en reikwijdte van de gegevensverwerking wordt begrensd door de doelbinding<sup>22</sup> en de beginselen van proportionaliteit en rechtmatigheid<sup>23</sup>. De gegevensverwerking draagt geen permanent karakter, maar is op grond van de doelbinding in tijd begrensd. Gelet op de uiteenlopende (sub)doeleinden waarvoor een

---

19. De verwijzing naar de handhaving van de rechtsorde impliceert dat het met het oog op de hulpverleningstaak gericht verwerken van politiegegevens over bepaalde personen niet mogelijk is.

20. De aanleiding voor gerichte verwerking kan voortkomen uit de basispolitiezorg (ongericht onderzoek) of uit andere onderdelen van de politietaak, maar kan ook een zelfstandige zijn.

21. Hieronder vallen ook de gegevensverwerkingen in verband met landelijke coördinatieonderzoeken (landelijke verkiezingen) en het bewaken en beveiligen van personen ten aanzien van wie er signalen zijn dat hun gezondheid of leven worden bedreigd. Ministerie van Justitie, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties 2003 (Nota ‘Nieuw Stelsel Bewaken en Beveiligen’).

22. Met het oog op de naleving van het doelbindingsbeginsel dient op grond van het tweede lid van art. 9 WPolg het doel van het onderzoek schriftelijk te worden vastgelegd.

23. Zie art. 3 WPolg.

gerichte gegevensverwerking mogelijk is, zij gewezen op het belang van een goede uitwerking/specificatie van zowel het doelbindings- als het noodzakelijkheidsbeginsel.

#### **Doelafwijkende verwerking**

Op grond van art. 9 lid 3 WPolg kunnen politiegegevens die in het kader van een gericht onderzoek worden verwerkt (na instemming van een bevoegde functionaris) beschikbaar worden gesteld voor verdere verwerking ten behoeve van een ander gericht onderzoek of een verwerking op grond van art. 8, 10 of 12 WPolg. Benadrukt wordt dat de gegevensverwerking als een vorm van eenrichtingsverkeer plaatsvindt en niet als wettelijke grondslag voor de huidige praktijk van gegevensuitwisseling middels MRO/VROS; daartoe dient de weg van art. 11 WPolg te worden bewandeld. Dit roept echter de vraag op of deze mogelijkheid van beschikbaarstelling in de praktijk toegevoegde waarde heeft. Wanneer men niet van (alle) andere onderzoeken op de hoogte is, zal er geen aanleiding tot verstrekking aanwezig zijn. Nieuw ten opzichte van de huidige regeling is dat informatie uit een gericht onderzoek (tijdelijk register) kan worden verstrekt ten behoeve van een ander gericht onderzoek. Opvallend is dat (afgeschermd) informatie uit een gericht onderzoek ook beschikbaar kan komen voor de dagelijkse politietaak. Terughoudendheid lijkt hier echter geboden. Op grond van art. 9 lid 4 WPolg worden de gegevens die in het kader van een gericht onderzoek zijn verwerkt verwijderd, indien deze niet langer noodzakelijk zijn voor dat onderzoek. Overeenkomstig de huidige regeling is dat in beginsel het moment waarop het doel van het onderzoek is bereikt. De WPolg verschaft evenwel de mogelijkheid de gegevens nog gedurende een periode van maximaal een half jaar na afloop van het onderzoek te doen verwerken teneinde na te gaan, of deze aanleiding geven tot nieuw gericht onderzoek als bedoeld in art. 9 of 10 WPolg. Het lijkt overigens onwaarschijnlijk dat opsporingsambtenaren van deze mogelijkheid geen gebruik zouden maken. Eenmaal verwijderde gegevens worden niet direct vernietigd, maar zijn niet langer beschikbaar voor operationele doeleinden. In art. 14 WPolg wordt bepaald onder welke voorwaarden de verwijderde gegevens alsnog kunnen worden verwerkt en hoe lang zij mogen worden bewaard alvorens te worden vernietigd.

#### *13.2.3 Gerichte verwerking van artikel 10*

Een gerichte gegevensverwerking kan ook plaatsvinden op grond van art. 10 WPolg. In tegenstelling tot art. 9 WPolg staat daarbij niet zozeer de gebeurtenis of situatie centraal, alswel de opbouw van de informatiepositie (pro actieve functie) en heeft de verwerking een meer permanent karakter. Een zodanige gegevensverwerking wordt noodzakelijk geacht omdat de politie een informatiepositie moet opbouwen teneinde zicht te krijgen en te behouden op ontwikkelingen en verschijnselen als zware criminaliteit, terrorisme en verstoringen van de openbare orde, die een ernstige bedreiging van de rechtsorde dan wel de openbare orde kunnen vormen. Door middel van omvangrijke en op bepaalde personen gerichte gegevensverzameling wordt getracht een beeld te krijgen van de betrokkenheid van die personen bij handelingen of misdrijven van een bepaalde ernst.

Een dergelijk min of meer permanent proces van analyse leidt tot het vastleggen van gegevens over veelal (nog) onverdachte personen. Op basis van de informatiepositie kan worden besloten tot een operationeel opsporingsonderzoek, dan wel tot operationele maatregelen in de sfeer van de openbare orde.<sup>24</sup> Een verwerking als bedoeld in art. 10 WPolg vindt enkel plaats door daartoe geautoriseerde politieambtenaren. Uit dit onderzoek<sup>25</sup> komt naar voren dat een register zware criminaliteit geschikt is voor het (langdurig) analyseren van gegevens ter verbetering van de (algemene) informatiepositie op het gebied van de zware criminaliteit. Registratie is mogelijk in de gevallen benoemd in art. 1 lid 1 onder *k* WPolr. De door de huidige wet- en regelgeving opgelegde vergaande beperkingen van dergelijke analyses lijken te worden versoepeld met art. 10 WPolg. De wetgever merkt de verwerking die in dat kader plaatsvindt aan als een gerichte verbetering van de informatiepositie nu het, evenals bij art. 9 WPolg, handelt om een gerichte en omvangrijke verwerking van persoonsgegevens. Redenerend vanuit de bevindingen van dit onderzoek moet de ‘gerichtheid van de verbetering van de informatiepositie’ in het kader van de verwerking van art. 10 WPolg evenwel worden betwijfeld. Hoewel bij de bestrijding van de zware criminaliteit sprake is van een gerichte doelstelling, strekt de reikwijdte van de verwerking zich uit voorbij een specifiek geval. De verwerking is gericht op een verbetering van de informatiepositie van een politieregister dat in algemene zin ziet op de bestrijding van de zware criminaliteit als geheel. Een dergelijke verwerking heeft in zoverre kenmerken van een gerichte verwerking dat de inbreuk die ermee wordt gemaakt veel ingrijpender is dan normaliter bij een ongericht onderzoek het geval is. Bovendien heeft de verwerking van art. 10 WPolg een meer permanent karakter, nu de betrokkenheid van bepaalde personen bij bepaalde ernstige strafbare feiten of bij handelingen die relevant zijn voor het inzicht in bedreigende maatschappelijke problemen dan wel die de openbare orde bedreigen in de beschouwingen wordt betrokken. Een permanent karakter is in dit onderzoek juist kenmerkend voor de ongerichte gegevensverwerking. In tegenstelling tot art. 9 WPolg zijn de categorieën van personen over wie in het kader van art. 10 WPolg gegevens kunnen worden verwerkt, wettelijk ingekaderd. Hiermee blijven de beperkingen die na de IRT-affaire zijn gesteld aan de registratie van CIE-subjecten in beginsel gehandhaafd. De ruime doelstelling van art. 10 WPolg wordt in het eerste lid nader gespecificeerd. Een verwerking is mogelijk met het oog op het verkrijgen van inzicht in de betrokkenheid van personen bij:

*a. het beramen of plegen van misdrijven:*

*1° als omschreven in artikel 67, eerste lid van het Wetboek van Strafvordering, die in georganiseerd verband worden beraamd of gepleegd en die gezien hun aard of*

---

24. *Kamerstukken II*, 2005/06, 30 327, nr. 3, p. 12.

25. Sectie 9.6.

- de samenhang met andere misdrijven die in het georganiseerde verband worden beraamd of gepleegd, een ernstige inbreuk op de rechtsorde opleveren, of;*
- 2° waarop naar de wettelijke omschrijving een gevangenisstraf van acht jaar of meer is gesteld, of;*
- 3° als omschreven in artikel 67, eerste lid van het Wetboek van Strafvordering, die bij algemene maatregel van bestuur zijn aangewezen en die gezien hun aard of samenhang met andere door de betrokkene begane misdrijven een ernstige inbreuk op de rechtsorde opleveren.*

Met het criterium onder *a* wordt bedoeld op de zogenaamde CIE-taak. Deze regeling is letterlijk overgenomen van genoemd art. 1 lid 1 onder *k* WPolr inzake de registratie in een register zware criminaliteit. In de gevallen, genoemd in art. 10 lid 1 onder *a* WPolg is een doelafwijkende verwerking mogelijk van gegevens die zijn verkregen in het kader van de art. 8 en 9 WPolg ter verkrijging van inzicht in de betrokkenheid van personen bij het beramen of plegen van genoemde misdrijven. Hierbij is ten aanzien van de gegevens die zijn verkregen in het kader van art. 9 WPolg een schifting mogelijk nu een bevoegde functionaris toestemming dient te geven voor verdere verwerking. In art. 10 lid 2 WPolg wordt de verwerking van politiegegevens als bedoeld in art. 10 lid 1 onder *a* WPolg beperkt tot een beperkte categorie van personen. Hiermee is aansluiting gezocht op het huidige art. 13a lid 1 WPolr.

