Brandstof voor de opsporing

Brandstof voor de opsporing

Evaluatie Wet bevoegdheden vorderen gegevens

Toine Spapens
Mirjam Siesling
Ellen de Feijter

Boom Juridische uitgevers
Den Haag
2011

ISBN 978-90-8974-408-1
NUR 820

www.bju.nl

Voorwoord

Informatie kan worden beschouwd als de 'brandstof voor de opsporing' en is derhalve cruciaal voor het rechercheproces. De Wet bevoegdheden vorderen gegevens (Wbvg) speelt bij het verkrijgen van die informatie een zeer belangrijke rol. Deze wet biedt overheidsinstanties, in beginsel, de mogelijkheid om alle informatie te vorderen die over een individu, of een rechtspersoon, voorhanden is bij andere instanties of bij private partijen, uiteraard onder voorwaarden. Toch spraken sommige rechtswetenschappers van een revolutionaire ontwikkeling in het strafrecht. Nu, vier jaar na het van kracht worden van de wet is de Wbvg onderwerp geweest van een evaluatie. Het voor u liggende boek vormt daarvan de weerslag.

In deze studie worden de verschillende onderdelen van de wet onder de loep genomen. Dat gebeurt ten eerste vanuit juridisch perspectief, waarbij onder andere de vragen of de Wbvg wordt toegepast zoals bedoeld door de wetgever en de naleving van de waarborgen in de wet aan de orde komen. Ten tweede wordt het praktische functioneren van de Wbvg vanuit het gezichtspunt van de gegevensvragers en informatieverstrekkers beschouwd.

Het empirische onderzoek in deze rapportage kon alleen maar tot stand komen dankzij de medewerking van velen die bereid waren ons te ontvangen voor een interview of informatie ter beschikking te stellen. Bovendien bedanken we speciaal de parketten en opsporingsdiensten die hun welwillende medewerking hebben verleend aan de uitgevoerde dossierstudies. In het bijzonder zijn we (in alfabetische volgorde) Dick de Boer, Mark Brons, Dick Crijns, Fred Gloudemans, Marianne Kauwenberg, Jolanda de Klerk, Arjen Polstra, Jo van de Rijdt, Arnold Weistra en Ben van der Zanden erkentelijk voor de tijd die zij hebben genomen om de onderzoekers gegevens te verschaffen en wegwijs te maken in de documenten.

Een woord van dank gaat vanzelfsprekend ook uit naar de leden van de begeleidingscommissie, onder voorzitterschap van professor Evert Stamhuis, voor hun bijdrage aan de inhoudelijke en procesmatige voortgang van het uitgevoerde onderzoek (zie bijlage 2). Tot slot bedanken wij ook professor Tijs Kooijmans van de Tilburgse vakgroep Strafrecht voor zijn bijdrage aan de rapportage, en Jorine de Muijnk van het IVA voor haar inspanningen ten behoeve van het empirische onderzoek.

Toine Spapens
Mirjam Siesling
Ellen de Feijter

Tilburg, oktober 2010

Inhoudsopgave

Lijst van gebruikte afkortingen x

Samenvatting xiii

1 Inleiding 1
1.1 Achtergrondschets 1
1.2 Vraagstelling 2
1.3 Informatiebronnen 4
1.3.1 Cijfermatig overzicht van het gebruik van de Wbvg 5
1.3.2 Verdiepende dossieranalyse 8
1.3.3 Interviews 9
1.4 Leeswijzer 10

2 De totstandkoming van de Wbvg 13
2.1 Inleiding 13
2.2 De Commissie Mevis 13
2.2.1 De knelpunten in de toenmalige praktijk 13
2.2.2 Het standpunt van de Commissie Mevis 15
2.3 Het conceptwetsvoorstel van de Commissie Mevis 16
2.4 Het standpunt van het kabinet 17
2.5 Besluit 20

3 De inhoud van de Wbvg 23
3.1 Inleiding 23
3.2 De systematiek van de toedeling van bevoegdheden in de Wbvg 23
3.3 Identificerende gegevens 25
3.4 Andere dan identificerende gegevens (historisch) 28
3.5 Andere dan identificerende gegevens (toekomstig) 31
3.6 Gevoelige gegevens 35
3.7 Ontsleutelen van versleutelde gegevens 42
3.8 Doorzoeking ter vastlegging van gegevens 42
3.9 Besluit 45

4 De verhouding van de Wbvg tot andere bevoegdheden 47
4.1 Inleiding 47
4.2 Het vorderen van gegevens van aanbieders van telecommunicatie 47
4.3 De bevoegdheden tot inbeslagneming van voorwerpen 49
4.4 Bevoegdheden in het kader van ontnemingsvorderingen 50

4.5 De bevoegdheden van de Algemene wet bestuursrecht 51
4.6 De bevoegdheden in enkele bijzondere wetten 52
4.7 Besluit 53

5 Het opsporingsproces in relatie tot de Wbvg 55
5.1 Inleiding 55
5.2 De organisatie van het opsporingsproces 55
5.2.1 De rol van het openbaar ministerie 55
5.2.2 De organisatie van de opsporing bij de politie 56
5.2.3 De opsporingstaken van de Koninklijke Marechaussee.....58
5.2.4 De opsporingstaken van de Bijzondere Opsporingsdiensten 58
5.3 Uitvoering van opsporingsonderzoek.....59
5.3.1 Reactief opsporingsonderzoek 60
5.3.2 Proactief opsporingsonderzoek 65
5.4 Besluit 67

6 Het beroep op de Wbvg: omvang, aard en procedures 69
6.1 Inleiding 69
6.2 Het beroep op art. van de Wbvg.....69
6.2.1 Geregistreerde vorderingen per wetsartikel 70
6.2.2 De aard van de gevraagde gegevens 74
6.2.3 De geadresseerde gegevenshouders 76
6.2.4 Identificerende gegevens 77
6.3 Procedures in relatie tot de Wbvg 79
6.3.1 Vorderingen door de politie en de BOD'en 80
6.3.2 De werkwijze op de parketten.....81
6.4 Besluit 83

7 De toepassing van de wet: perspectief van gegevensvragers.....85
7.1 Inleiding 85
7.2 De ervaringen van opsporingsambtenaren met de Wbvg.....85
7.2.1 Politie 85
7.2.2 FIOD 89
7.2.3 Algemeen oordeel vanuit de optiek van de opsporingsdiensten 93
7.3 De ervaringen van het openbaar ministerie met de Wbvg 95
7.3.1 Toepassing van de verschillende onderdelen van de wet.....95
7.3.2 Verhouding tot andere BOB-bevoegdheden 96
7.3.3 Gebruik van gegevens in meerdere onderzoeken.....97
7.3.4 Notificatieplicht 98
7.3.5 Knelpunten in de praktijk.....99
7.3.6 'Trans Link' en de gevolgen 101

7.3.7 Algemeen oordeel over de Wbvg: verbetering?.....107
7.4 Besluit.....108

8 De toepassing van de wet: het perspectief van de gegevenshouders ..111
8.1 Inleiding.....111
8.2 Financiële instellingen.....111
8.2.1 Aantal vorderingen en werkbelasting.....111
8.2.2 Procedure.....112
8.2.3 Vrijwilligheid.....113
8.2.4 Waarborgen ter bescherming van de gegevensverstrekkers.....114
8.2.5 Beklagregeling.....115
8.2.6 Knelpunten.....115
8.3 Niet-financiële instellingen.....117
8.3.1 Aantal vorderingen en werkbelasting.....117
8.3.2 Procedure.....117
8.3.3 Vrijwilligheid.....118
8.3.4 Waarborgen ter bescherming van de gegevensverstrekkers.....120
8.3.5 Beklagregeling.....121
8.3.6 Knelpunten.....121
8.4 Besluit.....122

9 Algemeen besluit.....125
9.1 Inleiding.....125
9.2 Beantwoording van de onderzoeksvragen.....125
9.3 Afsluitende observaties.....135

Summary.....137

Bijlage 1 Schematisch overzicht bevoegdheden Wbvg.....145

Bijlage 2 Samenstelling van de begeleidingscommissie.....153

Bibliografie.....155

Lijst van gebruikte afkortingen

AID	Algemene Inspectiedienst
Awb	Algemene wet bestuursrecht
Awr	Algemene wet inzake rijksbelastingen
BOB	Bijzondere opsporingsbevoegdheden
BOD	Bijzondere Opsporingsdienst
BR	Bovenregionale Recherche
BVO	Basisvoorziening Opsporing
CIE	Criminele Inlichtingeneenheid
CIOT	Centraal Informatiepunt Onderzoek Telecommunicatie
COMPAS	Communicatiesysteem Openbaar Ministerie - Parket Administratie Systeem
EVRM	Europees Verdrag ter bescherming van de rechten van de mens
FIOD	Fiscale Inlichtingen- en Opsporingsdienst - Economische Controledienst
FP	Functioneel Parket
GVO	Gerechtelijk Vooronderzoek
GW	Grondwet
Hovj	Hulpofficier van justitie
HR	Hoge Raad
IOD	Inlichtingen- en Opsporingsdienst, ministerie van VROM
KLPD	Korps Landelijke Politiediensten
KMAR	Koninklijke Marechaussee
LP	Landelijk Parket
LROvJ	Landelijke vergadering van rechercheofficieren van justitie
MTV	Mobiel Toezicht Vreemdelingen
MvT	Memorie van Toelichting
NAW	Naam-adres-woonplaats
NR	Nationale Recherche
nVWA	Nieuwe Voedsel en Warenautoriteit
OVC	Opnemen van vertrouwelijke communicatie met een technisch hulpmiddel
PV	Proces-verbaal
SFO	Strafrechtelijk Financieel Onderzoek
SIOD	Sociale Inlichtingen- en Opsporingsdienst
Sr	(Wetboek van) Strafrecht
Sv	(Wetboek van) Strafvordering
TGO	Team Grootschalige Opsporing
Wbp	Wet bescherming persoonsgegevens
Wbvg	Wet bevoegdheden vorderen gegevens

WED	Wet op de Economische Delicten
Wet BOB	Wet op de Bijzondere opsporingsbevoegdheden
WODC	Wetenschappelijk Onderzoek- en Documentatiecentrum
WVMC	Wet Voorkoming Misbruik Chemicaliën
WvSv	Wetboek van Strafvordering

Samenvatting

Tot enkele jaren geleden waren de bevoegdheden voor opsporingsdiensten (de politie en de bijzondere opsporingsdiensten) om van derde partijen gegevens te verkrijgen op een aantal punten problematisch. De Commissie Mevis kreeg derhalve tot taak te onderzoeken of het Wetboek van Strafvordering (WvSv), gelet op de ontwikkelingen op het gebied van de informatie- en communicatietechnologie, voorzag in een toereikend wettelijk kader voor die vormen van gegevensvergaring die voor de strafvordering noodzakelijk zijn. De commissie kwam tot de conclusie dat het WvSv aanpassing behoefde en vertaalde die bevinding in een conceptwetsvoorstel. Dit voorstel is uitgemond in de Wet bevoegdheden vorderen gegevens (Wbvg), die op 1 januari 2006 in werking is getreden. De centrale doelstelling van deze wet is een einde te maken aan de onduidelijkheid en rechtsonzekerheid die werd veroorzaakt door de ontoereikendheid van de kaders voor het vorderen van gegevens van derden die op dat moment ter beschikking stonden.

De Wbvg diende, conform de toezegging van de minister van Justitie aan de Tweede Kamer, na vier jaar te worden geëvalueerd. Daartoe is een onderzoek uitgevoerd door het Departement Strafrechtswetenschappen van de Universiteit van Tilburg en het IVA, onderzoeksinstituut voor sociaalwetenschappelijk beleidsonderzoek en -advies, dat is gelieerd aan de Universiteit van Tilburg.

De evaluatie van de wet concentreerde zich op drie principiële onderwerpen. Allereerst diende het aantal en de aard van de vorderingen die op grond van de Wbvg worden gedaan te worden vastgesteld. In de tweede plaats moest de toepassing van de wet en de waarborgen die erin zijn opgenomen, worden beoordeeld. Ten derde diende het oordeel van de gegevenshouders en gegevensvragers omtrent het functioneren van de Wbvg te worden onderzocht. Deze drie onderdelen zijn vertaald in vier hoofdvragen:

1 In welke mate en ten behoeve waarvan wordt een beroep op de Wbvg gedaan?
2 Wordt de wet toegepast zoals bedoeld en omschreven door de wetgever?
3 Worden de waarborgen die zijn opgenomen in de Wbvg nageleefd?
4 Hoe functioneert de Wbvg vanuit het perspectief van de gegevensverstrekkers?

Onderzoeksmethoden

Om de bovenstaande vragen te kunnen beantwoorden zijn drie methodieken toegepast: verzamelen en analyseren van cijfermatige gegevens, analyse van dossiers van afgesloten opsporingsonderzoeken en interviews met gegevenshouders

en gegevensvragers. In de praktijk bleken de beide eerstgenoemde gegevensbronnen aan beperkingen onderhevig.