Echter, een verwerking in dit kader is op grond van art. 10 lid 2 sub *c* WPolg ook mogelijk ten aanzien van personen die in een bepaalde relatie staan tot degenen, bedoeld in onderdeel *b*, dat handelt over de zogenaamde themaverwerking. Hiermee wordt het aantal mogelijk vast te leggen personen uitgebreid. Dit lijkt haaks te staan op de stelling van de wetgever dat op het punt van de verwerking van gegevens over CIE-subjecten niet wordt beoogd om te komen tot verruiming van de wettelijke mogelijkheden tot opslag van gegevens.<sup>26</sup>

### **Themaverwerking**

Politiegegevens kunnen ook gericht worden verwerkt met het oog op het verkrijgen van inzicht in de betrokkenheid van personen bij:

- b. 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.*<sup>27</sup>

26. Kamerstukken II, 2005/06, 30 327, nr. 3, p. 50.

27. Het bepaalde in art. 10 lid 1 onder *c* WPolg blijft hier buiten beschouwing.

Het CBP spreekt ten aanzien van het doel als omschreven in art. 10 lid 1, aanhef en onder *b* WPolg over ‘themaverwerking’. Binnen de politie worden daartoe zogenaamde informatieknooppunten opgericht die worden belast met het bijeenbrengen van relevante gegevens over bepaalde aandachtsgebieden. Op landelijk niveau vindt een dergelijke gegevensverwerking plaats bij het KLPD, meer specifiek de DNRI, waar op meer permanente basis gegevens bijeen worden gebracht inzake bepaalde delictsgebieden als mensensmokkel<sup>28</sup> of milieucriminaliteit. De introductie van themaverwerkingen hangt samen met het verdwijnen van het voorlopige politieregister. Het voorgestelde wettelijke regime biedt de mogelijkheid tot verwerking van politiegegevens met het oog op het verkrijgen van inzicht in de betrokkenheid van personen bij bepaalde ernstige misdrijven of handelingen die relevant zijn voor het inzicht in bedreigende maatschappelijke problemen dan wel die de openbare orde bedreigen, zonder dat bij voorbaat restricties gelden ten aanzien van de mate van betrokkenheid van die personen. Aan de introductie van de themaregisters ligt de behoefte ten grondslag om gegevens omtrent onverdachte personen gedurende langere tijd te kunnen verwerken voor specifieke ‘thema’s’ binnen de opsporing, zoals terrorismebestrijding. Dergelijke gegevens kunnen nu worden vastgelegd in een tijdelijk politieregister of een register zware criminaliteit. In het geval van een tijdelijk politieregister zijn de verstrekkingmogelijkheden echter beperkt en dient een verwerking in beginsel steeds te zijn gebaseerd op een specifiek onderzoek. De doelstelling van een register zware criminaliteit is aanmerkelijk ruimer dan die van een tijdelijk register en sluit daarmee goed aan op de mogelijkheid van themaverwerking. Voorts biedt het register zware criminaliteit de mogelijkheid tot gegevensregistratie gedurende langere tijd en zijn de mogelijkheden tot verstrekking ruimer. Voor een zelfstandige registratie in dit bijzondere politieregister gelden echter strikte criteria met het oog op de inbreuk die hiermee wordt gemaakt op de persoonlijke levenssfeer. Omtrent de personen in een register zware criminaliteit kunnen weliswaar alle denkbare vormen van informatie worden opgenomen (open bronnen, informatie uit het buitenland, informatie als gevolg van observatie of afkomstig van informanten) maar de mogelijkheid tot registratie van de persoon op zich is beperkt. Het themaregister, geïntroduceerd door de werkgroep ‘Wetgeving informatie-uitwisseling’ in het rapport ‘Gegevensuitwisseling en Terrorismebestrijding’, is een tussenvorm van enerzijds de permanente registers waarbij inhoudelijke criteria de mogelijkheid tot opslag van gegevens beperken, maar waarvoor een ruim verstrekkingenregime geldt en anderzijds de tijdelijke registers waarin in het kader van een concreet opsporingsonderzoek in beginsel een onbeperkte hoeveelheid gegevens mag worden opgeslagen doch waarop een beperkt verstrekkingenregime rust. De wetgever lijkt met art. 10 lid 1 onder *b* WPolg aansluiting te hebben gezocht bij dit voorstel.

---

28. Inmiddels DNR.

De mogelijkheid tot de aanleg van themaregisters is een reden voor het verdwijnen van het voorlopig politieregister. De gegevens die in het laatstgenoemde register werden vastgelegd kunnen nu worden verwerkt in het kader van art. 10 WPolg. Een essentieel verschil met de huidige voorlopige politieregisters is dat er op grond van art. 10 WPolg niet enkel sprake is van een bevoegdheid tot registratie maar van een bevoegdheid tot verwerking. Dit betekent dat persoonsgegevens verwerkt kunnen worden zonder dat voldaan is aan de voorwaarden die nu gelden voor een registratie in een register zware criminaliteit. Hiermee wordt de mogelijkheid tot registratie in een register zware criminaliteit (onder de WPolg een verwerking op grond van art. 10) verruimd. Tegelijkertijd wordt hiermee de belangrijkste reden weggenomen waarom een register zware criminaliteit niet geschikt zou zijn als themaregister. Gegevens over onverdachte personen die momenteel niet in aanmerking komen voor opslag in een register zware criminaliteit maar wel relevant kunnen zijn voor de bestrijding van terrorisme, kunnen dan wel in aanmerking komen voor opslag (in een register zware criminaliteit).

De WPolg bevat geen zelfstandige grondslag tot gegevensgaring maar geeft de kaders aan voor de verwerking van gegevens die zijn verkregen op basis van een wettelijke regeling. Op grond van art. 10 lid 1 onder *b* WPolg kan een gegevensverwerking plaatsvinden met het oog op het verkrijgen van inzicht in de betrokkenheid van personen bij 'handelingen die kunnen wijzen op het beramen of plegen van bij algemene maatregel van bestuur 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'. Voor de opbouw van een informatiepositie inzake is volgens de wetgever verwerking van gegevens over een ruimere groep personen vereist. Ook gegevens die zijn verkregen in het kader van de art. 8 en 9 WPolg kunnen in beginsel voor dit doel verder verwerkt worden. Deze verwerking wordt in het derde lid van art. 10 WPolg beperkt door te bepalen dat zij enkel plaatsvindt omtrent personen die in een bepaalde relatie staan tot de personen als bedoeld in lid 1 onder *a* en personen die betrokken zijn bij de handelingen als genoemd in lid 1 onder *b*. Deze tweede bepaling lijkt geen beperking maar een bevestiging te zijn van de themaverwerking als bedoeld in art. 10 lid 1 onder *b* WPolg. Voor een verwerking op basis hiervan is het lidmaatschap van een schietvereniging<sup>29</sup> of wellicht het volgen van vlieglessen reeds voldoende. Voor een themaverwerking is niet een redelijk vermoeden van schuld aan ernstige strafbare feiten vereist. Alleen al de betrokkenheid bij handelingen die op het plegen van dergelijke feiten kunnen wijzen is voldoende voor de verwerking. Themaverwerkingen hebben aldus betrekking op onverdachte personen in een proactieve fase. Dit staat op gespannen voet met de eisen van proportionaliteit en subsidiariteit die het internationaal juridisch kader stelt. Burgers die voldoen aan de opnamecriteria voor een themaverwerking worden daarin opgenomen als potentieel

---

29. *Kamerstukken II, 2005/06, 30 327, nr. 3, p. 50.*

dader van zeer ernstige criminaliteit. Alleen al op die grond vormt een dergelijke verwerking van gegevens een groot risico voor hen.<sup>30</sup> In beginsel zal hiervoor sprake dienen te zijn van een wettelijke regeling op grond waarvan een actieve verwerking kan plaatsvinden in het geval er enkel sprake is van handelingen die kunnen wijzen op het beramen of plegen van bij bepaalde misdrijven die door hun omvang of ernst of hun samenhang met andere misdrijven een ernstig gevaar voor de rechtsorde opleveren. In dat geval verdient het de voorkeur om niet de delictomschrijving aan te halen maar, om overeenkomstig art. 10 lid 1 onder *a* WPolg, in meer algemene zin te verwijzen naar de betreffende misdrijven. Het is de vraag of de beoogde doelstellingen in combinatie de waarborgen van sectie 5 WPolg opwegen tegen de mogelijkheid die de WPolg lijkt te bieden om zonder een specifieke wettelijke grondslag gegevens langdurig, doelafwijkend en op een zodanige ruime wijze te verwerken. Op grond van art 10 lid 5 WPolg kunnen de gegevens die in het kader van dit artikel zijn verwerkt, (voor een ander doel) verder worden verwerkt in het kader van de art. 8, 9, 10 en 12 WPolg.

De gegevens die zijn verwerkt op grond van art. 10 lid 1 WPolg dienen uiterlijk vijf jaar na datum van de laatste verwerking te worden verwijderd. Deze voorwaarde lijkt evenwel, gezien de definitie van de term ‘verwerken’, weinig houvast te bieden. In de praktijk leidt iedere verwerking van de gegevens er namelijk automatisch toe, dat de termijn voor verwijdering opnieuw gaat lopen. Gegevens die deel uitmaken van een voortdurende analyse zouden hierdoor (op grond van art. 10 lid 6 WPolg) mogelijk veel langer dan 5 jaar kunnen worden bewaard.

#### *13.2.4 Geautomatiseerd vergelijken en in combinatie zoeken artikel 11*

Op grond van de art. 8, 9 en 10 WPolg kunnen gegevens ter beschikking worden gesteld ten behoeve van ander onderzoek. In deze gevallen is steeds sprake van eenrichtingsverkeer waarbij het initiatief tot verstrekken uitgaat van de oorspronkelijke verwerker. De wetgever maakt het onder bepaalde voorwaarden mogelijk dat in het kader van art. 9 lid 1 WPolg een geautomatiseerde gegevensvergelijking plaatsvindt met gegevens die zijn verwerkt in het kader van art. 8 of 9 WPolg. CIE-gegevens vallen in beginsel buiten deze vergelijking. Ten behoeve van een verwerking als bedoeld in art. 10 lid 1 WPolg wordt deze mogelijkheid in art. 11 lid 2 WPolg uitgebreid tot gegevens die in het kader van art. 10 lid 1 WPolg zijn verwerkt. Het betreft in beide gevallen verificatie waarbij de gegevensvergelijking plaatsvindt op basis van hit/no hit.<sup>31</sup> Zo kan dubbel onderzoek worden voorkomen en wordt overlapping van onderzoek beperkt. Met deze verruiming van

---

30. CBP 2004, p. 28.

31. De vergelijking vindt plaats op basis van een aantal, bij AMvB nader vast te stellen categorieën van gegevens.

de verwerkingsmogelijkheden lijkt een wettelijke basis te worden gegeven aan de huidige praktijk, die deze inzichten verschaft middels verwijsindexen als MRO en VROS.

De mogelijkheid om te zoeken op basis van gegevensvergelijking impliceert zowel een verruiming als een beperking van de huidige verwerkingsmogelijkheden. Op basis van de WPolr kan in het kader van een gericht onderzoek in beginsel steeds gebruik worden gemaakt van gegevens die zijn vastgelegd in gewone politieregisters. Op grond van de WPolg mag enkel nog aan de hand van bepaalde gegevens een verwerking (vergelijking) plaatsvinden van gegevens die zijn verwerkt met het oog op de dagelijkse uitvoering van de politietaak; juist met betrekking tot die gegevens lijkt het echter wenselijk, dat deze tot het moment van verwijdering optimaal operationeel kunnen worden aangewend. Deze beperking geldt ook voor een verwerking als bedoeld in art. 10 lid 1 WPolg. Voorts kan er in het kader van een verwerking op grond van art. 9 WPolg niet worden vergeleken met gegevens die zijn verwerkt in het kader van art. 10 WPolg. Daar staat tegenover dat deze mogelijkheid andersom wel bestaat.<sup>32</sup> Hiermee kan hetzelfde resultaat worden bereikt terwijl de inbreuk op de persoonlijke levenssfeer beperkt blijft. Een onbeperkte vergelijking met de gegevens die zijn verwerkt in het kader van art. 8 WPolg is wel mogelijk op grond van art. 11 lid 4 WPolg, het betreft hier echter een uitzondering. De beperkingen die art. 10 in lid 2, 3 en 4 stelt aan de verwerking als bedoeld in het eerste lid lijken niet van toepassing te zijn op de verwerking van art. 11 lid 2 WPolg.

Voorts biedt art. 11 lid 4 WPolg de mogelijkheid tot een veel uitgebreidere vorm van bewerken, namelijk het in combinatie met elkaar verwerken van gegevens. Volgens de MvT rechtvaardigt de ernstige bedreiging van de rechtsorde het combineren of doorzoeken van alle beschikbare politiegegevens ten behoeve van de opsporing van bepaalde strafbare feiten. Hierbij wordt het voorbeeld genoemd van terroristische acties of een dreiging daarvan. Maar ook bij bijvoorbeeld een reeks landelijke overvallen of ten behoeve van tactische analyses is een dergelijke onbeperkte gegevensverwerking mogelijk.<sup>33</sup> Ook in dit geval lijken de beperkingen die lid 10 WPolg in beginsel aan een verwerking stelt niet van toepassing. Het is, gelet op de behoefte aan een permanente informatiepositie inzake bijvoorbeeld terrorisme, mogelijk om gebruik te maken van de mogelijkheden die in art. 11 lid 4 WPolg worden geboden. Er dient voor te worden gewaakt dat de praktijk van het op onbeperkte schaal verwerken van personen tijdens de IRT-affaire in de toekomst niet wordt herhaald in het kader van art. 11 WPolg.<sup>34</sup>

32. Art. 11 lid 2 WPolg.

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

34. En wellicht ook in het kader van art. 10 WPolg.

Ten slotte is het niet geheel duidelijk welke regeling nu van toepassing is bij een vergelijking van gegevens dan wel het in combinatie met elkaar verwerken van gegevens. Is art. 8 WPolg van toepassing wanneer een vergelijking met deze gegevens plaatsvindt of is in dat geval art. 9 of 10 WPolg van toepassing? Het antwoord hierop is bepalend voor de duur van de verwerking. Indien een (geautomatiseerde) vergelijking dan wel het in combinatie met elkaar verwerken in het kader van art. 11 WPolg een verstrekking impliceert, worden de gegevens in beginsel verwerkt in het kader van art. 9 of 10 WPolg.

### *13.2.5 Ondersteunende taken van artikel 13*

Het komt regelmatig voor dat de politie op verschillende plaatsen onderzoek doet naar dezelfde personen zonder dat de betreffende politieambtenaren dit van elkaar weten. Ook kunnen onder de huidige wet- en regelgeving de binnen de politie beschikbare gegevens niet optimaal worden benut voor de opheldering van criminaliteit. Er bestaat dan ook behoefte aan verruiming van het doelbindingsbeginsel. Op grond van het bepaalde in art. 13 WPolg kunnen persoonsgegevens die oorspronkelijk zijn verwerkt voor de doelstellingen van art. 8, 9 of 10 WPolg voor een ander doel worden verwerkt, namelijk de ondersteuning van de politietoek op de volgende vijf terreinen (subdoeleinden):

- a. vaststellen van eerdere verwerkingen ten aanzien van eenzelfde persoon of zaak, onder meer ter bepaling van eerdere betrokkenheid bij strafbare feiten;
- b. ophelderen van strafbare feiten die nog niet herleid konden worden tot een verdachte;
- c. identificatie van personen of zaken;
- d. onder de aandacht brengen van personen of zaken met het oog op het uitvoeren van een gevraagde handeling danwel met het oog op een juiste bejegening van personen;
- e. uitvoeren van taken ten dienste van de justitie.

Met deze regeling wordt onder meer uitwerking gegeven aan de verplichting van art. 15 WPolg om gegevens die voor een andere verantwoordelijke relevant zijn aan deze ter beschikking te stellen. Een belangrijk onderscheid is dat art. 15 betrekking heeft op incidentele gevallen terwijl art. 13 ziet op bepaalde categorieën van gegevens waarvan op voorhand reeds duidelijk is dat zij relevant kunnen zijn voor daartoe geautoriseerden in andere korpsen. Terwijl de mogelijkheden tot koppeling van politiegegevens onder de WPolr in principe te beperkt zijn, lijken die in de WPolg elkaar op onderdelen te overlappen. De verrijking van gegevens op grond van art. 13 lijkt deels ook te kunnen worden bereikt op grond van art. 11 WPolg. Het is niet geheel duidelijk hoe het geautomatiseerd vergelijken en in combinatie zoeken per onderzoek zich verhoudt tot de verwerking met het oog op ondersteunde taken op basis van art. 13 WPolg.