Landelijke registratiegegevens om een cijfermatig beeld te kunnen schetsen van het gebruik van de Wbvg zijn niet voorhanden. Ook bij de individuele parketten, politieregio's en de bijzondere opsporingsdiensten bleken zulke registraties maar beperkt voorhanden. Om die reden is gekozen om cijfers, waar mogelijk, zelf te verzamelen bij vier parketten, drie politieregio's en een bijzondere opsporingsdienst. Achtereenvolgens betrof het de parketten van Amsterdam, Den Bosch en Groningen en het Functioneel Parket (FP), de politieregio's Amsterdam-Amstelland, Brabant-Noord, Groningen en de Fiscale Inlichtingen- en Opsporingsdienst - Economische Controledienst (FIOD). Van de parketten van Den Bosch en Groningen, alsmede van de FIOD kon de gevraagde informatie worden verkregen. Op de andere locaties was dit slechts beperkt of in het geheel niet mogelijk.

In de tweede plaats leverde een diepgaande dossierstudie, anders dan verwacht, maar een beperkte bijdrage aan de beantwoording van de onderzoeksvragen, zo bleek na het bestuderen van een dertigtal zaakdossiers. De nadruk van de evaluatie is om deze redenen sterker dan bedoeld, komen liggen op interviews met gegevenshouders en gegevensvragers.

De inhoud van de Wbvg

Op grond van de Wbvg kunnen om te beginnen, door een opsporingsfunctionaris, identificerende gegevens worden gevorderd (art. 126nc Sv). De officier van justitie heeft de bevoegdheid andere dan identificerende gegevens te vorderen die de gegevenshouder al heeft verwerkt (art. 126nd Sv) en kan derden bevelen medewerking te verlenen aan het ontsleutelen van gegevens die versleuteld zijn opgeslagen (art. 126nh Sv). De officier van justitie heeft voorts de bevoegdheid de doorzoeking ter vastlegging van gegevens te vorderen (art. 125i Sv). Hiernaast kunnen ook toekomstige gegevens (art. 126ne Sv) die bij een derde beschikbaar komen, worden gevorderd, alsmede gevoelige gegevens (art. 126nf Sv). In die gevallen dient de officier van justitie echter over een machtiging van de rechter-commissaris te beschikken. De voorwaarden die gelden voor het vorderen van gegevens op grond van de Wbvg zijn derhalve zwaarder al naar gelang de categorie gegevens ingrijpender is voor de persoonlijke levenssfeer en/of naarmate meer handelingen van een derde worden gevraagd. De Wbvg biedt de mogelijkheid niet alleen over de verdachte gegevens te vorderen, maar ook over andere personen indien dat in het belang van het onderzoek is. Beklag tegen een vordering staat (achteraf) open op grond van art. 552a Sv.

Het gebruik van de Wbvg in de praktijk

Navolgend wordt ingegaan op de uitkomsten van het empirische onderzoek dat in het kader van de onderhavige evaluatie is uitgevoerd. Om te beginnen zijn daarbij de aard en omvang van het gebruik van Wbvg-bevoegdheden aan de orde, alsmede de procedures die door de opsporingsinstanties worden gehanteerd bij het doen van vorderingen.

Een eerste belangrijke bevinding is dat slechts enkele onderdelen van de Wbvg intensief worden gebruikt. Het gaat daarbij om art. 126nc Sv en 126nd Sv. Verzoeken om toekomstige gegevens (art. 126ne Sv), gevoelige gegevens (art. 126nf Sv), het ontsleutelen van versleutelde gegevens (art. 126nh Sv) en de digitale doorzoeking (art. 125i Sv) zijn in opsporingsonderzoeken zelden nodig. Overigens mag worden verwacht, gezien een uitspraak van de Hoge Raad in de zaak Trans Link (zie hierna), dat in de toekomst het beroep op art. 126nf Sv zal toenemen.

In de tweede plaats kan worden vastgesteld dat weliswaar informatie wordt gevorderd over een breed spectrum aan onderwerpen, maar dat de nadruk sterk ligt op slechts twee typen gegevens: financiële informatie en camerabeelden. Deze omvatten 72 procent van de vorderingen op grond van de Wbvg. Financiële instellingen ontvangen verreweg de meeste verzoeken, die overigens ook vaak op camerabeelden betrekking hebben. Daarnaast krijgen overheidsinstanties relatief veel vorderingen op grond van de Wbvg.

De opsporingsdiensten en de parketten hanteren vaste procedures met betrekking tot het indienen van Wbvg-vorderingen. Eén van de veronderstellingen van de wetgever, namelijk dat bij de opsporingsdiensten slechts een beperkt aantal functionarissen zou worden geautoriseerd om vorderingen op grond van art. 126nc te doen, blijkt niet te kloppen. Bij sommige opsporingsdiensten kunnen alle hulpofficieren van justitie deze vorderingen doen, en bij andere zijn zelfs alle opsporingsmedewerkers gerechtigd identificerende gegevens te vorderen, voor zover het niet gaat om financiële gegevens.

Ervaringen van gegevensvragers

De Wbvg blijkt bij de opsporingsinstanties te zijn ‘ingeburgerd’ en veelvuldig door hen te worden gebruikt. Het van kracht worden van de wet heeft inhoudelijk echter geen grote veranderingen met zich meegebracht. De consequentie is vooral dat de gang van zaken rond het opvragen van gegevens bij derden thans duidelijker is geformaliseerd. De relaties met de gegevenshouders worden vanuit de optiek van de gegevensvragers als goed beoordeeld. In vrijwel alle zaken werkt de gegevensverstrekker mee aan het uitleveren van de gevorderde gegevens.

De opsporingsdiensten en het openbaar ministerie waarderen de toegenomen zorgvuldigheid van de procedure van het vorderen van gegevens bij der-

den door de komst van de Wbvg. De verplichting om mee te werken heeft een einde gemaakt aan soms langdurige discussies met de privacyexperts van gegevenshouders en de juridische waarborgen van de procedure zijn niet alleen voor hen, maar ook voor de gegevensvragers waardevol.

Voor de wetgever was een essentieel punt dat vrijwillige gegevensverstrekking met de Wbvg zou worden uitgebannen. De rondgang langs gegevensvragers laat zien dat dit ook goeddeels gerealiseerd is. De procedures van de Wbvg zijn inmiddels breed bekend, en in principe weten de medewerkers van de opsporingsinstanties dat zij deze moeten hanteren. Zij willen bovendien geen procesrisico lopen en zorgen ervoor dat verantwoord kan worden hoe opsporingsinformatie verzameld is. Ook de regelmatig aangezochte gegevenshouders zijn inmiddels goed op de hoogte van hun rechten en plichten en zijn niet (meer) bereid vrijwillig informatie te verstrekken. Alleen wanneer partijen slechts zeer incidenteel om informatie wordt gevraagd, door opsporingsfunctionarissen die niet goed op de hoogte zijn van de Wbvg, is vrijwillige uitlevering soms nog aan de orde, alsook in zeer incidentele gevallen waarin zowel de Wbvg als andere wetgeving niet voorziet in de mogelijkheid de informatie formeel te vorderen.

Praktische knelpunten vanuit het gezichtspunt van gegevensvragers

De gegevensvragers brengen twee praktische en vier juridische knelpunten naar voren in verband met het functioneren van de Wbvg. Navolgend wordt eerst ingegaan op de praktische knelpunten.

Het eerste praktische probleem dat algemeen wordt ervaren is de toegenomen administratieve belasting als gevolg van het van kracht worden van de Wbvg. Het vorderen van gegevens vergt bijvoorbeeld het opmaken van aanvraag processen-verbaal, die ter toetsing moeten worden voorgelegd aan de officier en eventueel ook de rechter-commissaris, de feitelijke vordering moet worden opgemaakt, de ontvangst van de gegevens moet worden geadministreerd, en degene omtrent wie informatie is gevorderd, moet in bepaalde gevallen worden genotificeerd. Dit alles brengt in de ogen van de opsporingsinstanties een omvangrijke ‘papierwinkel’ met zich mee.

Het tweede praktische probleem is de wijze waarop banken en geldinstellingen gevorderde financiële gegevens aanleveren. Deze klacht kan vooral worden beluisterd bij de FIOD, die vaak grootschalige vorderingen doet. Om te beginnen zijn financiële instellingen vaak traag met het uitleveren van gegevens. Voorts weigeren zij informatie digitaal aan te leveren, waardoor de gegevensvragers met hogere kosten worden geconfronteerd, niet alleen omdat nu per afschrift moet worden betaald, maar ook omdat de aangeleverde informatie eerst weer in de computer moet worden ingevoerd.

Juridische knelpunten vanuit het gezichtspunt van de gegevensvragers

De vier knelpunten met een meer juridisch dan praktisch karakter betreffen de gevolgen van de uitspraak van de Hoge Raad in het zogenoemde 'Trans Link-arrest', het maken van een correct onderscheid tussen art. 126nc Sv en 126nd Sv, de overlap tussen de begrippen 'gegeven' en 'voorwerp' en, tot slot, de problematiek rondom geheimhouders.

In de zaak Trans Link ging het om door het openbaar ministerie gevorderde foto's van houders van OV-chippassen. De Hoge Raad oordeelde in deze zaak dat dergelijke foto's gevoelige informatie kunnen bevatten – iemands etnische afkomst kan er bijvoorbeeld uit worden afgeleid – die bovendien direct is gekoppeld aan andere gegevens zoals de naam van de betrokkene. De consequentie van deze uitspraak is dat dergelijke informatie alleen op grond van art. 126nf Sv mag worden gevorderd. Hiervoor is niet alleen een zwaardere verdenking vereist, maar ook de tussenkomst van de rechter-commissaris. Dit criterium werd in eerste instantie ook van toepassing geacht op camerabeelden die in de openbare ruimte worden gemaakt. Omdat deze beelden veelvuldig worden gevorderd, ook wanneer sprake is van relatief lichte strafbare feiten, zou dat dus grote consequenties hebben voor de opsporingspraktijk. Dit knelpunt is nog altijd niet weggenomen, hoewel lagere rechtbanken het Trans Link-arrest inmiddels wel hebben genuanceerd. De minister van Justitie volgt vooralsnog de lijn van de Hoge Raad inzake de bijzondere bescherming voor beeldmateriaal die aan persoonsgegevens kan worden gekoppeld. De minister lijkt beelden van bewakingcamera's echter uit te sluiten van de categorie 'bijzondere persoonsgegevens' waar art. 125nf Sv op ziet, zij het dat hij het eindoordeel aan de officier van justitie over laat.

Het tweede knelpunt van juridische aard is het maken van onderscheid tussen art. 126nc Sv en 126nd Sv. De wetgever heeft deels een limitatieve lijst in de Wbvg opgenomen van vorderingen die onder de noemer van art. 126nc vallen, maar deels ook enige ruimte gelaten voor interpretatie. Die ruimte betreft de administratieve kenmerken waarmee een persoon bij een bedrijf of instelling bekend. Daaronder kunnen *bijvoorbeeld* een nummer van een polis, of een lidmaatschapsnummer vallen. Vanzelfsprekend geven vragen die wel op grond van art. 126nc Sv worden gesteld, maar daarop onterecht zijn gebaseerd, bijvoorbeeld hoe lang iemand al een kluis huurt bij een bank, aanleiding tot discussie.

Ten derde is een onderscheid tussen een 'voorwerp' en een 'gegeven' niet in alle gevallen duidelijk te maken. Een origineel document met tekst bevat bijvoorbeeld gegevens, maar is ook een voorwerp. Eén vraagpunt is of documenten die op grond van de Wbvg zijn verkregen ook als voorwerp mogen worden behandeld, en bijvoorbeeld ook voor forensisch onderzoek mogen worden gebruikt. Een ander aandachtspunt is dat bij inbeslagneming van voorwerpen

waarborgen gelden, bijvoorbeeld de mogelijkheid tot teruggave, die niet van toepassing zijn wanneer het voorwerp op grond van de Wbvg is verkregen.

Tot slot is het vraagstuk van misbruik van verschoningsgerechtigden naar voren gekomen. Dit wordt nu nog niet breed ervaren, maar wel gesignaleerd als een vraagstuk waarvan het belang in de toekomst kan groeien. Het probleem bestaat eruit dat van geheimhouders geen gegevens kunnen worden gevorderd op grond van de Wbvg. Opsporingsinstanties zien dat malafide (rechts)personen bij uiteenlopende zakelijke transacties een verschoningsgerechtigde, bijvoorbeeld een advocatenkantoor, inschakelen om deze aldus af te schermen. Vanzelfsprekend wordt de opsporing daardoor ernstig gehinderd.

Ervaringen van gegevenshouders

Wanneer de ervaringen van gegevenshouders worden beschouwd, kan onderscheid worden gemaakt tussen de financiële instellingen enerzijds, en de overige bedrijven anderzijds. De eerstgenoemden ontvangen, zoals al werd vermeld, verreweg de meeste vorderingen.

In algemene zin kan worden geconcludeerd dat gegevenshouders, zowel in de financiële sector als daarbuiten, tevreden zijn over de veranderingen die de Wbvg met zich mee heeft gebracht. De regelgeving heeft ook voor gegevenshouders duidelijkheid gecreëerd omtrent de procedure van het uitleveren van informatie, en heeft een einde gemaakt aan de soms langdurige discussies met opsporingsinstanties over vrijwillige uitlevering. De behandeling van vorderingen op grond van de Wbvg verloopt zonder noemenswaardige problemen. Dit neemt niet weg dat er wel enkele structurele aandachtspunten zijn.