Met het bepaalde in art. 13 WPolg wordt in feite een landelijke informatiepositie gecreëerd ten behoeve van de bovenstaande subdoeleinden. In dit verband zij ook gewe-

zen op ABRIO (Aanpak Bedrijfsvoering Recherche Informatiehuishouding en Opleidingen)<sup>35</sup> en meer specifiek op de ontwikkeling en invoering van de Politie Suite Opsporing (PSO), de toekomstige verzameling van ICT-voorzieningen op het gebied van opsporing. In 2004 is gestart met de gefaseerde invoer van PSO. Met het wetslagen van deze politio-  
nele informatiehuishouding zal een noodzakelijke voorwaarde voor de landelijke beschikbaarheid van politiegegevens worden vervuld. Met een landelijk uniform systeem worden veel stappen binnen de informatieverwerking overbodig, waardoor de daarmee gepaard gaande afbreukrisico's worden geëlimineerd. Bovendien vindt de verwerking op efficiëntere wijze plaats en kan informatie zo optimaal mogelijk worden benut. Het is cruciaal dat een dergelijke landelijke informatievoorziening aansluiting vindt op de van toepassing zijnde wet- en regelgeving. De gegevens die op grond van art. 13 WPolg kunnen worden verwerkt zijn beperkt en behoren tot een set van bij AMvB te benoemen politiegegevens die door de betrokken politieambtenaren beschikbaar zijn gesteld ten behoeve van raadpleging door ambtenaren van politie van alle regiokorpsen. De aanlevering van informatie is in beginsel verplicht op grond van art. 15 lid 1 WPolg. In dat artikel is de verplichting geregeld voor de verantwoordelijke om politiegegevens ter beschikking te stellen aan personen die zijn geautoriseerd voor de verwerking van politiegegevens, voor zover zij deze behoeven voor de uitvoering van hun taak. Deze verplichting tot het beschikbaar stellen van gegevens sluit aan bij de verplichting van art. 10 Politiewet 1993, inhoudende dat alle ambtenaren, belast met de politietaak, elkaar wederkerig de nodige hulp verlenen en bij voortduring een eendrachtige samenwerking betrachten bij het uitvoeren van die taak.<sup>36</sup> Zij verlenen elkaar waar mogelijk de gevraagde medewerking. Hierop is alleen in bijzondere gevallen een uitzondering mogelijk zoals valt te lezen in art. 15 lid 2 WPolg.

### 13.3 Ten slotte

Met de WPolg wordt onder meer voorzien in de behoefte om gegevens op ruimere schaal te verwerken ten behoeve van de opsporing. Omdat hierbij direct aansluiting is gezocht op de Wbp worden veel beperkingen van de huidige regeling opgeheven en sluit de WPolg aan op de huidige inzichten en opvattingen inzake de bescherming van de privacy. Hierbij is het wel de vraag of de beperkte reikwijdte van de WPolg tot het verwerken van persoonsgegevens, wenselijk is. De mogelijkheden en beperkingen van de verwerking van persoonsgegevens in het kader van de opsporing hangen nauw met elkaar samen en worden in sterke mate bepaald door het noodzakelijkheids- en het doelbindingsbeginsel. Een duidelijke invulling van deze beginselen is daarom van belang, temeer nu het onderscheid tussen gegevens over verdachte en onverdachte personen wordt losge-

---

35. Zie ook Ministerie van Justitie, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties 2001.

36. *Kamerstukken II*, 2005/06, 30 327, nr. 3, p. 68.

laten. Dit onderscheid speelt nu een belangrijke rol binnen het spanningsveld tussen opsporing en privacy.

In de nieuwe situatie kan als uitgangspunt worden genomen dat een verwerking noodzakelijk dient te zijn voor de specifieke politietaak. Nu is dat nog de algemene politietaak. Voor wat betreft de doelbinding kan aansluiting worden gezocht bij de verschillende doeleinden waarvoor de WPolg een verwerking mogelijk maakt. Daarbij is het uitgangspunt dat striktere waarborgen dienen te worden gehanteerd naarmate een verwerking gepaard gaat met een grotere inbreuk op de persoonlijke levenssfeer. Voorts zal een in dit onderzoek voorgestelde uitwerking van het doelbindingsbeginsel een voortdurend herhalen van de algemene privacywaarborgen per afzonderlijke verwerking in de WPolg overbodig maken. Eén duidelijke en algemene bepaling op dit punt kan voorkomen dat verschillende verwerkingsbevoegdheden elkaar op onderdelen overlappen. Met betrekking tot het noodzakelijkheidsbeginsel dient men zich bewust te zijn van het feit dat bij een koppeling, een combinatie van gegevens en de toepassing van datamining als geheel, in beginsel wordt gezocht naar verborgen verbanden die pas ná een verwerking zichtbaar worden. Juist daarom kan niet (eenvoudig) op voorhand worden vastgesteld of een verwerking noodzakelijk is. Een ander punt van aandacht is het onderscheid tussen het verwijderen en vernietigen en het verstrekken en beschikbaar stellen van gegevens in de WPolg. Bij het verwijderen en vernietigen van gegevens dient duidelijk te zijn in welk stadium welke regels gelden. De voor het verstrekken en beschikbaar stellen gehanteerde terminologie dient zo uniform mogelijk te worden toegepast. Ook lijkt het wetsvoorstel op bepaalde punten (te veel) geredigeerd te zijn door de politiepraktijk. Bijvoorbeeld waar het gaat om de zogenoemde themaverwerkingen. De WPolg dient niet alleen als instrument voor de politiepraktijk maar is tevens bedoeld als mogelijkheid tot toetsing en begrenzing van diezelfde politiepraktijk. De invulling van de waarborgen die de WPolg biedt tegen een al te vergaande verwerking van gegevens wordt in grote mate bij de politie zelf neergelegd.<sup>37</sup> In combinatie met de vergaande bevoegdheden inzake de verwerking van gegevens in het kader van de opsporing, is een actieve en regulerende rol weggelegd voor het CBP. In aansluiting op de ontwikkeling die de WPolg voorstaat dienen ook andere aspecten die van invloed zijn op het al dan niet optimaal gebruik van de voor handen zijnde gegevens te worden meegenomen. Het CBP wees in een brief over het gebruik van informatie binnen de politie in 2003<sup>38</sup> al op organisatorische problemen, de bestaande politiecultuur en technische belemmeringen die uitwisseling van informatie binnen de politie in de weg zouden staan. Met de ontwikkeling van de PSO en de verplichte uitwisseling van informatie in de WPolg wordt de aanzet gegeven tot een volledig uniforme informatiehuishouding op nationaal niveau.

---

37. *Kamerstukken II, 2005/06, 30 327, nr. 2, p. 14-15.*

38. Kenmerk z2002-1397, onder verwijzing naar een rapport van de Algemene Rekenkamer over het gebruik van informatie binnen de politie.

### Terugkoppeling aandachtspunten

In het navolgende wordt een terugkoppeling gemaakt naar de in het vorige hoofdstuk neergelegde aandachtspunten c.q. aanbevelingen ten behoeve van een zo optimaal mogelijke verwerking van gegevens in het kader van de privacy, de opsporing en de uitvoering van de opsporingstaak.

### Privacy

- Met de WPolg wordt de bestaande wettelijke regeling in de WPolr en het BPolr aangepast aan de huidige (herziene) opvattingen inzake privacy.
- Hierbij staat niet langer de registratie van gegevens in een register centraal, maar wordt uitgegaan van de ‘verwerking’ van gegevens.
- Een uitwerking van het in de WPolg gehanteerde doelbindings- en noodzakelijkheidsbeginsel waarbij in beginsel per geval een afweging plaatsvindt.
- Blijkens het wetsvoorstel heeft de wetgever ruim aandacht besteed aan de bescherming van de persoonlijke levenssfeer. De privacywaarborg zal worden verbeterd met behulp van audits, de inzet van privacyfunctionarissen en technologische hulpmiddelen. Actief toezicht en handhaving zijn hierbij essentieel.

### Opsporing

- Met de WPolg komt de wetgever in het algemeen tegemoet aan de huidige opvattingen en wensen inzake de mogelijk- en onmogelijkheden van gegevensverwerking in het kader van de opsporingstaak.
- Het is de vraag of de invloed van de (behoeften vanuit de) dagelijkse politiepraktijk niet te zeer leidend is geweest bij de formulering en uitwerking van de WPolg. Hoewel het uitgangspunt, de verwerking van gegevens, past in het streven naar een algemeen geformuleerde en techniekonafhankelijke regeling, lijken met de keuze voor een op de politiepraktijk toegespitste regeling veel concessies te zijn gedaan ten opzichte van de (beperkende) regelingen van WPolr en het BPolr.
- Het onderscheid tussen raadplegen en analyseren (in het kader van het vastleggen van gegevens) doet niet langer terzake wanneer wordt uitgegaan van een verwerking van gegevens in plaats van de registratie daarvan. De WPolg introduceert wel een nieuw onderscheid binnen een verwerking, te weten een verwerking middels geautomatiseerd vergelijken en in combinatie zoeken. Hierbij is het opmerkelijk dat een vergelijking op basis van zoekgegevens minder mogelijkheden lijkt te bieden dan het huidige raadplegen van een (gewoon) politieregister.

### Uitvoering

- Met de WPolg wordt de (juridische) aanzet gegeven tot een uniforme gegevensverwerking binnen de politie. De mogelijkheden tot informatie-uitwisseling worden uitgebreid en soms zelfs verplicht. Om hieraan in de praktijk gevolg te geven is een uniforme informatiehuishouding een essentiële randvoorwaarde. Het is de vraag of de

politiepraktijk aansluit, dan wel in de nabije toekomst kan aansluiten, op de veranderingen die de WPolg met zich meebrengt c.q. mogelijk maakt.

- De WPolg is duidelijker in het toewijzen van bepaalde taken dan de WPolr en het BPolr. Van bepaalde taken is echter nog steeds niet duidelijk aangegeven wie daarvoor verantwoordelijk is. Het is wenselijk om duidelijk te bepalen wie welke informatieproducten levert. Inzake de verrijking van informatie binnen de politie zou bijvoorbeeld kunnen worden overwogen om (in aansluiting op de MvT bij de WPolg) bepaalde taken bij het KLPD als nationaal coördinerend korps neer te leggen. Hiermee kan ook uitvoering worden gegeven aan het streven naar een uniforme gegevensverwerking die primair op nationaal, en secundair op lokaal niveau plaatsvindt.