Om te beginnen klagen vooral financiële instellingen over de substantiële groei van het aantal en de complexiteit van de vorderingen. Ook geven zij aan dat de opsporingsdiensten ten onrechte denken dat de informatie waarom zij vragen (altijd) met een druk op de knop voorhanden is. Verder achten vertegenwoordigers van financiële instellingen de vergoedingen voor het aanleveren van gegevens niet in overeenstemming met de kosten die moeten worden gemaakt. Andere bedrijven, en dan vooral degene die regelmatig met vorderingen op grond van de Wbvg worden geconfronteerd, beschouwen eveneens de tijd en de kosten die gepaard gaan met het afhandelen van de informatievragen als knelpunt. Zowel de financiële instellingen als andere gegevenshouders zetten af en toe ook vraagtekens bij de omvang van de vorderingen waarmee zij soms te maken krijgen.

De beklagregeling waarin in de Wbvg is voorzien, wordt niet of nauwelijks gebruikt. Hier is de oorzaak echter niet zozeer dat de regeling niet adequaat is, maar eerst en vooral de omstandigheid dat de gegevenshouders en -vragers geschillen op andere manieren, in onderling overleg, oplossen. De regeling moet

vooral worden gezien als *ultimum remedium* en behoeft als zodanig geen aanpassing.

Tot slot kan worden vastgesteld dat de notificatieregeling die is opgenomen in de Wbvg in de praktijk slecht functioneert. Deels lijkt dit een probleem van onbekendheid met de regeling. Voor een ander deel blijkt de regeling voor opsporingsinstanties moeilijk interpreteerbaar en hanteerbaar.

Afsluitende observaties

Op grond van het uitgevoerde onderzoek is een aantal afsluitende observaties gedaan. De belangrijkste worden hier op een rij gezet.

Over het algemeen blijkt uit deze evaluatie dat gegevenshouders ruimhartig medewerking verlenen aan vorderingen op grond van de Wbvg. Alleen financiële instellingen blijken drempels op te werpen, door lang over uitlevering te doen en gegevens alleen op papier aan te leveren en niet digitaal. In dit kader zouden stringentere eisen kunnen worden gesteld, gezien de grote verantwoordelijkheid die financiële instellingen in het economische verkeer hebben, en het toenemende belang van onderzoek naar geldstromen.

Een mogelijkheid om meer duidelijkheid te scheppen, die ook van belang is in verband met het thans niet geheel afgebakende onderscheid tussen een 'gegeven' en een 'voorwerp', is de gegevensvrager te laten aangeven hoe hij de gewenste informatie wenst te ontvangen. Daarmee kan enerzijds worden voorkomen dat voorwerpen worden uitgeleverd wanneer gegevens worden gewenst en anderzijds dat gegevenshouders er om hun moverende redenen voor kiezen informatie uit te leveren op manieren die zowel voor henzelf als voor de gegevensvragers inefficiënt zijn.

Vervolgens valt het te overwegen om de reikwijdte van art. 126nc, die nu niet volledig is afgebakend, duidelijker te definiëren. In het verlengde daarvan is het een optie om de bevoegdheid tot het afgeven van dergelijke vorderingen expliciet te beperken tot hulpofficieren van justitie, en die, voor zover dat thans niet reeds het geval is, ook specifiek op te leiden op het vlak van de Wbvg.

Voorts is duidelijk geworden dat de ruimte die de wetgever heeft gelaten met betrekking tot de 'bijvangst' van gevoelige gegevens terwijl de opsporingsinstanties daar niet specifiek in geïnteresseerd zijn, tot problemen heeft geleid en wel in het Trans Link-arrest. Hoewel lagere rechters deze uitspraak inmiddels hebben genuanceerd, is het toch een punt van overweging om, conform een advies van professor Mevis, het 'ernstvereiste' in het geval van het vorderen van camerabeelden in de openbare ruimte te laten vervallen.

Tot slot is het misbruik dat malafide (rechts)personen kunnen maken van geheimhouders, omdat die thans geheel zijn gevrijwaard van vorderingen in het kader van de Wbvg, een aandachtspunt waarop nadrukkelijk dient te worden geanticipeerd.

1 Inleiding

1.1 Achtergrondschets

Informatie is van essentieel belang voor het rechercheproces. De politie verzamelt tijdens opsporingsonderzoeken enerzijds met eigen middelen gegevens, maar is anderzijds ook aangewezen op informatie die bij andere partijen voorhanden is. Dat kunnen andere overheidsinstanties zijn, zoals de gemeente of de belastingdienst. Het kan echter ook gaan om private partijen, in de vorm van bedrijven en instellingen, of individuele burgers. Snelle technische ontwikkelingen, bijvoorbeeld in de informatie- en communicatietechnologie, hebben er in de afgelopen decennia voor gezorgd dat steeds meer voor de opsporing relevante gegevens bij private partijen beschikbaar zijn. Te denken valt aan verkeersgegevens van mobiele telefoons, tenaamstellingen van IP-adressen, beelden van bewakingscamera's, informatie omtrent goederen die aangekocht zijn via het internet, enzovoort. Uiteraard is het zaak dat opsporingsinstanties in voorkomende gevallen op deze informatie een beroep kunnen doen, welk beroep vanzelfsprekend moet zijn omkleed met waarborgen. Tot enkele jaren geleden waren de bevoegdheden om van derde partijen, dat wil zeggen niet-overheidsinstanties, gegevens te verkrijgen ontoereikend en dit vormde de aanleiding om tot de Wet bevoegdheden vorderen gegevens (Wbvg) te komen.

Aan de wet ligt het rapport van de Commissie Mevis ten grondslag. De commissie was ingesteld naar aanleiding van in de strafvorderlijke praktijk ervaren moeilijkheden met betrekking tot de vergaring van gegevens voor de opsporing en de vervolging van strafbare feiten. De taak van de commissie was dan ook te onderzoeken of, op dat moment, het Wetboek van Strafvordering (WvSv) voorzag in een toereikend wettelijk kader voor die vormen van gegevensvergaring die voor de strafvordering noodzakelijk zijn. De commissie constateerde verschillende knelpunten en werkte die uit in een conceptwetsvoorstel. Het kabinet deelde het standpunt van de Commissie Mevis dat aanpassing van het WvSv aangewezen was en nam het concept op hoofdlijnen over. Het resultaat was de Wbvg, die op 1 januari 2006 in werking is getreden. Tijdens de mondelinge behandeling in de Eerste Kamer van de Wbvg is door de toenmalige minister van Justitie de toezegging gedaan de desbetreffende wet te evalueren.[1] Het voor u liggende boek vormt daarvan de weerslag. Deze evaluatie is, in opdracht van het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) van het ministerie van Justitie, uitgevoerd door het Departement Strafrechtsweten-

[1] *Handelingen I*, 2004-2005, p. 1493-1504.

schappen van de Universiteit van Tilburg, in samenwerking met het IVA, onderzoeksinstituut voor sociaalwetenschappelijk beleidsonderzoek en -advies, dat is gelieerd aan de Universiteit van Tilburg. Het onderzoek werd gestart in november 2009 en afgerond in september 2010.

1.2 Vraagstelling

De door de minister van Justitie gevraagde evaluatie van de Wbvg heeft betrekking op drie principiële onderwerpen. Allereerst diende de feitelijke aard en de omvang van de vorderingen die op grond van de Wbvg worden gedaan cijfermatig te worden vastgesteld. In de tweede plaats diende een beoordeling te worden gegeven van de toepassing van de wet en de waarborgen die erin zijn opgenomen. Tot slot is verzocht het oordeel van de gegevensvragers en gegevenshouders omtrent het functioneren van de Wbvg te evalueren. Deze drie centrale onderwerpen zijn vertaald in de volgende vier onderzoeksvragen:

1 In welke mate en ten behoeve waarvan wordt een beroep op de Wbvg gedaan?
2 Wordt de wet toegepast zoals bedoeld en omschreven door de wetgever?
3 Worden de waarborgen die zijn opgenomen in de Wbvg nageleefd?
4 Hoe functioneert de Wbvg vanuit het perspectief van de gegevensverstrekkers?

In het vervolg van deze paragraaf worden deze vragen nader afgebakend.

1 In welke mate en ten behoeve waarvan wordt een beroep op de Wbvg gedaan?

De eerste onderzoeksvraag heeft betrekking op de kwantitatieve aspecten van de Wbvg. Om te beginnen is de vraag aan de orde hoe vaak in een gegeven periode een beroep is gedaan op de Wbvg. Daarnaast dient ook inzichtelijk te worden gemaakt door wie de onderzoeksgegevens worden gevorderd en in het kader van welk type opsporingsonderzoeken, alsmede aan welke derde partijen de vorderingen worden gericht. Op voorhand kan worden gesteld dat deze vragen maar gedeeltelijk konden worden beantwoord, aangezien hieromtrent noch op landelijk niveau, noch bij de geraadpleegde parketten, politieregio's en een Bijzondere Opsporingsdienst, te weten de FIOD, een (complete) registratie werd bijgehouden. In paragraaf 1.3 wordt op de problematiek van het verkrijgen van kwantitatieve gegevens gedetailleerder teruggekomen.

2 Wordt de wet toegepast zoals bedoeld en omschreven door de wetgever?

De tweede onderzoeksvraag doelt enerzijds op de werking van de Wbvg in de praktijk en anderzijds op de vraag of het feitelijke gebruik ook aansluit bij de bedoeling van de wetgever.

In de Wbvg is onderscheid gemaakt tussen verschillende categorieën van gegevens (zie hoofdstuk 3, alsmede bijlage 1) en worden per type uiteenlopende randvoorwaarden aan de vordering gesteld. De vraag is dan ook of deze indeling in de praktijk hanteerbaar en toepasbaar is. In algemene zin diende te worden nagegaan of de bevoegdheden waarin de Wbvg voorziet toereikend zijn vanuit het perspectief van de opsporingsverantwoordelijken. Ook andere uitvoeringsaspecten, zoals de administratieve belasting voor de opsporingsinstanties, de tijdigheid waarmee gegevens ter beschikking komen, liggen ter evaluatie voor. Voorts is het de vraag of de Wbvg (soms) juist niet wordt toegepast in situaties waarin dat mogelijk is, maar waarin ook voor alternatieven kan worden gekozen. Een belangrijk aspect daarbij is het feit dat de Wbvg niet het gehele spectrum van de gegevensverstrekking door derden afdekt. Ook andere regelgeving biedt de mogelijkheid gegevens van private partijen te verkrijgen.

3 Worden de waarborgen die zijn opgenomen in de Wbvg nageleefd?

Het vorderen van privacygevoelige gegevens van burgers dient met waarborgen te zijn omkleed, en ook daarin is in de Wbvg vanzelfsprekend voorzien. De vraag die voorligt, is of deze waarborgen in de praktijk ook worden nageleefd. Worden gegevens bijvoorbeeld alleen in het belang van het onderzoek gevorderd? Houden de opsporingsinstanties zich aan de voorwaarde dat niet meer gegevens dan strikt noodzakelijk worden gevorderd? Wordt er alleen gericht om informatie gevraagd? Wordt er zorgvuldig omgegaan met persoonsgegevens? Functioneert de notificatieplicht in de praktijk? Wordt de hand gehouden aan het getrapte systeem van bevoegdheidstoedeling?

4 Wat zijn de gevolgen van de Wbvg voor de gegevensverstrekkers?

De vierde hoofdvraag in het onderzoek betreft de gevolgen van het moeten voldoen aan vorderingen in het kader van de Wbvg voor de gegevensverstrekkers. Het vertrekpunt is dat bedrijven, instellingen of individuen die te maken krijgen met een informatievordering daarmee zo min mogelijk mogen worden belast. Ook op dat vlak zijn waarborgen in de Wbvg opgenomen. Zo kan van derden niet worden verlangd dat zij informatie vastleggen die niet al in het kader van de gewone bedrijfsvoering wordt geregistreerd. Buiten deze en andere waarborgen

is het in de praktijk onvermijdelijk dat partijen die gegevens verstrekken daarvoor soms inspanningen moeten doen buiten de normale bedrijfsvoering om. De mogelijkheid bestaat ook dat bepaalde databases niet zonder meer geschikt zijn om de gevorderde informatie in op te zoeken, en dat mogelijk technische aanpassingen moeten worden gedaan om dat wel mogelijk te maken. De vragen die dit met zich meebrengt, zijn welke kosten met de informatieverstrekking gemoeid zijn en welke infrastructurele maatregelen de gegevensbeheerders eventueel hebben moeten treffen om gevraagde gegevens te kunnen leveren.

1.3 Informatiebronnen

Om de Wbvg te kunnen evalueren is, gezien de aard van de onderzoeksvragen, informatie uit verschillende bronnen benodigd. In deze paragraaf zullen deze bronnen en de gehanteerde onderzoeksopzet nader de revue passeren. Ten behoeve van de onderhavige studie was een drieledige aanpak voorgenomen, die echter niet helemaal volgens plan kon worden uitgevoerd.