---

## Summary

Criminal investigation is pre-eminently a knowledge-intensive activity. Information is often fragmented and contains important (hidden) knowledge, which only becomes perceptible after processing of the data. In order to obtain and keep a good information position, large-scale and (by this also) efficient processing of information is mandatory. From a technical point of view, there should not be too many obstacles in the way of reaching that goal. The possibilities of digital processing of information and the ever-advancing technological developments in this field make efficient processing of (potential) usable data feasible. The process of datamining could be an important tool in criminal investigation activities. However, the civil interest within the scope of the protection of his or her personal privacy should not be neglected. This investigation intends to create clarity in regard of the possibilities and the impossibilities concerning the data processing in view of the criminal investigation task. For that purpose, the following questions need to be answered:

- *‘What is the context of criminal proceedings and privacy law for the application of datamining investigation by the Dutch government on behalf of the criminal investigation task?’*
- *‘In what way can (and may) the Dutch government utilize the process of datamining on behalf of the criminal investigation task?’*

### **The framework of criminal proceedings for datamining investigation**

In order to be able to outline the framework of criminal proceedings for datamining, the meaning of the concept of ‘datamining’ has to be established. With that, it is important to know in which way the datamining process is related to the process of information gathering. Although an unambiguous definition is lacking, the datamining process could be characterized as: a partly or totally computerized analysis related to one or more data file(s) and centred on the discovery of new information (anomalies, certain characteristics or connections) which cannot (or only can with much more effort) be obtained otherwise.

The datamining process can be executed in very many ways. In order to set these methods in a practicable regulation, this investigation makes a distinction between random and specific datamining investigation. Random datamining investigation is applied for the improvement of the (general) information position of a police register, a police

force or the entire Dutch police system. The key point within the process of information gathering is the phase of building and maintaining a certain information position, taking into account that primarily it is not being searched with reference to a certain indication, case or conduct. In the scope of a random datamining investigation, only a limited degree in intrusion on personal privacy will occur.

The specific datamining variable can be deployed for the improvement of the information position in a certain case. This applies to the information position of a temporary police register, which can be set up in the scope of the police task in a specific case or an exploratory investigation in the sense of art. 126<sup>gg</sup> Sv (Code of Criminal Procedure). A specific investigation will be based on an indication or suspicion of committed or devised legal offences. Strictly speaking, verification is in order when the question of datamining investigation is no longer applicable. The attention is focussed on verification of already existing knowledge, rather than on gathering fresh information. Whether there is a question of specific datamining investigation or of verification depends on the degree of suspicion. In cases of conclusively well-founded suspicion there will no longer be a search for new information; the already obtained results will be verified or checked.

The way, in which the various application variables of the datamining process are related to the process of information gathering, sets the boundaries for the application of datamining investigation on behalf of the criminal investigation task. Although the datamining process offers numerous application possibilities, deployment of these applications in all random circumstances is out of the question. By means of the breakdown within the datamining process, the possibilities for realising legitimate application of the various datamining variables will become clear. The way in which this datamining process is related to the process of information gathering has been described in the figure below. This process is divisible into three phases, which are: criminal investigation, exploratory investigation and building and maintaining a certain information position.

	Discovering		Checking
<b>Application variables in the datamining process</b>	Random data-mining investigation	Specific datamining investigation	Verification
<b>The process of information gathering</b>	<i>Building and maintaining information position</i>	<i>Exploratory investigation</i>	<i>Criminal investigation</i>
<b>Leading points</b>	No suspicion	← Transitional stage ⇒	Suspect

*Relationship between the three datamining variables and the stages of the process of information gathering*

In relationship with the framework of criminal proceedings for the application of datamining investigation by the Dutch government on behalf of the criminal investigation task, a complete judicial vacuum appears to be out of the question, thanks to relatively technology-independent regulation and legislation. The existing legislation, however, is predominantly indirectly applicable to the datamining process and does insufficient justice to the contemporary social reality and the changed opinions on a.o. (The protection of personal privacy). Therefore it is suggested to consider the data processing as starting point. In that way a technology-independent regulation of existing and future operations in regard to the police data within the framework of the police task will be covered; with that the protection of personal privacy will be applicable to each data processing activity.

### **Personal privacy**

The investigation into the application of datamining reveals an area of tension between the significance of the criminal investigation on the one hand and the protection of personal civil privacy on the other. Therefore, measures should be taken in order to create a judicial framework in which the possibilities of the criminal investigation can be fully utilized and, by the same token, include guarantees for the protection of privacy. The present privacy regulations have a definable impact on the framework in which the datamining process, or the data processing as part of the criminal proceedings, must be executed. As the views on criminal proceedings and personal privacy since the realization of the WPolr (Law Police registers) and the BPolr (Decree Police registers) have shifted considerably, drastic adaptation of those regulations are mandatory. The framework for privacy law arrangements for the application of datamining investigation initially comprises the international regulation and legislation in this matter. On that basis, at least a statutory regulation will be required which complies with a number of conditions primarily regarding the prevention of inadmissible intrusion into privacy. The judicial boundaries of the WPolr and the BPolr offer insufficient guarantees for the protection of privacy. The present WPolr is based on the former Wpr (Law registration of personal data) instead of the Wbp (Law protection of personal data) and is primarily focussed on data registration instead of data processing. Even if the legal safeguards would be aligned to the present views on privacy protection, one should permanently appreciate the fact that the quality of the administration of the police registers and the supervision on compliance with the legal provisions are playing just as an important part in the protection of privacy. Privacy protection should be extended over each data processing activity. When adjusting the WPolr, it should be taken into account that the present guarantees on privacy protection often needlessly restrict the possibilities for data processing (in context with a datamining investigation) within the police system. This data can be applied more effectively, without devaluation of the privacy protection. General regulation, applicable to all forms of data processing, is to be preferred above the present situation, in which a specific (guarantee) regulation for each separate process activity is mandatory.

### **Judicial framework**

Adjustment of the present regulation and legislation is not only necessary in view of the effective protection of the personal privacy; it should also take care of a better benefit from the possibilities of the present data processing techniques. The present national and international regulation and legislation forms a judicial basic framework for data processing in the sphere of criminal investigation, which appears to be alternately directional and direction defining. The severely outdated character of this basic framework prompts some adjustment, also considering the increased possibilities of and need for data processing combined with the socially prevailing view on privacy and security. Data processing in the framework of the police task cannot be executed in all circumstances. When the processing is deemed as not being major, the general article 2 Politiewet (Public Order Act) 1993 will do. However, should the application involve an intrusion on personal privacy, there has to be a specific legal foundation. The larger the breach, the stricter the conditions. The Wpol has a definable impact on the way in which obtained information can and may be processed further. For that, the judicial framework is formed by a.o. (The principle of purpose binding). In view of the privacy protection, the initial purposes for obtaining the information in the first place should always be taken into account. By that, a balance is obtained in the area of tension between the two fields of interest. In this respect it should be mentioned that information about unsuspected persons which is obtained from investigation in the light of serious crime fighting can (in principle) not yet be processed within the police organization on an unlimited scale for all kinds of purposes. After all, those purposes will not always form a justification for (coherent with the data processing) intrusion on privacy. The WPolr and the BPolr regulate the three functions that can be fulfilled by a police register, these being data registration, data analysing and data consulting. The way in which the police registers cover one or more of these purposes bears, under the present regulation and legislation, a strong definable impact on the application possibilities of datamining investigation.

The way in which the WPolr provides a structure in the registration of police data reduces the possibilities for the processing thereof in relation with datamining investigation. At the time, while regulating the registration of information in the police registers, which is closely connected with the several functions of those records, a connection was sought on the basic principles of the Wpr and the then state of the art. Although new possibilities are now open for executing analyses (nowadays often considered as being essential) without pushing aside the aspects of privacy, certain forms of data analysis are, precisely in view of securing that privacy, being excluded as a result of the legal provisions of the WPolr and the BPolr. By partly disconnecting the analysis function from the registration and consultation functions, an (autonomous) registration to the cause of consultation can be distinguished from a registration to the cause of analysis in such a way, that the current privacy guarantees will not be violated.

The analysis function of a police register is contributory to the way in which police data can be processed. This function has been specified in the linking regulation of art. 6 WPolr. Within the WPolr, the linking regulation is an essential part of the protection of personal privacy. Amongst others, it stipulates whether (and if so, in which way) for a specific purpose registered data can be linked to each other. With that, it does not only concern the mutual linking of police registers, but also (on behalf of the criminal investigation practice) the ever increasing importance of the comparison of police data with information from outside the police sphere.

In attempting an as efficient as possible use of the available information, an important part is played with the linking of data files. The present linking regulation, being severely outdated, excludes many forms of data processing; therefore, adjustment is necessary. It would also be advisable to provide in a central, technique independent regulation. Linking is, to a larger extent than already is the case right now, to be left to the discretion of the principles of necessity and purpose binding. For that purpose, these principles could be further specified in the regulations. The proposed reformulating of the concept of linking and the associating regulation and legislation offers extension of the possibilities of data processing in the framework of the police task on the one hand and guarantees that the processing takes place in a legitimate way on the other.

As a source of information, police registers fulfil a pivotal role within the criminal investigation; the extent in which consultation of the information is allowed is inextricably bound up with the processing possibilities. The consultation role of a police register also determines, apart from the answer to the question whether data can be provided (for processing) within the police organization or not, who will be authorized for executing the data processing. Data is registered for a specific purpose and, subsequently, can be consulted in accordance with that purpose. Standard is that the purpose of processing justifies the consequential intrusion on personal privacy. Under certain circumstances, processing of data for another purpose than initially intended will be desirable. The possibilities for doing so are limited for the time being. In order to enable investigation services to process the data more efficiently, a distinction can be made between registration for general consultation and registration for analysing purposes.

#### **Allocation of tasks and technique**

For the best possible use of information in relationship to the criminal investigation task, it ought to be clear who is responsible for which information position. The intake of information can take place on a local/regional level. It is important, however, that subsequent information processing (analysis) will be carried out on a central, c.q. at national level. This enables univocal and effective data processing and prevents information fragmentation. The final purpose is to attain a central information position within

the police forces and the criminal investigation authorities (intelligences) on behalf of the individual inquirers.

Technology can also play a key role in the drive toward legitimate and good data processing. If processed uniformly and if mutually interchangeable, data can be utilized to the full. For that purpose, one flexible system could be organized in such a way, that it will be able to fulfil present as well as future needs and make information available to authorized persons only. By dividing the authorizations, specific data will be made available in a fast and simple way, e.g. on behalf of CIE (Criminal Intelligence Unit) investigation. Moreover, linking the various authorizations to the availability of data supplies guarantees legitimate processing, by which possible privacy intrusions will be minimized. By means of this technique, compliance with the statutory guarantees can also be checked.

### **Points of interest**

Hereafter follows a summary of the most important points of interest for the best possible data processing from the view point of privacy, criminal investigation and carrying out the criminal investigation task respectively. The basic principle hereby is the drive to attain a situation of balance between the law as instrument for the authorities and the law as protection of the civil privacy.

#### **Privacy**

- Adjustment of in particular the WPolr and BPolr to the present (revised) views on privacy.
- Starting point is data processing.
- Further detailing of the principles of necessity and purpose binding.
- Application of technological tools for safeguarding the privacy and actualisation of authorizations in practice.

#### **Criminal investigation**

- Adjustment of particularly the WPolr and BPolr to the present (revised) views and desires (terrorism) in relationship with the possibilities and impossibilities of data processing.
- Simplification of the regulation for data processing by striving for a generally formulated and technique independent regulation.
- Distinguish consulting from analysing in relationship with data registering.

#### **Implementation**

- Striving for a uniform data processing system within the police organization by means of a statutory obligation to co-operate and introduce one single system and/or follow a mutually simply interchangeable file format.
- Distinct and clear (statutory) division of tasks and regulation of responsibilities.
- Processing primarily on a national and secondary on a local level.

**Law Police Data (WPolg)**

In conclusion of this investigation the developments in respect of the bill WPolg should be pointed out. With this, the legislator seems to provide in outlines in the bottlenecks as described in this investigation.

The WPolg meets a.o. the need for data processing on a wider scale on behalf of the criminal investigation. By doing so, a direct link with the Wbp has been sought, many limitations of the present legislation were eliminated and a connection was achieved with the present perceptions and opinions with regards to the protection of privacy. However, it remains to be seen whether the limited extent of the process of personal details will be advisable. There is a distinct relationship between the possibilities and the limitations; both are highly influenced by the principles of necessity and purpose binding. Therefore, a clear interpretation of these principles is important, all the more since the distinction between data about suspect and unsuspected persons has been abandoned. This distinction played an important part within the area of tension between criminal investigation and privacy.

In the new situation, specific police task oriented data processing will be mandatory, rather than the present general police task orientation. As far as the purpose binding is concerned, a connection with the various purposes on behalf of which the WPolg allows processing should be sought. With this, the basic principle is that, depending on the degree of intrusion on the personal privacy, stricter guarantees will be applied. One single, clear and general legal provision on this matter could prevent partial overlapping of different processing authorizations. As for the application of the principle of necessity, one should appreciate that with linking, combining of data or unlimited data processing through the help of datamining; hidden connections may only become visible by means of the processing activity. This is precisely why it is impossible to (simply) establish in advance whether processing will be necessary. Another point of interest is the distinction in the WPolg between removal and destruction, and provision of data and making them available. For removal or destruction it should be clear in which stage the rules will be applicable. The terminology for provision and making available should be applied as uniformly as possible.

In certain aspects, the bill seems to be formulated (too much) on the basis of the police practice, e.g. with regard to the so-called 'theme processing'. The WPolg does not only serve as a tool for the police practice, it is also meant to facilitate the testing and defining of that same police practice. The interpretation of the guarantees offered by the WPolg against too far reaching data processing, is largely allocated to the police themselves. For supervision of this matter, combined with the far stretching authorization on the topic of data processing in the framework of criminal investigation, an active and controlling role is reserved for the CBP (Council protection personal particulars). In association

with the development advocated by the WPolg, other aspects affecting the optimal or otherwise use of the available data should be taken into consideration as well. In a letter about the use of information within the police force, the CBP indicated already in 2003 the existence of organizational problems, the existing police culture and the technical impediments, which allegedly could stand in the way of exchanging information within the police force. In this field, the necessary work is yet to be done. An important first step has been taken by incepting the WPolg with its judicial framework for data processing with respect to the criminal investigation. However, much depends on the way in which the criminal investigation authorities decide and particularly on their implementation of data processing methods in general.

---

## Literatuurlijst

Advies van het College van Procureurs-generaal 1997

*Advies van het College van Procureurs-generaal met betrekking tot de inzet van (bijzondere) opsporingsmethoden en -middelen; voorlopige uitgangspunten*, advies van 24 januari 1997.

Alberdingk Thijm 2002

C. Alberdingk Thijm, 'Het einde van spam? Regulering van ongevraagde e-mail', *Privacy & Informatie* 2002/6, p. 250-259.

Artz & Van Eijk 2000

M.J.T. Artz, & M.M.M. van Eijk, *Klant in het web. Privacywaarborgen voor internettoegang*. (Achtergrondstudies en verkenningen 17) 2000.

Asscher & Ekker 2003

L.F. Asscher & A.H. Ekker (red.), *Verkeersgegevens. Een juridische en technische inventarisatie*, Amsterdam: Otto Cramwinckel Uitgever 2003.

Berry & Linoff 1997

M.J.A. Berry & G. Linoff, *Data Mining Techniques*, New York: John Wiley & Sons Inc. 1997.

Beijer e.a.

A. Beijer, R.J. Bokhorst, M. Boone, C.H. Brants & J.M.W. Lindeman, *De Wet bijzondere opsporingsbevoegdheden. Eindevaluatie*, Den Haag: Boom 2004.

Borking, Artz & Almelo 1998

J.J. Borking, M. Artz & L. Almelo, *Gouden bergen van gegevens. Over datawarehousing, datamining en privacy*. (Achtergrondstudies en verkenningen 10) 1998.

Buruma 2004

Y. Buruma, 'Acht nieuwe wetten: de zin en onzin van gegevensbescherming', *Delikt en delinkwent* 2004, p. 665-675.

CBP 1998

*Uitspraak van het CBP betreffende de Albert Heijn Bonus Kaart (97.V.0034)*, Den Haag: CBP 1998.

CBP 2001

*Advies over circulaire toezicht op het beheer van de bijzondere politieregisters*, (z2001-1312), Den Haag: CBP 2001.

## CBP 2001a

*Advies van het CBP aan het Landelijk Expertisecentrum voor de opsporing en vervolging (LEXPO) betreffende de verhouding tussen de aangifteprocedure ingevolge art. 160 e.v. Sv en de regeling betreffende de wettelijke bewaartermijnen van gegevens van onverdachte personen zoals bedoeld in art. 5a WPolr, (z2000-1166, 29), Den Haag: CBP 2001.*

## CBP 2002

*Elektronische overheid en privacy. Bescherming van persoonsgegevens in de informatie-infrastructuur van de overheid, Den Haag: CBPP 2002.*

## CBP 2004

*Advies van het College bescherming persoonsgegevens betreffende het conceptwetsvoorstel inzake de verwerking van politiegegevens (Wet politiegegevens), (z2004-0467), Den Haag: CBP 2004.*

## Clarke 1994

R. Clarke, 'Dataveillance by Governments: The Technique of Computer Matching', *Information Technology & People* 1994/7/2, p. 6-37.

## Clarke 1995

R. Clarke, 'Computer Matching by Government Agencies: The Failure of Cost/Benefit Analysis as a Control Mechanism', *Information Infrastructure & Policy* 1995/4/1, p. 29-65.

## Corstens 2002

G.J.M. Corstens, *Het Nederlands strafprocesrecht*, Arnhem: Gouda Quint 2002.

## Dijstelbloem &amp; Schuyt 2002

H. Dijstelbloem & C.J.M. Schuyt (red.), *De publieke dimensie van kennis*, Den Haag: Sdu Uitgevers 2002.

## Dommering e.a. 2000

E.J. Dommering, L. Asscher, N. van Eijk, J. Kabel, A. Nieuwenhuis, G. Schuijt & N. Sitompoel (red.), *Informatierecht, fundamentele rechten voor de informatiesamenleving*, Amsterdam: Cramwinckel 2000.