In de eerste plaats was voorgenomen registratiegegevens te verzamelen omtrent het gebruik van de Wbvg, zowel op landelijk niveau als bij vier geselecteerde parketten, drie politieregio's en een BOD. Ten tweede was het de bedoeling om een selectie van opsporingsdossiers, tijdens welke onderzoeken gegevens op grond van de Wbvg werden gevorderd, diepgaand te analyseren. Tot slot zouden gegevensvragers en gegevenshouders, zowel ten aanzien van deze dossiers als meer in het algemeen, worden geïnterviewd.

In de praktijk bleek, zoals hiervoor al werd opgemerkt, het om te beginnen, te ontbreken aan registratiegegevens die nodig waren om een compleet cijfermatig beeld te kunnen schetsen, zowel op landelijk als op lokaal niveau.[2] Voorts leverde een diepgaande dossierstudie anders dan verwacht maar een beperkte bijdrage aan de beantwoording van de onderzoeksvragen, zo bleek na het bestuderen van een dertigtal zaakdossiers. De nadruk van de evaluatie is om deze redenen sterker komen liggen op interviews met gegevensvragers en gegevenshouders. Navolgend wordt nader ingegaan op de uitvoering van het onderzoek en de vraagstukken die daarbij aan de orde zijn gekomen.

---

[2] Dit werd overigens ook al onderkend tijdens het debat in de Eerste Kamer waarin de evaluatie van de Wbvg aan de orde kwam. Toenmalig minister van Justitie Donner wees er al op dat cijfermatige evaluatie niet mogelijk zou zijn omdat het afzonderlijk moeten registreren hoe vaak de bevoegdheden zijn gebruikt en op welke wijze, tot een vrijwel onmogelijke administratieve last zou leiden bij de opsporingsinstanties. *Handelingen I*, 2004-2005, p. 1495.

1.3.1 Cijfermatig overzicht van het gebruik van de Wbvg

In het kader van de Wbvg kunnen verschillende instanties gegevens vorderen. Deels kunnen de opsporingsdiensten zelfstandig vorderingen doen, en deels is daarvoor de tussenkomst van de officier van justitie of de rechter-commissaris noodzakelijk (zie bijlage 1 en hoofdstuk 3).

Opsporingsdiensten[3]

De Nederlandse politie is georganiseerd in 25 politieregio's en het Korps Landelijke Politiediensten. Daarnaast bestaan er vier Bijzondere Opsporingsdiensten (BOD'en), namelijk de Fiscale Inlichtingen- en Opsporingsdienst Economische Controledienst (FIOD)[4], de Sociale Inlichtingen- en Opsporingsdienst (SIOD), de Algemene Inspectiedienst (AID) van het toenmalige ministerie van Landbouw, Natuur en Voedselkwaliteit, en de Inlichtingen- en Opsporingsdienst van het toenmalige ministerie van Volkshuisvesting, Ruimtelijke Ordening en Milieu (IOD).[5] *Last but not least* verricht ook de Koninklijke Marechaussee (KMAR) opsporingstaken.

Aangezien het hierbij allemaal gaat om in hoge mate zelfstandige organisaties, wekt het geen verwondering dat van een landelijke registratie van vorderingen op grond van de Wbvg geen sprake is. Om die reden zijn dan ook vier instanties, de politieregio's Amsterdam-Amstelland, Groningen, Brabant-Noord, alsmede de FIOD, geselecteerd om dan tenminste een gedeeltelijk cijfermatig beeld te kunnen schetsen. Echter, ook dat doel kon op drie van de vier locaties niet of maar zeer beperkt worden bereikt, door gebrek aan informatie.

Bij de politie Amsterdam-Amstelland is elke hulpofficier van justitie gerechtigd vorderingen op grond van de Wbvg te doen, voor zover die bevoegdheid toekomt aan een opsporingsambtenaar. Een overzicht daarvan is echter niet voorhanden. Er zijn in de politieregio ruim 300 Hulpofficieren van justitie (Hovj's). Benaderen van individuele hulpofficieren om na te gaan welke vorderingen zij hebben geaccordeerd, was om praktische redenen niet mogelijk.

---

3 In dit boek wordt met de term 'opsporingsdienst' verwezen naar de politie, de Koninklijke Marechaussee en de Bijzondere Opsporingsdiensten. Indien van 'opsporingsinstanties' wordt gesproken, wordt daaronder ook het openbaar ministerie begrepen.

4 Tot juni 2010 werd de afkorting FIOD-ECD gebruikt. Daarna is deze veranderd in FIOD.

5 Per 14 oktober 2010 zijn de ministeries van VROM en LNV opgeheven. Het eerstgenoemde departement is opgegaan in het ministerie van Infrastructuur en Milieu en het laatstgenoemde in het ministerie van Economische zaken, landbouw en innovatie. De AID, tot slot, zal per 1 januari 2012 fuseren met de Nieuwe Voedsel en Warenautoriteit (nVWA).

Bij de politie Groningen worden uitsluitend de zogeheten CIOT (Centraal Informatiepunt Onderzoek Telecommunicatie)-aanvragen centraal geregistreerd omdat die, in tegenstelling tot Wbvg-vorderingen, via het Regionaal Informatieknooppunt/Infodesk worden verstuurd. De vorderingen op grond van de Wbvg worden derhalve niet centraal geadministreerd.[6] Ook hier bleek het onmogelijk om individuele functionarissen te belasten met de vraag cijfermatige gegevens aan te leveren.

Bij de politie Brabant-Noord, waar evenmin een centrale administratie van uitgaande Wbvg-vorderingen wordt bijgehouden, kon enige informatie worden verkregen. De vorderingen kunnen hier op drie verschillende plaatsen zijn geadministreerd, namelijk op de netwerkschijven van de individuele politiemedewerkers die de vorderingen opstellen, of op de netwerkschijven van een team of een district, of in de Basisvoorziening opsporing (BVO), een registratiesysteem waarin opsporingsonderzoeken met betrekking tot zwaardere strafbare feiten zijn opgenomen. Dit laatste systeem is nagezien door een politiefunctionaris, waaruit bleek dat over de periode van januari 2009 tot en met medio mei 2009 in totaal 52 handelingen waren vastgelegd met betrekking tot artikelen uit de Wbvg.[7] Nadere inhoudelijke informatie kon echter niet worden verkregen.

Slechts bij de FIOD konden de vorderingen die door de opsporingsambtenaren zelf waren gedaan, worden achterhaald, aangezien die bij deze dienst worden bijgehouden in het administratiesysteem GEFIS. Het gaat daarbij overigens niet om een registratie waaraan de ten behoeve van het onderzoek benodigde gegevens zonder meer konden worden ontleend. In plaats daarvan kon het worden gebruikt om de oorspronkelijke schriftelijke vorderingen terug te zoeken, waaruit vervolgens door de onderzoekers handmatig de gewenste informatie is overgenomen, en in een apart bestand gezet. Dit is gebeurd bij alle geregistreerde vorderingen van het jaar 2008, waarbij het in totaal om 138 verzoeken ging.

Parketten

Vorderingen op grond van de Wbvg waarvoor de tussenkomst van de officier van justitie of de rechter-commissaris vereist is, worden verstuurd via de arrondissementsparketten, waarvan er 19 zijn, en door het Landelijk Parket (LP) en FP. Het openbaar ministerie registreert zijn werkzaamheden landelijk in het Communicatiesysteem Openbaar Ministerie - Parket Administratie Systeem

---

6 Bron: e-mail van de Projectleider Regionaal Informatieknooppunt politie Groningen, d.d. 11 januari 2010.

7 Bron: gesprek met een recherchemedewerker van de politie Brabant-Noord, d.d. 25 mei 2010.

(COMPAS). Echter, vorderingen op grond van de Wbvg bleken in dit systeem niet te worden geadministreerd.

Ook hier werden derhalve vier parketten geselecteerd om ter plekke nadere informatie te verzamelen. Het betrof de parketten Amsterdam, Groningen, Den Bosch en het FP, de justitiële tegenhangers van de hiervoor genoemde politieregio's, respectievelijk de FIOD. Deze parketten administreren de Wbvg-vorderingen op verschillende manieren, en de navolgende werkwijze kon ten behoeve van de onderhavige evaluatie worden toegepast.

Bij het parket Amsterdam-Amstelland bleek sinds september 2009 een (eenvoudig) registratiesysteem te zijn opgezet in het computerprogramma Microsoft Excel, waarmee de voortgang van zowel de vorderingen in het kader van de Wet op de Bijzondere Opsporingsbevoegdheden (Wet BOB) als de Wbvg wordt bewaakt. Op grond van dit bestand kon inzicht worden verkregen in het aantal vorderingen dat in de maanden september 2009 tot en met januari 2010 was gedaan. In totaal ging het om 383 vorderingen, wat neerkomt op 77 vorderingen per maand. In dat cijfer zijn echter de vorderingen in verband met opsporingsonderzoeken van de regionale recherche niet inbegrepen: deze worden niet centraal geadministreerd. Ook bevat het Excelbestand geen informatie over de aard van de gestelde vraag, en slechts summier over de geadresseerde gegevenshouder. Verdere handmatige gegevensverzameling om ook die informatie te verkrijgen bleek niet haalbaar, aangezien het voor de medewerkers van de desbetreffende administratieve afdeling te belastend was om de afgegeven vorderingen te achterhalen. Daarvoor zou elk afzonderlijk onderzoek moeten worden geopend (digitaal) of opgezocht (papier) en de tekst van de vordering moeten worden nagekeken.

Bij het parket Groningen worden de vorderingen in het kader van de Wet op de Bijzondere Opsporingsbevoegdheden (Wet BOB) en de Wbvg centraal geregistreerd. Helaas voor het onderhavige onderzoek gebeurt dat aan de hand van verzamelcategorieën, namelijk 'telecommunicatie', 'tap', 'observatie' en 'inlichtingenverstrekking'. Onder de laatste categorie worden ook de Wbvg-vorderingen geschaard. Voor het onderhavige onderzoek is die indeling dus niet specifiek genoeg om direct bruikbaar te zijn. Er worden echter ook schriftelijke kopieën van alle uitgaande vorderingen bewaard bij de verantwoordelijke afdeling, de zogeheten 'BOB-kamer'. Hier bleek het wel mogelijk om ter plekke de relevante dossiers in te zien en de benodigde informatie te verzamelen. In totaal zijn 312 dossiers bestudeerd waarin vorderingen in het kader van de Wbvg waren opgenomen. Deze betroffen allen het jaar 2008.

Bij het parket Den Bosch is hoofdzakelijk dezelfde werkwijze toegepast. Hier bleek de centrale registratie verfijnder dan in Groningen, omdat in het systeem elke BOB-activiteit tot op het niveau van art.lid wordt gespecificeerd. In Den Bosch konden dus de Wbvg-activiteiten eerst worden geselecteerd,

waarna de bewuste papieren vorderingen konden worden opgezocht en geanalyseerd. Een nadeel van het registratiesysteem is echter dat het alleen voor de 'reguliere' vorderingen wordt gehanteerd, dat wil zeggen: de meer kleinschalige opsporingsonderzoeken. In 2008 werden in totaal 932 vorderingen gedaan. Vanwege praktische aspecten, zoals de hoge werkdruk op de afdeling die de dossiers in het computersysteem voor de onderzoekers moesten opzoeken, moest hier worden volstaan met een steekproef van 100 dossiers. Aangezien het stuk voor stuk om eenvoudige vorderingen ging, was dat ook voldoende om een beeld te kunnen verkrijgen.

De dossiers van opsporingsonderzoeken die betrekking hebben op zware en georganiseerde misdaad, alsmede op onderzoeken in moordzaken, worden niet geregistreerd bij de BOB-administratie. De dossiers van deze onderzoeken waren echter wel op papier beschikbaar en konden afzonderlijk worden geanalyseerd. Er zijn bij het parket Den Bosch, met inbegrip van de hiervoor genoemde, in totaal 285 dossiers bestudeerd.

Bij het FP, tot slot, worden Wbvg-vorderingen evenmin centraal geadministreerd. Om een beeld te kunnen verkrijgen zouden medewerkers de databestanden van afzonderlijke opsporingsonderzoeken handmatig in de computer moeten nazien om daaruit de relevante vorderingen te achterhalen. Bovendien heeft het FP meerdere locaties en zou dit daarom bij elke afzonderlijke locatie moeten plaatsvinden. Aan een dergelijke exercitie wenste het FP om capacitaire redenen niet mee te werken.

Zonder vooruit te willen lopen op conclusies, kan worden vastgesteld dat het onderzoek slechts een beperkt en louter indicatief cijfermatig beeld heeft opgeleverd van de toepassing van de Wbvg.

1.3.2 Verdiepende dossieranalyse

De tweede stap in de onderhavige studie was een verdiepende analyse van dossiers van opsporingsonderzoeken waarin door een opsporingsambtenaar, een officier van justitie of een rechter-commissaris vorderingen op grond van de Wbvg zijn gedaan. De primaire gedachte hierachter was na te gaan in welke context de vorderingen worden gedaan en of de wijze waarop dat gebeurt conform de bedoeling van de wetgever is. De Wbvg omvat, zoals in hoofdstuk 3 nader zal worden uiteengezet, zes relevante wetsartikelen. Het doel was om per wetsartikel 15 vorderingen diepgaand te bestuderen, in totaal dus 90 stuks.

Feitelijk zijn 31 dossiers bestudeerd. Dit had twee belangrijke redenen. In de eerste plaats konden alleen bij de parketten Groningen, Den Bosch en Amsterdam dossiers worden ingezien. Bij het FP en de politieregio's Amsterdam-Amstelland, Brabant-Noord en Groningen, was dit niet mogelijk, aangezien,

vanwege de hiervoor beschreven ontbrekende centrale registratie, geen selectie kon worden gemaakt van relevante zaken. Van de FIOD, tot slot, kon wel informatie worden verkregen omtrent onderzoeken waarin gegevensvorderingen door opsporingsambtenaren werden gedaan. Deze vorderingen kwamen echter pas in een zeer laat stadium van het onderzoek voorhanden, waardoor de gelegenheid ontbrak om deze te koppelen aan dossiers, deze op te vragen, en nader te bestuderen.

In de tweede plaats bleken slechts enkele artikelen uit de Wbvg (intensief) te worden gebruikt. Daardoor was het niet mogelijk om de vooraf beoogde steekproef te realiseren. De 31 dossiers die wel konden worden ingezien, hadden op twee na alle betrekking op een wetsartikel.

Als onderdeel van de verdiepende dossierstudie was tevens voorgenomen om de betrokken officier van justitie en de gegevenshouders te interviewen over die specifieke zaak om de gemaakte afwegingen in kaart te brengen. In tegenstelling tot de verwachtingen vooraf bleek echter dat met een vordering slechts in zeer uitzonderlijke gevallen een ingewikkelder afweging gemoeid was. Ten aanzien van de 31 bestudeerde dossiers was daarvan in het geheel geen sprake. Om die reden is er dan ook van afgezien om individuele gegevensvragers en -verstrekkers specifiek over de geanalyseerde dossiers te bevragen.

1.3.3 Interviews

Gegeven de hiervoor beschreven praktische problemen, maar niet in de laatste plaats ook vanwege de bevinding dat de Wbvg anders functioneerde dan vooraf was gedacht, is de nadruk van het empirische onderzoek sterker komen liggen op persoonlijke interviews met gegevensvragers en -verstrekkers. In totaal zijn (telefonische) gesprekken gevoerd met 21 respondenten namens gegevensvragers en met 16 personen namens gegevenshouders.

In eerste instantie was voorgenomen de interviews met gegevensvragers te houden binnen de geselecteerde parketten, politieregio's en bij de FIOD. Vanwege de tussentijdse uitkomsten van het empirische onderzoek hebben wij deze inperking laten vervallen. In plaats daarvan is ervoor gekozen de gesprekken te verbreden naar andere arrondissementen, politieregio's en BOD'en met als belangrijkste doel in kaart te brengen of de uitkomsten met betrekking tot de oorspronkelijk gekozen locaties ook algemeen op Nederland van toepassing waren.

De gesprekken zijn gevoerd aan de hand van een globaal gesprekprotocol. De gestelde vragen hadden betrekking op de mate waarin de gesprekpartner van de verschillende onderdelen van de Wbvg gebruikmaakt, op de procedure die binnen de eigen organisatie wordt gevolgd bij het vorderen van gegevens,

op de hanteerbaarheid van de wet, en uiteraard ook op de aandachtspunten en knelpunten.

Er is gesproken met zes politiefunctionarissen (werkzaam op recherche-afdelingen) die werkzaam zijn in de politiekorpsen Zeeland, Brabant-Noord, Brabant Zuid-Oost, Midden- en West Brabant en Limburg-Zuid. Tevens zijn (telefonische) interviews gehouden met vijf opsporingsmedewerkers van de FIOD en met twee leidinggevenden van deze dienst. Daarnaast zijn op het niveau van het openbaar ministerie tien officieren van justitie en parketsecretarissen geïnterviewd, werkzaam op de arrondissementsparketten Amsterdam, Groningen, Den Bosch en Rotterdam. Voorts waren twee respondenten werkzaam bij het FP en twee anderen bij het LP.

Om inzicht te krijgen in de mate waarin de doelstellingen van de Wbvg zijn bereikt en om antwoord te krijgen op de vraag of de wet de geconstateerde knelpunten bij het vorderen van gegevens voor opsporingsdoeleinden heeft verholpen, dan wel dat er nieuwe knelpunten zijn ontstaan, zijn ook (telefonische) interviews gehouden met gegevenshouders. Daarbij ging het om bedrijven, instellingen of individuen die (regelmatig) te maken krijgen met Wbvg-vorderingen. Het be-trof vertegenwoordigers van ABN Amro, Ars T&TT (een onafhankelijke leverancier van innovatieve technologische oplossingen voor de markt van verkeer en vervoer), Beta Nederland (de belangenvereniging van exploitanten van benzinestations), BOVAG, Equens (verantwoordelijk voor de verwerking van girale en aan pintransacties en creditcards gerelateerde betalingen), Holland Casino, de ING bank, de Koninklijke Horeca Nederland, de Nederlandse Spoorwegen, de Nederlandse Vereniging van Banken, de Rabobank, de SNS Bank, TNT Post en UVIT verzekeraars. Tot slot zijn enkele exploitanten van benzinestations afzonderlijk geïnterviewd. De gevoerde gesprekken hadden een soortgelijk karakter als de interviews met gegevensvragers, maar uiteraard werden de vragen daarbij gesteld vanuit het perspectief van de verstrekkers.

1.4 Leeswijzer

Deze studie valt uiteen in twee delen en omvat een juridische en een empirische analyse van de Wbvg.

Het eerste deel van dit rapport bestrijkt de hoofdstukken 2 tot en met 4. Hoofdstuk 2 beschrijft de totstandkoming van de wet, waarbij de werkzaamheden van de Commissie Mevis, respectievelijk de parlementaire behandeling van de wet, centraal staan. Hoofdstuk 3 gaat in op de inhoud van de Wbvg en beschrijft de verschillenart. in het Wetboek van Strafvordering die op de wet betrekking hebben. In hoofdstuk 4 is het centrale onderwerp een analyse van de

verhouding van de Wbvg tot andere bevoegdheden die opsporingsinstanties kunnen toepassen om gegevens te verkrijgen van private partijen.

Het empirische deel van deze studie omvat de hoofdstukken 5 tot en met 8. In hoofdstuk 5 wordt allereerst gestart met een meer algemene beschrijving van het opsporingsproces en de rol die het vorderen van gegevens daarin speelt. Dit hoofdstuk biedt de lezer een kader om de daarna gepresenteerde empirische bevindingen in hun context te kunnen plaatsen. In hoofdstuk 6 wordt ingegaan op de cijfermatige en organisatorische aspecten van de Wbvg. Het gaat daarbij enerzijds om de vragen hoe vaak gegevens worden gevorderd, van wie of van welke organisatie, en om welke reden. Daarnaast wordt ingegaan op de procedures die de betrokken overheidsinstanties toepassen bij het vorderen van gegevens. In de hoofdstukken 7 en 8 komt het praktische functioneren van de Wbvg aan de orde vanuit het perspectief van de gegevensvragers, respectievelijk vanuit het gezichtspunt van de gegevensverstrekkers.

Hoofdstuk 9 besluit dit rapport. In dit hoofdstuk worden de onderzoeksvragen beantwoord en een aantal afsluitende observaties gepresenteerd.

2 De totstandkoming van de Wbvg

2.1 Inleiding

In dit hoofdstuk komt kort de totstandkoming van de wet aan bod. De Commissie Mevis speelde daarbij een hoofdrol. Navolgend worden zowel het rapport van de commissie als het door de commissie geschreven conceptwetsvoorstel en het bijbehorende kabinetsstandpunt besproken.

2.2 De Commissie Mevis

In mei 2001 overhandigt de Commissie Strafvorderlijke gegevensvergaring in de informatiemaatschappij (hierna naar haar voorzitter te noemen 'de Commissie Mevis') haar rapport aan de minister van Justitie.[8] De commissie was in maart 2000 ingesteld als gevolg van de in de strafvorderlijke praktijk ontstane problemen met betrekking tot de vergaring van gegevens ten behoeve van de opsporing en de vervolging van strafbare feiten. De commissie kreeg als taak te onderzoeken of het Wetboek van Strafvordering, gelet op de ontwikkelingen op het gebied van de informatie- en communicatietechnologie, voorzag in een toereikend wettelijk kader voor die vormen van gegevensvergaring die voor de strafvordering noodzakelijk zijn.[9]

2.2.1 De knelpunten in de toenmalige praktijk

Een eerste probleem dat de commissie signaleerde, was de fragmentarische regeling van de bevoegdheden die aangewend konden worden om gegevens te verkrijgen ter opsporing van strafbare feiten. De bevoegdheden waren zowel in het WvSv als in bijzondere regelingen terug te vinden.[10] Dit leverde hoofdzakelijk twee knelpunten op.

De eerste centrale kwestie was enerzijds dat de bevoegdheden in het WvSv slechts een beperkt deel van de praktische strafvorderlijke gegevensvergaring dekten. Anderzijds waren de algemeen geformuleerde bevoegdheden uit

---

8 Rapport Commissie Mevis 2001.

9 Zie o.a. art. 2 Regeling commissie strafvorderlijke gegevensvergaring in de informatiemaatschappij (*Stcrt*. 2000, nr. 55 en Rapport Commissie Mevis 2001, p. 2 en 14).

10 Voorbeelden van bijzondere regelingen zijn de Wet op de Economische Delicten (o.a. art. 18 en 19 WED) en de Algemene wet inzake rijksbelastingen (o.a. art. 81 Awr).

de bijzondere regelingen slechts van toepassing op bepaalde typen strafbare feiten.[11] Het gebrek aan een uniforme wettelijke regeling leidde tot onduidelijkheid en rechtsonzekerheid, niet alleen bij de met opsporing belaste instanties maar ook bij de derde die over de gegevens beschikte.[12]

Als tweede knelpunt voerde de commissie aan dat de wettelijke bevoegdheden niet toereikend waren wanneer bepaalde gegevens van derden voor het strafvorderlijk onderzoek noodzakelijk waren. De houders van de gegevens werd dan verzocht deze op vrijwillige basis te verstrekken. Uit het onderzoek van de commissie bleek dat de bereidheid daartoe over het algemeen aanwezig was, maar dat daar voor alle betrokken partijen wel haken en ogen aan zaten.
Zo diende de houder van de gegevens op grond van art. 43 Wet bescherming persoonsgegevens (Wbp) te beoordelen of sprake was van een dwingende en gewichtige reden die maakte dat de vrijwillige verstrekking van gegevens noodzakelijk was. Aangezien deze derde vaak niet op de hoogte was van de feiten en omstandigheden die de achtergrond vormden van het verzoek tot verstrekking van de gegevens, was het maken van een dergelijke afweging uiterst lastig. Daar kwam nog bij dat houders van gegevens in het kader van de vrijwillige medewerking verantwoordelijk en aansprakelijk waren voor de gegevensverstrekking omdat er geen wettelijke regeling bestond op grond waarvan zij verplicht waren mee te werken aan een verzoek tot verstrekking van gegevens.[13]

Voor degenen over wie informatie werd verstrekt, betekende dit dat de behartiging van hun belangen in handen van de gegevenshouders lag, die echter door een gebrek aan informatie moeilijk tot een juiste belangenafweging konden komen. Zij konden de houders van de gegevens bovendien slechts achteraf aanspreken op de gemaakte belangenafweging en ter verantwoording roepen.

Omgekeerd was de situatie ook voor de met opsporing belaste instanties niet ideaal, daar zij afhankelijk waren van de bereidheid van de gegevenshouders om mee te werken aan de verstrekking van gegevens. Voorts moesten die, om een deugdelijke belangenafweging te kunnen maken, worden gekend in vertrouwelijke onderzoeksgegevens die de opsporingsinstanties logischerwijs niet openbaar wilden maken.[14] Indien een gegevenshouder weigerde aan een verzoek tot verstrekking van gegevens te voldoen waren de opsporingsinstanties soms genoodzaakt over te gaan tot een zwaarder dwangmiddel: de doorzoeking ter vastlegging van gegevens.[15]

---

11 Rapport Commissie Mevis 2001, p. 44.
12 Jongeneel-van Amerongen 2005, p. 954.
13 Rapport Commissie Mevis 2001, p. 44.
14 Jongeneel-van Amerongen 2005, p. 954.
15 Rapport Commissie Mevis 2001, p. 44.