## Dontje 2000

M.J. Dontje, 'Wet persoonsregistraties naar Wet bescherming persoonsgegevens', *Compact* 2000.

## Fahmy 2000

St@tsurf, *About Data Mining* (T. Fahmy), WWW <<http://www.statserv.com/datamining.html>>, bijgewerkt 2000.

## Fayyad 1996

U. Fayyad, *Advances in Knowledge Discovery and Datamining*, Cambridge, USA: MIT Press 1996.

- Fayyad, Piatetsky-Shapiro & Smyth, 1996a  
U. Fayyad, G. Piatetsky-Shapiro & P. Smyth, 'From data mining to knowledge discovery in databases', *AI Magazine* 1996, p. 37-54.
- Fayyad, Piatetsky-Shapiro & Smyth 1996b  
U. Fayyad, G. Piatetsky-Shapiro & P. Smyth, 'The KDD process for extracting useful knowledge from volumes of data', *Communications of the ACM* 39/11/1996, p. 27-34.
- Frawley, Piatetsky-Shapiro & Matheus 1991  
W. J. Frawley, G. Piatetsky-Shapiro & C. J. Matheus, 'Knowledge discovery in databases. An overview', in: G. Piatetsky-Shapiro & W. J. Frawley, *Knowledge Discovery in Databases*, AAAI/MIT Press 1991, p. 1-27.
- Frissen 1996  
P.H.A. Frissen, *De virtuele staat, politiek, bestuur, technologie: een postmodern verhaal*, Schoonhoven: Academic Service 1996.
- Gardeniers, Van Kralingen & Schreuders 1996  
H.J.M. Gardeniers, R.W. van Kralingen & E. Schreuders, 'Knowledge discovery in databases. Privacyaspecten van informatiemijnbouw', in: S. Nouwt en W. Voermans (red.), *Privacy in het informatietijdperk*, Den Haag: Sdu Uitgevers 1996, p. 69-81.
- Handboek voor de opsporingspraktijk 2000  
Openbaar Ministerie, *Handboek voor de opsporingspraktijk*, Den Haag: Sdu Uitgevers 2000.
- Handleiding 2000  
Handleiding *Informatie Inwinning Openbare Orde*, 2000.
- Hes & Borking 1998  
R. Hes & J. Borking, *Privacy Enhancing Technologies: the path to anonymity*. (Achtergrondstudies en Verkenningen 11) 1998.
- Hoeksema 2001  
E. Hoeksema, 'Datamining klaar voor de massa?', *Technieus/TN9909*, 2001.
- Jaarverslag* 2001  
*Jaarverslag Meldpunt Ongebruikelijke Transacties* 2001.
- Jaarverslag* 2003  
*Jaarverslag Meldpunt Ongebruikelijke Transacties* 2003.
- Klerks e.a. 2002  
P.P.H.M. Klerks, C.J.E. in 't Velt, A.Ph. van Wijk, M.M.E.A. Scholtes, P.S. Nijmeijer & J.G.M. van der Velde, *De voorhoede van de opsporing*, Den Haag: Elsevier 2002.

Koops & Vedder 2001

B.J. Koops & A. Vedder, met bijdragen van J. Mensink & S. Raaijmakers, *Opsporing versus privacy. De beleving van burgers*, ITeR-reeks deel 45, Den Haag: Sdu Uitgevers 2001.

Kruissink, Verwers & Dijkhoff 1998

M. Kruissink, C. Verwers & N. Dijkhoff, *Organisatie van de recherchefunctie, een inventarisatie in de 25 regiokorpsen* (Onderzoeksnotities WODC 1998/2) 1998.

Lopez 2000

M.J.J. Lopez, 'Meer informatie uit bestaande gegevens, de mogelijkheden van data-mining voor de Nederlandse politie', *Tijdschrift voor de politie* 2000-6, p. 26-29.

Meij 2004

J.M. Meij, *Data Mining Projectplan*, WWW <<http://www.stt.nl/stt2/projecten/datm/datmprojectplan/datmprojectplantekst.htm>>, publicatie 14 oktober 1999.

Middelkoop 2002

Y. Middelkoop, *Onderzoek Telewerken BZK Politie, Deelrapport 2: Juridische aspecten*, 17 juni 2002.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties 2000

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, *nota Contract met de toekomst, een visie op de elektronische relatie overheid-burger*, 19 mei 2000.

Ministerie van Justitie 1998

Ministerie van Justitie, *nota Wetgeving voor de elektronische snelweg*, Kamerstukken II, 1997/98, 25 880, nrs. 1-2.

Ministerie van Justitie 2003

Ministerie van Justitie, *onderzoek Bewaren Verkeersgegevens door Telecommunicatieaanbieders*. (Uitgebracht aan het WODC van het Ministerie van Justitie Uitgebracht door: Stratix Consulting Group B.V., Schiphol) 2003.

Ministerie van Justitie & Ministerie van Binnenlandse Zaken en Koninkrijksrelaties 2001

Ministerie van Justitie & Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, *nota Criminaliteitsbeheersing. Investeren in een zichtbare overheid*, Den Haag: Hega Offset 2001.

Ministerie van Justitie & Ministerie van Binnenlandse Zaken en Koninkrijksrelaties 2003

Ministerie van Justitie & Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, *nota Nieuw Stelsel Bewaken en Beveiligen*.

Naeyé e.a. 2004

J. Naeyé, L. Huberts, C. van Zweden, V. Busato & B. Berger, *Integriteit in het dagelijks politiewerk. Meninge en ervaringen van politiemensen*, Zeist: Kerckebosch 2004.

Patijn 2003

A. Patijn, 'Verplichte opslag van verkeersgegevens?', *Computerrecht* 2003/2, p. 135-136.

Prins 2004

J.E.J. Prins, 'Technologie en de nieuwe dilemma's rond identificatie, anonimiteit en privacy', *Justitiële verkenningen* 2004/8.

*Rapport Evaluatie wet bijzondere politieregisters* 2004

*Rapport Evaluatie wet bijzondere politieregisters*, Rotterdam; Capelle a/d IJssel; Leiden: Erasmus Universiteit Rotterdam, Net2Legal Consultants, Mazars Paardekooper Hoffman 2004.

*Rapport Gegevensuitwisseling en Terrorismebestrijding* 2003

*Rapport Gegevensuitwisseling en Terrorismebestrijding* (werkgroep wetgeving informatie-uitwisseling, actiepoint 43 van het Actieplan Terrorismebestrijding en Veiligheid) 2003.

*Rapport Opsporing gezocht* 1994

*Rapport Opsporing gezocht* (werkgroep vooronderzoek opsporingsmethoden) Den Haag: Sdu Uitgevers 1994.

Rapport Parlementaire Enquêtecommissie Opsporingsmethoden 1996

Rapport Parlementaire Enquêtecommissie Opsporingsmethoden (ook wel genoemd naar de voorzitter van de commissie: Rapport van de Commissie Van Traa), Den Haag: Sdu Uitgevers 1996.

*Rapport van de Commissie Grondrechten in het digitale tijdperk* 2000

*Rapport van de commissie Grondrechten in het digitale tijdperk* (ook wel genoemd naar de voorzitter van de commissie: Rapport van de Commissie Franken) (*Stb.* 1999, 101) 2000.

*Rapport van de Commissie Strafvorderlijke gegevensvergaring in de informatiemaatschappij* 2001

*Rapport van de Commissie 'Strafvorderlijke gegevensvergaring in de informatiemaatschappij', Gegevensvergaring in strafvordering, nieuwe bevoegdheden tot het vorderen van gegevens ten behoeve van strafvorderlijk onderzoek.* (ook wel genoemd naar de voorzitter van de commissie: Rapport van de Commissie Mevis) 2001.

Rapport van de Tijdelijke Commissie Evaluatie Opsporingsmethoden 1999

Rapport van de Tijdelijke Commissie Evaluatie Opsporingsmethoden, Opsporing in uitvoering, (ook wel genoemd naar de voorzitter van de commissie: Rapport van de Commissie Kalsbeek), Den Haag: Sdu 1999 (Kamerstukken II, 1998 /99, 26 269).

*Rapport werkgroep Misdaadanalyse* 1991

*Rapport werkgroep Misdaadanalyse* (rapport van de recherche adviescommissie (RAC)) 1991.

*Richtsnoeren 2003*

*Richtsnoeren voor de interpretatie van de Wet Identificatie bij dienstverlening en de Wet MOT* (versie 1.0 d.d. 27 mei 2003).

## Schreiber e.a. 2000

G. Schreiber, H. Akkermans, A. Anjewierden, R. de Hoog, N. Shadbolt, W. van de Velde & B. Wielinga, *Knowledge Engineering and Management. The Common KADS Methodology*, MIT Press, 2000.

## Schreuders 1995

E. Schreuders, *Het gesloten verstrekkingenregime van de Wet politieregisters*, Rijswijk: CBP 1995.

## Schreuders &amp; Van Kralingen 1998

E. Schreuders & R. van Kralingen, 'Klantenkaarten, chipcards en data-mining; een (juridische) verkenning', in: R. van Kralingen, M. Lips & C. Prins (red.), *De kaarten op tafel; Een verkenning van de juridische en bestuurskundige aspecten van chipcards*, Den Haag: Sdu Uitgevers 1998, p. 99 – 115.