2.2.2 Het standpunt van de Commissie Mevis

In haar rapport kwam de Commissie Mevis tot de conclusie dat het Wetboek van Strafvordering aanpassing behoefde en zij gaf daartoe een aanzet in de vorm van een conceptwetsvoorstel. De commissie was van mening dat er een nieuwe regeling in het Wetboek van Strafvordering diende te komen, specifiek met betrekking tot het vorderen van gegevens. Deze nieuwe regeling zou moeten voorzien in precies omschreven bevoegdheden en aldus een einde dienen te maken aan de bestaande onduidelijkheden in de verantwoordelijkheden van justitie en van de gegevenshouder. Eén van de speerpunten van het voorstel van de commissie was dat de gegevenshouders niet langer gevraagd zou kunnen worden vrijwillig mee te werken aan de gegevensverstrekking, maar dat zij daartoe verplicht werden door middel van een vordering. De verplichting om daaraan te voldoen zorgde er voor dat de verantwoordelijkheid voor de gegevensvergaring geheel bij de opsporingsinstanties zou komen te liggen. Daarmee werden ook de belangen versterkt van degene over wie gegevens worden verstrekt.[16]

De commissie realiseerde zich dat de bevoegdheden als ingrijpend konden worden gezien omdat in beginsel elk gegeven in het kader van een opsporingsonderzoek zou kunnen worden gevorderd en de bevoegdheden het recht op bescherming van de persoonlijke levenssfeer zoals vervat in art. 10 van de Grondwet (GW) en art. 8 van het Europees Verdrag ter bescherming van de rechten van de mens (EVRM) zouden kunnen beperken. Het eerstgenoemde wetsartikel vereist voor een beperking van het grondrecht een basis in een wet in formele zin. Art. 8 EVRM acht een beperking op de bescherming van de persoonlijke levenssfeer slechts mogelijk voor zover deze 'bij wet is voorzien' en het 'in een democratische samenleving noodzakelijk is' in het belang van enkele met name genoemde doelen, waaronder het voorkomen van strafbare feiten. Onder dat doelcriterium is onder meer de opsporing van strafbare feiten begrepen.[17]

De voornoemde, door art. 8 EVRM gestelde eisen, werden mede ingevuld aan de hand van de door de commissie geconstateerde, hierboven genoemde knelpunten.[18] Bovendien is gegevensvergaring voor de strafvorderlijke praktijk onmisbaar. Dat maakte volgens de commissie het belang om gegevens te kunnen verkrijgen die zich bij derden bevinden dusdanig groot dat een nieuwe regeling, die niet langer gebaseerd was op vrijwillige verstrekking, noodzakelijk

---

16 Mevis 2002, p. 33.
17 Rapport Commissie Mevis 2001, p. 46.
18 Jongeneel-van Amerongen 2005, p. 955.

kon worden geacht. Dat belang was bovendien groter geworden omdat talrijke ontwikkelingen op het gebied van informatie- en communicatietechnologie ertoe leiden dat steeds meer gegevens beschikbaar zijn bij bedrijven en instellingen, bijvoorbeeld over de personen die hun diensten of producten afnemen, en dat deze gegevens vaak alleen nog in geautomatiseerde bestanden zijn opgeslagen. Het in beslag nemen van de dragers van geautomatiseerde gegevens is dus in veel gevallen disproportioneel, terwijl het motief om in beslag te nemen als oneigenlijk kan worden beschouwd. Immers, niet de informatiedrager, maar de gegevens zelf zijn van belang voor de strafvordering. Deze ontwikkelingen zorgden er voor dat er in de praktijk ook behoefte bestaat om geautomatiseerde gegevens te vorderen en wel in ruimere mate dan op basis van art. 125i (oud) Sv[19] mogelijk was.[20]

2.3 Het conceptwetsvoorstel van de Commissie Mevis

De Commissie Mevis vertaalde de bevoegdheden met betrekking tot het vorderen van gegevens in een conceptwetsvoorstel.[21] Zij werden door de commissie gekwalificeerd als bijzondere opsporingsbevoegdheden, kregen een plaats naast de al bestaande bevoegdheden tot inbeslagneming en dienden ter vervanging van art. 125i (oud) Sv.[22]

De voorgestelde regeling van bevoegdheden kent een indeling in categorieën naar de aard van de gegevens. De commissie maakte grofweg een onderscheid tussen identificerende gegevens, andere dan identificerende gegevens en gevoelige gegevens. Binnen die indeling werd gekozen voor een stelsel van getrapte bevoegdheden. Naarmate de te vorderen gegevens naar hun aard een grotere inbreuk maken op de persoonlijke levenssfeer, werd het aantal gevallen waarin gegevens gevorderd kunnen worden beperkt en diende een andere autoriteit de desbetreffende gegevens te vorderen. Op eenzelfde wijze is ook rekening gehouden met de gegevenshouder. Naarmate die handelingen moet verrichten die verder af liggen van het doel waarmee hij gegevens in het kader van zijn normale activiteiten verwerkt, is de regeling aan zwaardere voorwaarden gebonden.[23]

---

19 Art. 125i (oud) Sv regelt de bevoegdheid van de rechter-commissaris om te vorderen dat gegevens uit een geautomatiseerd werk worden verstrekt.

20 Rapport Commissie Mevis 2001, p. 44.

21 Voor het conceptwetsvoorstel van de Commissie Mevis zie hoofdstuk 11 van haar rapport, p. 100 e.v.

22 Rapport Commissie Mevis 2001, p. 44.

23 Rapport Commissie Mevis 2001, p. 54.

Wat betreft de autoriteit die de gegevens mag vorderen, stelde de commissie het volgende voor. Allereerst zou de opsporingsambtenaar de bevoegdheid krijgen om identificerende gegevens te vorderen. In de tweede plaats diende aan de officier van justitie de bevoegdheid toe te komen om (al dan niet na voorafgaande machtiging van de rechter-commissaris) andere dan identificerende gegevens (zowel historische als toekomstige) en gevoelige gegevens te vorderen. Daarnaast zou de officier van justitie bevoegd worden medewerking te vorderen aan het ontsleutelen van versleutelde gegevens en stelde de commissie voor hem de bevoegdheid te geven, na voorafgaande machtiging van de rechter-commissaris, te vorderen dat de gegevens kunnen worden bewerkt.

Tot slot omvatte het conceptwetsvoorstel de bevoegdheid van de hulpofficier van justitie om te vorderen dat gegevens gedurende veertien dagen toegankelijk blijven (bevriezing). De bevoegdheid tot doorzoeking ter vastlegging van gegevens werd in het voorstel van de commissie, in het nieuw voorgestelde art. 125i Sv, toegekend aan de opsporingsambtenaar, de (hulp)officier van justitie en de rechter-commissaris, afhankelijk van het te doorzoeken object.[24]

Het conceptwetsvoorstel voorzag ook in flankerende voorzieningen zoals een vergoeding voor de kosten die een gegevenshouder maakt om aan de vordering te voldoen en de mogelijkheid van de officier van justitie om geheimhouding op te leggen aan de gegevensverstrekker. Daarnaast waren onder meer een beklagrecht en een notificatieplicht opgenomen.[25]

2.4 Het standpunt van het kabinet

Het kabinet deelde het standpunt van de Commissie Mevis dat, gelet op de geschetste ontwikkelingen en knelpunten, de gegevensvergaring voor de opsporing van strafbare feiten een zelfstandige regeling in het Wetboek van Strafvordering vroeg.[26] Op hoofdlijnen nam het kabinet de voorgestelde regeling van de commissie dan ook over. Op enkele punten besloot de regering echter af te wijken van het conceptwetsvoorstel.

Zo meende het kabinet dat duidelijker moest worden gedefinieerd van welke partijen identificerende en toekomstige gegevens gevorderd zouden kunnen worden. Aan de voorgestelde formulering ‘degene die daar redelijkerwijs voor in aanmerking komt’, diende volgens het kabinet te worden toegevoegd ‘en die anders dan ten behoeve van persoonlijk gebruik gegevens verwerkt’. Uitge-

---

24 Rapport Commissie Mevis 2001, p. 72.
25 Rapport Commissie Mevis 2001, p. 83.
26 *Kamerstukken II* 2001/02, 28 366, nr. 1, p. 1.

sloten moest worden dat van iemand die uitsluitend persoonlijke contacten onderhoudt met de persoon op wie het onderzoek zich richt, gevorderd zou kunnen worden identificerende of toekomstige gegevens te verstrekken. Juist het vorderen van gegevens in de sfeer van persoonlijke contacten kon volgens het kabinet de indruk wekken dat het bij deze bevoegdheid om een soort informatieplicht zou gaan en dat kon als ingrijpend voor de persoonlijke levenssfeer worden gezien. Overigens ligt het belang voor de opsporingspraktijk vooral bij de gegevens bij bedrijven en instellingen.[27]

Daarnaast meende het kabinet dat de bevoegdheid tot het vorderen van identificerende gegevens, vanwege de proportionaliteit, over het algemeen slechts moest kunnen worden toegepast in het kader van 'verdenking van een misdrijf' in plaats van het door de commissie voorgestelde ruimere criterium 'verdenking van een strafbaar feit'.[28] Verder diende, in tegenstelling tot de opvatting van de Commissie Mevis, niet expliciet in de formulering van de bevoegdheid te worden vastgelegd dat antwoord gegeven zou moeten worden op een zogenoemde ja/nee-vraag: de vraag of identificerende gegevens over een persoon beschikbaar zijn. De verplichting hierop te antwoorden vloeide volgens het kabinet al voort uit de bevoegdheid de identificerende gegevens zelf te vorderen en deze beschikbaar te laten stellen.[29]

Voorts diende volgens het kabinet te worden afgezien van het toekennen van de bevoegdheid tot het vorderen van identificerende gegevens in het kader van een verkennend onderzoek als bedoeld in art. 126gg Sv. Reden hiervoor was het gebrek aan duidelijkheid omtrent de vraag of er binnen het toenmalige verkennend onderzoek voldoende mogelijkheden bestonden tot het bijeenbrengen van gegevens. Alvorens tot toekenning van de bevoegdheden over te gaan was derhalve een scherpere afbakening van het verkennend onderzoek nodig.[30]

Ook wat betreft de bevoegdheid tot het vorderen van een bewerking van gegevens stelde het kabinet een afwijkend kader voor. Erkend werd dat het be-

---

27 *Kamerstukken II* 2001/02, 28 366, nr. 1, p. 4, 12, 18, 31 en *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 7-8.

28 *Kamerstukken II* 2001/02, 28 366, nr. 1, p. 13. Er dient te worden opgemerkt dat in de uiteindelijke wettelijke regeling is afgeweken van dit kabinetsstandpunt aangezien het op basis van art. 126nd lid 6 Sv mogelijk is om in het geval van verdenking van een overtreding identificerende gegevens te vorderen. Dit betreft echter een uitzondering waarvoor een machtiging van de rechter-commissaris is vereist.

29 *Kamerstukken II* 2001/02, 28 366, nr. 1, p. 14.

30 *Kamerstukken II* 2001/02, 28 366, nr. 1, p. 13 en 14. Inmiddels is in art. 126ii Sv, art. 126nc lid 2-7 Sv van toepassing verklaard op het verkennend onderzoek van art. 126gg Sv.

werken van gegevens waardevol is voor de opsporing. Hierdoor kunnen namelijk nieuwe gegevens naar voren komen die zonder bewerking niet zichtbaar zijn. Zo kan onverwachte informatie over personen beschikbaar komen. In het afwijkende kader was het uitgangspunt echter niet langer dat de houder van de gegevens de bewerking uitvoert, maar dat de opsporingsambtenaren dat voor hun rekening zouden nemen. Het kabinet achtte het gewenst dit onderdeel in een apart wetsvoorstel onder te brengen.[31]

Voor de voorgestelde bevoegdheid van de hulpofficier van justitie om bevriezing van geautomatiseerde gegevens te vorderen voor de duur van 14 dagen was door de Commissie Mevis aansluiting gezocht bij de implementatieverplichting die het Verdrag Crime in Cyberspace, hierna te noemen Cybercrime Verdrag, met zich meebrengt.[32] De bevoegdheid is toegekend aan de officier van justitie, waarbij de termijn is verlengd naar 90 dagen.[33] Echter, deze bevoegdheid is niet in het wetsvoorstel opgenomen aangezien dat gebeurd is in wetgeving ter implementatie van het verdrag *'Crime in Cyberspace'* (hierna Cybercrime Verdrag).[34]

Tot slot stelde het kabinet als aanvulling voor te bepalen dat de bevoegdheid tot het vorderen van identificerende gegevens slechts door de daartoe aangewezen en geautoriseerde opsporingsambtenaren kan worden toegepast en dat politie en het openbaar ministerie inzicht moeten verschaffen in het aantal malen dat de bevoegdheden worden toegepast, alsmede in de verdere verwerking van de gevorderde gegevens.[35]

Met de Wbvg beoogt de wetgever dus een regeling van heldere bevoegdheden te creëren in het WvSv voor het vorderen van gegevens, zodat gegevens ter beschikking kunnen komen in het belang van de opsporing van strafbare feiten.[36] De directe aanleiding waren de onduidelijkheid en de rechtsonzekerheid weg te nemen die op dat moment bestonden. Daarnaast beoogde de wetgever zo veel mogelijk een einde te maken aan de noodzaak tot vrijwillige medewerking door de derde die over gegevens beschikt.[37] Gegevenshouders zouden echter nog wel op eigen initiatief bijdragen moeten kunnen leveren aan de opsporing van strafbare feiten, door van bepaalde feiten of omstandigheden

---

31 *Kamerstukken II* 2001/02, 28 366, nr. 1, p. 20.

32 Verdrag Crime in Cyberspace, *Trb.* 2002, 18. De bepaling (art. 126ni Sv) is inmiddels ingevoerd bij wet van 1 juni 2006, *Stb*. 300 (Wet computercriminaliteit II).

33 *Kamerstukken II* 2001/02, 28 366, nr. 1, p. 21.

34 *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 16.