## Schreuders 2001

E. Schreuders, *Data mining, de toetsing van beslisregels & privacy. Een juridische Odyssee naar een procedure om het toepassen van beslisregels te kunnen toetsen*, ITeR-reeks deel 48, Den Haag: Sdu Uitgevers 2001.

## Schuurman &amp; Jordens 2000

Schuurman & Jordens, *Wet politieregisters*, Deventer: W.E.J. Tjeenk Willink 2000.

## Sietsma e.a. 2002

R. Sietsma, J. Verbeek & H.J. van den Herik, *Datamining en opsporing. Toepassing van datamining ten behoeve van de opsporingstaak*, ITeR-reeks deel 55, Den Haag: Sdu Uitgevers 2002.

## Sietsma 2004

R. Sietsma, 'Opsporen in een digitale omgeving', *Mediaforum* 2004/5, p. 146-155.

## St@tsurf 2000

St@tsurf, *About Data Mining*, (Gartner Group), WWW <<http://www.statserv.com/datamining.html>>, bijgewerkt 2000.

## Stol 2004

W.Ph. Stol, *Handhaven: eerst kiezen, dan doen, technische mogelijkheden en beperkingen* (deelrapport III, Expertisecentrum Rechtshandhaving, Ministerie van Justitie) 2004.

## Terlouw &amp; Aron 1996

G.J. Terlouw & U. Aron, *Twee jaar MOT. Een evaluatie van de uitvoering Onderzoek en Beleid*, Arnhem: Gouda Quint 1996.

## Trajecta lexicon 2001

*Trajecta lexicon*, WWW <<http://www.trajecta.com/neural/lexicon.htm>>, (geraadpleegd 4 oktober 2001).

- U.S. Congress, Office of Technology Assessment 1986  
U.S. Congress, Office of Technology Assessment, *Federal Government Information Technology: Electronic Record Systems and Individual Piracy*, OTA-CIT-296, Washington DC: U.S. Government Printing Office 1986.
- Van Bommel 2003  
N. van Bommel, 'Zachte informatie in een hard dossier', *De Volkskrant*, 10 januari 2003.
- Van Blarkom & Borking 2001  
G.W. van Blarkom & J.J. Borking, *Beveiliging van persoonsgegevens*. (Achtergrondstudies en Verkenningen 23) 2001.
- Van der Pol 2000  
R.W. van der Pol, *Knowledge-based Query Formulation in Information Retrieval*, SIKS dissertation series; no. 2000-5, IKAT Universiteit Maastricht 2000.
- Van Kempen 2005  
P.H.P.H.M.C. van Kempen, 'Het conceptwetsvoorstel voorkoming, opsporing en vervolging van terroristische misdrijven: terrorisme bestrijding door marginalisering strafvorderlijke waarborgen', 2005, p. 7-8.
- Van Ruth & Schreuders 2000  
A.G.P. van Ruth & E. Schreuders, *Politiegegevens beschermd. Een toelichting op het gesloten regime van de WPolr*, Den Haag: CBP 2000.
- Verbeek e.a. 1999  
J.P.G.M. Verbeek, H.J. van den Herik, L.A. Plugge & Th.A. de Roos, *Politie en Intranet. Normering van netwerkkoppeling en grensoverschrijdend gebruik van multimediale databases op een internationaal politieel Intranet*, ITeR-reeks deel 19, Deventer: Kluwer 1999.
- Verbeek, De Roos & Van den Herik 2000  
J.P.G.M. Verbeek, H.J. van den Herik & Th.A. de Roos, *Interceptie van vertrouwelijke communicatie*, ITeR-reeks deel 35, Den Haag: Sdu Uitgevers 2000.
- Warehouse 2000  
*Data Warehouses Simplify Decision Making for Executives*, WWW  
<[http://www.decisionsupport.net/data\\_warehouse.asp](http://www.decisionsupport.net/data_warehouse.asp)>, bijgewerkt 2000.
- Warren & Brandeis 1980  
S.D. Warren & L.D. Brandeis, 'The right to privacy' *Harvard Law Review* 1980, nr. 5, p. 195.
- Westin 1967  
A.F. Westin, *Privacy and Freedom*, New York 1967, p. 7.
- Wuchold 2001  
H. Wuchold, 'Datenvergleich, Im Raster der Terroristen-Jäger', *Hamburger Abendblatt*, 5 oktober 2001.



---

## Trefwoordenregister

Bedrijfsprocessensysteem (BPS)	300, 359, 396
Besluit Politierregisters	91
bewerken van gegevens	24, 40, 62, 69, 155, 400, 435
bijzondere opsporingsmethoden	40, 55
bijzondere politierregisters	117, 202, 261, 277, 359
– functieverdeling	284
Bureau Ontnemingswetgeving Openbaar Ministerie (BOOM)	235
College bescherming persoonsgegevens (CBP)	101, 111, 388, 432
commissie Mevis	24, 155, 237
computer matching	151, 158
computerprofiling	152, 159
criminele inlichtingeneenheid	277, 281, 334
dader(groep)analyse	63
Databeschermingsverdrag	94
dataminingsonderzoek	26, 68, 370
– functies van	169
– gericht	75, 82, 136, 341, 371
– ongericht	72, 81, 135, 169, 233, 277, 371
– varianten	135
dataminingsproces	25, 65, 71, 80, 156, 382
– flexibiliteit van	66
datawarehouse	99, 110, 125, 135, 242, 286, 348, 351, 393
delictanalyse	63
doelbindingsbeginsel	120, 130, 215, 300, 384
dubbele registratie	198

fenomeenonderzoek	33
fishing expeditions	182
functies politieregister	
– analyse	169-170
– raadpleging	169-170
– registratie	169-170
geautomatiseerd vergelijken	426
gericht dataminingonderzoek	75, 82, 136, 341, 371
– resultaat	128
Herkenningsdienstsysteem (HKS)	195
hulpverleningsregister	188, 327, 357, 423
hulpverleningstaak	192, 249
informatiegaring, proces van	37, 40, 61, 342, 370
informatiesystemen	195, 197
integratie van bestanden	154, 159
Knowledge Discovery in Databases (KDD)	23
koppelen	109, 130, 400, 422
– en dataminingsproces	163
– en gegevensverstrekking	166
– en registervergelijking	155
– vormen, van	149
– wettelijke regeling	154
Meldingen Districtelijke Recherche-Onderzoeken Subjecten (MRO)	196
Meldpunt Ongebruikelijke Transacties, register	188, 233, 327, 357
misdaadanalyse	63, 254, 293, 313, 375, 381
modelreglement	102, 145, 210, 269
naam-, adres- en woonplaats (NAW)gegevens	46, 346
noodzakelijkheidsbeginsel	175, 386
onbepaald en bepaald	48, 69, 110, 156-157, 402
onderzoeksmethode	62, 71
ongericht dataminingonderzoek	72, 81, 135, 169, 233, 277, 371
– resultaat	126
onverdachte personen	84, 106, 141, 423
– registerkoppeling	203

openbare registers	184, 246, 298, 325, 356
operatieanalyse	63
opsporing, proces van informatiegaring	37, 40, 61, 342, 370
opsporingsonderzoek	50, 85, 350
opsporingstaak	37
parlementaire enquêtecommissie (PEC)	37
persoonlijke levenssfeer, zie privacy	
persoonsgegevens	21, 96, 98, 104, 120, 175, 180, 382
persoonsregistratie	95, 114, 180, 377
politiegegevens	381, 422
politieregister	126
– functionaliteit	169, 193
– kenmerken van	126
politietaak	96, 111
Privacy Reglement MOT	245
privacy	58, 76, 92, 107, 129, 191, 376, 382, 417
– Enhancing Technologies (PET)	389
– reglement	100, 144, 245, 349, 388, 406
privacyfunctionaris	423
Privacyrichtlijn	94
pro-actieve fase	43, 49, 53, 86
Rasterfahndung	29
Regeling criminele inlichtingeneenheden (CIE)	278
Register Meldpunt Ongebruikelijke Transacties	188, 233, 327, 357
Register zware criminaliteit	120, 213, 266, 316, 396
– functies	323
– Modelreglement	223, 324
registervergelijking	155, 236
Richtlijn betreffende privacy en elektronische communicatie	94
specifieke profielanalyse	63
themaverwerking	431
tijdelijk politieregister	118, 205, 262, 353
verificatie	78, 150, 158, 371
verkennend onderzoek	44, 84, 343
– procedure	47
verstrekken	166, 182, 245, 256, 298, 325, 356

verstrekkingenregime	115, 139, 220
verwerken van gegevens	24, 69, 169, 181, 346, 424
verwijsindexen	196, 198
Verwijzingsindex Recherche-onderzoeken Subjecten (VROS)	196
voorlopig politieregister	119, 208, 263, 291
vrijwillige gegevensverstrekking	182, 245, 298, 325, 356
Wet bescherming persoonsgegevens	180
Wet Melding Ongebruikelijke Transacties	233
Wet persoonsregistratie	180
Wet Politiegegevens	421
Wet Politieregisters	91, 98
wetsvoorstel Vorderen gegevens telecommunicatie	345