35 *Kamerstukken II* 2001/02, 28 366, nr. 1, p. 31.

36 Het niet voldoen aan een vordering met betrekking tot de Wbvg kan overtreding van art. 184 Sr opleveren.

37 *Kamerstukken II* 2004/05, 29 441, C, p. 2.

melding te doen aan de politie of op andere wijze informatie aan de politie te verstrekken.[38]

Betreft het persoonsgegevens die onder de Wbp vallen, dan dient art. 43 van die wet in acht genomen te worden. Aan de hand van de beginselen van proportionaliteit en subsidiariteit dient de derde af te wegen of verstrekking van de gegevens in een concreet geval noodzakelijk is voor een van de in art. 43 Wbp benoemde doelen, waaronder de voorkoming, opsporing of vervolging van strafbare feiten.[39] Belangrijk is derhalve dat, indien sprake is van vrijwilligheid, het initiatief om gegevens te verstrekken bij de derde dient te liggen. Indien de derde de gegevens weliswaar op vrijwillige basis verstrekt ten behoeve van het opsporingsonderzoek, maar hij doet zulks op verzoek van de opsporingsambtenaar of de officier van justitie, dan kan, sinds de Wbvg van kracht is geworden, sprake zijn van onrechtmatig verkregen bewijs, afhankelijk van de omstandigheden van het geval.[40] Vanzelfsprekend kan een derde ook aangifte doen van een strafbaar feit of als getuige een verklaring afleggen omtrent wat hij over het strafbare feit heeft waargenomen. Daarop heeft de Wbvg geen betrekking.

Door deze nieuwe regeling wordt derhalve meer recht gedaan aan de in het geding zijnde belangen: het belang van de opsporing, het belang van de derde van wie de gegevens gevorderd worden en het belang van degene op wie de gegevens betrekking hebben.[41]

Het definitieve wetsvoorstel tot wijziging van het Wetboek van Strafvordering en enkele andere wetten in verband met de regeling van bevoegdheden tot het vorderen van gegevens werd door de toenmalige minister van Justitie Donner in maart 2004 ingediend.[42] Na behandeling is de Wbvg op 1 januari 2006 in werking getreden.[43]

2.5 Besluit

In dit hoofdstuk is kort de ontstaansgeschiedenis van de Wbvg uiteengezet. De centrale doelstelling van de wet is een einde te maken aan de onduidelijkheid en rechtsonzekerheid die werd veroorzaakt door de ontoereikendheid van de op dat moment bestaande kaders voor het vorderen van gegevens van derden. De wet is

---

38 *Kamerstukken I* 2004/05, 29 441, C, p. 3.
39 *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 2.
40 Zie *Kamerstukken I* 2004/05, 29 441, C, p. 3.
41 Zie o.a. *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 2 en 3 en *Kamerstukken I,* 2009/10, 29 441, G, p. 1.
42 *Kamerstukken II* 2001/02, 28 366, nr. 1, p. 31.
43 Wet bevoegdheden vorderen gegevens van 16 juli 2005, *Stb.* 2005, 390.

op 1 januari 2006 in werking getreden. Aan de Wbvg ligt het rapport van de Commissie Mevis ten grondslag. De commissie heeft verschillende knelpunten in de toenmalige praktijk geconstateerd. Het belangrijkste probleem is dat het systeem gebaseerd was op vrijwillige medewerking van de houder van de gegevens. De commissie heeft de benodigde aanpassingen neergelegd in een conceptwetsvoorstel. Het kabinet deelde het standpunt van de Commissie Mevis dat de gegevensvergaring voor de opsporing van strafbare feiten een zelfstandige regeling in het WvSv behoeft. Op hoofdlijnen nam het kabinet de voorgestelde regeling van de commissie over, op enkele punten zijn veranderingen doorgevoerd. Zo zijn onder meer de voorgestelde regeling rondom de bevoegdheid om bevriezing van geautomatiseerde gegevens te vorderen en de bevoegdheid om bewerking van gegevens te vorderen niet in het uiteindelijke wetsvoorstel opgenomen.

3 De inhoud van de Wbvg

3.1 Inleiding

In dit hoofdstuk komt de inhoud van de Wbvg aan de orde. Daarbij gaat het om de aard en de reikwijdte van de bevoegdheden, zoals die zijn onder te verdelen in bevoegdheden met betrekking tot het vorderen van identificerende gegevens; andere dan identificerende gegevens (zowel historische als toekomstige); gevoelige gegevens; het ontsleutelen van versleutelde gegevens en het doorzoeken ter vastlegging van gegevens. De wetsartikelen die op deze verschillende bevoegdheden betrekking hebben, worden in achtereenvolgende paragrafen besproken (3.3 tot en met 3.8). Allereerst zal echter in meer algemene zin worden ingegaan op de systematiek van de Wbvg (paragraaf 3.2). Paragraaf 3.9 besluit dit hoofdstuk met een beknopte samenvatting van de bevindingen.

3.2 De systematiek van de toedeling van bevoegdheden in de Wbvg

In de Wbvg zijn dwangmiddelen opgenomen die derden kunnen verplichten bepaalde opgeslagen of vastgelegde gegevens te verstrekken. Daarbij is sprake van twee afzonderlijke stelsels. Het eerste is neergelegd in de titel rondom de bijzondere bevoegdheden tot opsporing (titel IVa) en betreft art. 126nc-126nh Sv. Het tweede stelsel is terug te vinden in titel V (bijzondere bevoegdheden tot opsporing voor het onderzoek naar het beramen of plegen van ernstige misdrijven in georganiseerd verband) en betreft art. 126uc-126uh Sv. Hoewel het toepassingsbereik per stelsel verschilt, zijn ze qua inhoud vrijwel gelijk.[44] Ook art. 125i-125o Sv uit titel IV (enige bijzondere dwangmiddelen) behoren tot de bevoegdheden uit de Wbvg.

Zoals voorgesteld door de Commissie Mevis bevat de Wbvg een driedeling in bevoegdheden naar de aard van de gegevens: identificerende gegevens, andere dan identificerende gegevens en gevoelige gegevens. Daarnaast kent de wet een getrapt stelsel van bevoegdheden: al naar gelang de categorie gegevens ingrijpender is voor de persoonlijke levenssfeer en/of naarmate meer handelingen van een derde worden gevraagd, gelden zwaardere voorwaarden voor toepassing. Daarnaast kent de wet de bevoegdheid tot het vorderen medewerking te

---

[44] Mac Gillavry 2006.

verlenen aan het ontsleutelen van versleutelde gegevens en de doorzoeking ter vastlegging van gegevens.[45]

Voor alle bevoegdheden geldt dat de vordering om de gegevens te verstrekken schriftelijk dient te geschieden en dat er een proces-verbaal dient te worden opgemaakt. Daarnaast kunnen de bevoegdheden niet worden aangewend tegen een verdachte en is een verschoningsgerechtigde niet verplicht mee te werken aan een vordering tot gegevensverstrekking. De bevoegdheden kunnen ook worden gebruikt om gegevens te vergaren over andere personen dan de verdachte indien dat in het belang is van het opsporingsonderzoek.[46] Waar in de wettekst gesproken wordt over 'in het belang van het onderzoek' wordt bedoeld dat het moet gaan om het (kunnen) nemen van strafvorderlijke beslissingen.[47]

Indien van een derde partij gegevens worden gevorderd over een persoon is diegene doorgaans niet van de vordering op de hoogte. Daarom is in art. 126bb lid 1 Sv een notificatieregeling opgenomen die geldt voor de bevoegdheden van de titels IVa tot en met Vc van boek 1 van het WvSv. Hieronder vallen ook de bevoegdheden tot het vorderen van gegevens als bedoeld in de art. 126nc-126nh en 126uc-126uh Sv. Dat betekent dat, zodra het belang van het onderzoek dat toelaat, aan de betrokkene schriftelijk mededeling wordt gedaan van de uitoefening van de bevoegdheden. In art. 126bb lid 4 Sv zijn identificerende gegevens (art. 126nc en 126uc Sv), gezien de beperkte inbreuk van de bevoegdheid, uitgesloten van de notificatieregeling. De ratio van de regeling is dat de betrokkene in de gelegenheid wordt gesteld een rechtsmiddel aan te wenden tegen een mogelijke inbreuk op zijn persoonlijke levenssfeer.[48]

Gekoppeld aan de notificatieregeling kent art. 126bb Sv in lid 5 een geheimhoudingsplicht. Degene tot wie een vordering als bedoeld in onder meer art. 126nc-126nh en 126uc-126uh Sv is gericht, neemt in het belang van het onderzoek geheimhouding in acht omtrent al hetgeen hem ter zake van de vordering bekend is.

De Wbvg voorziet niet in een mogelijkheid om vooraf tegen de vordering beklag te doen. Het is immers niet gebruikelijk dat de toepassing van op-

---

45 Jongeneel-van Amerongen 2005, p. 955.

46 Hieronder vallen onder meer gegevens van het slachtoffer of van derden met wie de verdachte contacten heeft onderhouden en die kunnen bijdragen aan het opsporingsonderzoek. Hierbij gelden dezelfde wettelijke vereisten als bij het vorderen van gegevens over de verdachte met dien verstande dat uit de wetsgeschiedenis kan worden afgeleid dat met het oog op het proportionaliteitsbeginsel grote terughoudendheid geboden is bij het vorderen van gegevens over andere personen dan de verdachte. Zie *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 6.

47 *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 23.

48 Mac Gillavry 2006, 'aant. 22 op art. 126nc'.

sporingsbevoegdheden aan de rechter kan worden voorgelegd voordat deze worden uitgeoefend. Beklag is echter achteraf mogelijk op grond van art. 552a Sv.[49] Beklag heeft geen schorsende werking en staat open voor de belanghebbende. Gezien de wetsgeschiedenis betreft het daarbij zowel de derde van wie de gegevens worden gevorderd, als degene op wie de gegevens betrekking hebben.[50] Wordt de belanghebbende in het gelijk gesteld dan kan de rechter bepalen dat de gevorderde gegevens niet (meer) door de opsporingsinstanties gebruikt mogen worden en door hen dienen te worden vernietigd.[51] Als geen tijdige behandeling door de rechter gerealiseerd kan worden, staat in geval van een spoedeisend belang in beginsel de weg van de voorlopige voorziening open.[52] Hierna zullen de afzonderlijke bevoegdheden nader worden beschouwd. Voor een schematisch overzicht van de verschillende bevoegdheden verwijzen wij de lezer naar bijlage 1.

3.3 Identificerende gegevens

Op basis van art. 126nc en 126uc Sv kunnen bepaalde opgeslagen of vastgelegde identificerende gegevens worden gevorderd van een derde. Onder gegevens wordt volgens de Memorie van Toelichting (hierna verder: MvT) verstaan: informatie die is vastgelegd of opgeslagen op een gegevensdrager, hetzij op schrift, hetzij in elektronische vorm. Met de toevoeging 'opgeslagen of vastgelegd' is beoogd duidelijk te maken dat de gegevens historisch moeten zijn. De gegevens moeten op het moment van de vordering al door de derde zijn verwerkt. Met opgeslagen gegevens wordt informatie in een geautomatiseerd werk bedoeld, terwijl vastgelegde gegevens op een andere wijze zijn geregistreerd, bijvoorbeeld op papier.[53]

De gegevens waar het hier om gaat, zijn volgens art. 126nc lid 2 Sv naam, adres, woonplaats en postadres, geboortedatum en geslacht en administratieve kenmerken. In geval van een rechtspersoon kunnen bovendien naam, adres, postadres, rechtsvorm, vestigingsplaats en administratieve kenmerken worden gevorderd. Administratieve kenmerken zijn 'kenmerken die de relatie

---

49 Zie o.a. Rb. Zutphen 20 november 2007, *LJN* BB8606 en Rb. Den Haag 17 juni 2008, *LJN* BH2222.

50 *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 27.

51 *Kamerstukken II* 2003/04, 29 441, nr. 6, p. 23 en *Kamerstukken I,* 2004/05, 29 441, C, p. 7.

52 Zie o.a. *Kamerstukken II* 2003/04, 29 441, nr. 8, Van de Griend 2002, Groenhuijsen en Knigge 2004.

53 *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 7 en 23.

tussen de persoon die onderwerp is van onderzoek en de derde van wie de gegevens worden gevorderd aanduiden, dan wel de kenmerken van de diensten die de derde aan de persoon verleent'.[54] Gegevens die daar onder vallen, zijn onder andere een klantnummer, een polisnummer en een bankrekeningnummer. In lid 3 van art. 126nc Sv wordt nog expliciet vermeld dat de vordering geen betrekking kan hebben op gevoelige gegevens, zoals informatie over iemands godsdienst.[55]

De categorie identificerende gegevens is gelimiteerd door het feit dat de vordering en verstrekking in beginsel slechts in geringe mate inbreuk mogen maken op de persoonlijke levenssfeer. Daarnaast is het voldoen aan de vordering van deze gegevens voor de derde niet zeer belastend, terwijl de behoefte aan identificerende gegevens in de strafvordering groot is. Vooral bij de start van een opsporingsonderzoek spelen deze doorgaans een grote rol. Dit type gegevens kan er bijvoorbeeld toe leiden dat vastgesteld kan worden wie de personen zijn tot wie het opsporingsonderzoek zich richt en tot het zichtbaar maken van verbanden tussen situaties en personen.

Tegen deze achtergrond worden aan deze bevoegdheid geen zware voorwaarden gesteld.[56] Identificerende gegevens kunnen dan ook gevorderd worden in het kader van de opsporing van elk misdrijf, dan wel in geval van verdenking dat in georganiseerd verband misdrijven worden beraamd of gepleegd die, gezien hun aard of de samenhang met andere misdrijven die in dat georganiseerde verband worden beraamd of gepleegd, een ernstige inbreuk op de rechtsorde vormen. Daarnaast is het mogelijk om in geval van verdenking van een overtreding identificerende gegevens te vorderen, nu art. 126nd lid 6 Sv spreekt over 'verdenking van een ander strafbaar feit dan bedoeld in art. 126nd lid 1 Sv'. Aangezien art. 126nd Sv mede de bevoegdheid van art. 126nc Sv omvat, betekent dit dat op grond van art. 126nd lid 6 Sv ook in het geval van verdenking van een overtreding identificerende gegevens gevorderd kunnen worden. Dit betreft echter een uitzondering die aan strenge eisen is gebonden: art.

---

54 *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 7.

55 Identificerende gegevens kunnen tevens gevoelige gegevens zijn. Vanwege het getrapte stelsel van bevoegdheden kunnen die niet verkregen worden op grond van art. 126nc en 126nd Sv (want expliciet uitgesloten) en indien het een gering strafbaar feit betreft ook niet op grond van art. 126nf Sv. Die gegevens zijn dan niet te vorderen. Vrijwillige medewerking is ook geen optie gezien het systeem van de wet. Zie Mac Gillavry 2006, 'aant. 8 op art. 126nc Sv'.

56 Jongeneel-van Amerongen 2005, p. 955. Voor de toepassing van de bevoegdheden bij financiële dienstverleners gelden afwijkende regels die zijn vastgelegd in de Aanwijzing gegevensverstrekking financiële dienstverleners, *Stcrt.* 2004, 95. Zie Mac Gillavry 2006.

126nd lid 6 Sv vermeldt dat in een dergelijk geval een machtiging van de rechter-commissaris is vereist.

Op basis van art. 126nc lid 1 Sv is de opsporingsambtenaar bevoegd de gegevens te vorderen in het belang van het onderzoek. Uit de MvT blijkt dat per politieregio opsporingsambtenaren zullen worden aangewezen die geautoriseerd zijn om identificerende gegevens te vorderen.[57]

De wetgever heeft in art. 126nc Sv nog een nadere beperking aangebracht met betrekking tot de gegevens die op basis van dit artikel worden gevorderd. Lid 1 spreekt namelijk over 'bepaalde' identificerende gegevens. Wat onder 'bepaalde' identificerende gegevens van een persoon moet worden verstaan, blijkt niet duidelijk uit de wetsgeschiedenis. Uit de toelichting op art. 126nd Sv, waarin de bevoegdheid tot het vorderen van andere dan identificerende gegevens is vastgelegd, valt echter af te leiden dat het doel van deze eis is dat de officier van justitie moet preciseren welke gegevens hij vordert. De benodigde gegevens moeten derhalve zo nauwkeurig mogelijk in kaart worden gebracht. Door de vordering te beperken tot bijvoorbeeld een bepaalde tijdsperiode, tot vluchten met een bepaalde bestemming of herkomst, of tot huurders van een bepaald type auto, wordt de bepaaldheid van de identificerende gegevens bereikt.[58] Aangenomen moet worden dat in het kader van art. 126nc Sv voorts gegevens omtrent een groep personen kunnen worden gevorderd. Dat is (zie paragraaf 3.4 hierna) immers ook mogelijk op basis van art. 126nd Sv.[59]

De bevoegdheid kan worden aangewend jegens degene die daarvoor redelijkerwijs in aanmerking komt en die anders dan ten behoeve van persoonlijk gebruik gegevens verwerkt. Met deze formulering wordt beoogd te voorkomen dat van de derde die slechts persoonlijke contacten onderhoudt met de persoon die onderwerp is van onderzoek ook gegevens zouden kunnen worden gevorderd. Dat zou als ingrijpend voor de persoonlijke levenssfeer kunnen worden ervaren.[60] Het komt er dus op neer dat de opsporingsambtenaar de bevoegdheid enkel kan aanwenden jegens degene die gegevens verwerkt binnen het kader van

---

57 *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 7.

58 Mac Gillavry 2006, 'aant. 15 op art. 126nc'.

59 Zie *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 8. Als voorbeeld wordt daar genoemd het geval waar op een vlucht van Amsterdam naar Panama in de bagage van een reiziger een pakket cocaïne is gevonden. Dan kan de vordering van de passagierslijst van die vlucht eraan bijdragen dat de persoon die de bagage meebracht, kan worden achterhaald. Een vordering, niet gericht op een op voorhand bepaalde persoon, is in dit geval gerechtvaardigd omdat er een aanknopingspunt is voor een opsporingsonderzoek: er is cocaïne gevonden en dus een vermoeden van een strafbaar feit.

60 *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 7-8 en Jongeneel-van Amerongen 2005, p. 955.

een functie of beroepsuitoefening. Dit sluit ook aan bij de praktijk: verzoeken om identificerende gegevens worden vooral gericht tot bedrijven en instellingen. De wetsgeschiedenis noemt in dit verband overheidsdiensten, verenigingen, professionele dienstverleners en instellingen die diensten verlenen op het terrein van bijvoorbeeld cultuur, sport en hobby, al dan niet op commerciële basis.[61]

Onder 'degene die daarvoor redelijkerwijs in aanmerking komt' wordt de persoon verstaan ten aanzien van wie de opsporingsambtenaar aanwijzingen heeft, hoe licht ook, die erop wijzen dat er een kans is dat hij gegevens heeft die betrekking hebben op degene die onderwerp is van onderzoek. Er hoeft dus geen op feiten en omstandigheden gegrond redelijk vermoeden te bestaan dat de gegevens daadwerkelijk aanwezig zullen zijn. De bevoegdheid mag daarentegen niet ongericht – bij wijze van *fishing expedition* – jegens derden worden gebruikt. Indien gezocht wordt naar de winkel waar een persoon een computer heeft gekocht of het bedrijf waar een auto is gehuurd, dient een beperking van het aantal te bevragen winkels of bedrijven te worden aangebracht. Bijvoorbeeld alleen winkels in de omgeving waar de persoon woont.

Tot slot kan deze bevoegdheid ook worden gebruikt om van de derde te vorderen of hij over gegevens over de betreffende persoon beschikt, de zogenoemde ja/nee-vragen.[62] Indien een opsporingsambtenaar bijvoorbeeld verwacht dat een postorderbedrijf een klant heeft op een bepaald adres dat in het onderzoek van belang is, kan aan de vermoedelijke houder van de informatie gevraagd worden of hij inderdaad over gegevens over de betreffende persoon beschikt. Indien het antwoord bevestigend is, kan worden overgegaan tot het vorderen van de identificerende gegevens.[63]

3.4 Andere dan identificerende gegevens (historisch)

Art. 126nd en 126ud Sv verlenen de bevoegdheid om ook andere dan identificerende gegevens te vorderen. Het gaat bijvoorbeeld om gegevens over diensten die verleend zijn, zoals de duur, de data, de plaats en de aard van de dienstverlening, of om rekening- en betalingsgegevens.[64] In lid 2 van art. 126nd Sv worden gevoelige gegevens wederom uitgezonderd.[65]

---

61 *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 7.
62 *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 20.
63 *Kamerstukken II* 2001/02, 28 366, nr. 1, p. 14 en *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 20.
64 *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 8.
65 Zie ook HR 3 maart 2009, *LJN* BG9218 waarin de HR overwoog dat uit de identiteitsgegevens van personen die zich voor enige vorm van medische hulp of informatie bij een

Ook andere dan identificerende gegevens kunnen, doorgaans indien het onderzoek verder gevorderd is, van groot belang zijn om zicht te krijgen op bepaalde gebeurtenissen en op het gedrag of het patroon van gedragingen van een bepaalde persoon. Bij dat laatste valt te denken aan zijn reisgedrag, de plaatsen waar hij verblijft, de duur van zijn verblijf, zijn financiële transacties of de lading van voertuigen waarbij hij betrokken is. In vergelijking met art. 126nc Sv blijkt dat de gegevens die op basis van art. 126nd Sv kunnen worden gevorderd in ruimere mate zien op de persoonlijke levenssfeer van de persoon op wie de gegevens betrekking hebben. Vanzelfsprekend zijn er dan ook zwaardere voorwaarden aan de uitoefening van deze bevoegdheid verbonden.[66]

Zo wordt de bevoegdheid toegekend aan de officier van justitie (en niet aan de 'gewone' opsporingsambtenaar). Die kan in geval van verdenking van een misdrijf als omschreven in art. 67 lid 1 Sv, dan wel in geval van verdenking dat in georganiseerd verband misdrijven worden beraamd of gepleegd die, gezien hun aard of de samenhang met andere misdrijven die in dat georganiseerde verband worden beraamd of gepleegd, een ernstige inbreuk maken op de rechtsorde, andere dan identificerende gegevens vorderen als dat in het belang van het onderzoek is.

Aangezien identificerende gegevens niet uitgezonderd worden, omvat art. 126nd Sv mede de lichtere bevoegdheid van art. 126nc Sv. Indien de officier van justitie zowel identificerende als andere dan identificerende gegevens wil vorderen, is hij niet gehouden twee vorderingen te doen, maar kan hij volstaan met een vordering op basis van art. 126nd Sv.[67] Dit heeft echter drie gevolgen.
Ten eerste spreekt art. 126nd Sv, in tegenstelling tot art. 126nc Sv, niet over 'de derde die anders dan ten behoeve van persoonlijk gebruik de gegevens verwerkt'. Dit leidt ertoe dat identificerende gegevens door de officier van justitie ook kunnen worden gevorderd van personen die voor persoonlijk gebruik gegevens verwerken, met andere woorden: van gewone burgers.[68]

Het tweede gevolg houdt verband met het feit dat de bevoegdheid van art. 126nd Sv kan worden toegepast jegens degene van wie redelijkerwijs kan worden vermoed dat hij toegang heeft tot bepaalde opgeslagen of vastgelegde gegevens. Het redelijke vermoeden dat bepaalde gegevens bij de derde beschikbaar zijn, moet gebaseerd zijn op concrete feiten of omstandigheden, zoals in-

---

ziekenhuis hebben gemeld, indirect informatie over de gezondheid van de betreffende personen kan worden afgeleid en dat zij daarom gegevens zijn betreffende de gezondheid in de zin van art. 126nd lid 2, derde volzin Sv.

66 *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 8.

67 *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 23.

68 Mac Gillavry 2006, 'aant. 4 op art. 126nd Sv'.

formatie die al naar voren is gekomen uit observaties of door toepassing van de bevoegdheid tot vordering van identificerende gegevens in het opsporingsonderzoek. Deze eis is zwaarder dan de eis die in art. 126nc Sv wordt gesteld, te weten dat de derde redelijkerwijs in aanmerking moet komen. Ontbreekt voldoende informatie om van een redelijk vermoeden te spreken, maar is er wel sprake van aanwijzingen dat de derde toegang zou kunnen hebben tot de gegevens van een bepaalde persoon, dan kan duidelijkheid verkregen worden door de bevoegdheid van art. 126nc Sv te gebruiken: het vorderen van identificerende gegevens.[69] Dan geldt, gezien het vereiste van art. 126nc Sv dat de derde de gegevens anders dan ten behoeve van persoonlijk gebruik moet verwerken, dat die vordering alleen gericht kan worden tot degene die uit hoofde van functie of beroep de gegevens verwerkt.[70] Dit vereiste geldt niet voor art. 126nd Sv waardoor andere dan identificerende gegevens in het kader van art. 126nd lid 1 Sv wel gevorderd worden van een derde die de gegevens verwerkt voor persoonlijk gebruik.[71]

Het derde gevolg vloeit voort uit art. 126nd lid 6 Sv. Dit artikel geeft aan dat ook bij verdenking van een ander strafbaar feit dan bedoeld in het eerste lid van art. 126nd Sv, de bevoegdheid van art. 126nd Sv kan worden toegepast. De officier van justitie dient dan wel over een voorafgaande schriftelijke machtiging van de rechter-commissaris te beschikken. Nu art. 126nd Sv mede de bevoegdheid van art. 126nc Sv omvat, betekent dit dat op grond van art. 126nd lid 6 Sv ook in het geval van verdenking van een overtreding identificerende en andere dan identificerende gegevens kunnen worden gevorderd. De MvT geeft aan dat toepassing van het zesde lid tot bijzondere gevallen beperkt dient te blijven.[72]

Evenals bij identificerende gegevens dient het bij andere dan identificerende gegevens te gaan om 'bepaalde' opgeslagen of vastgelegde gegevens. Dit duidt op de eis dat de officier van justitie vooraf de te vorderen gegevens zo nauwkeurig mogelijk moet omschrijven.[73] Hieronder valt bijvoorbeeld de vermelding van de persoon op wie de gevorderde gegevens betrekking hebben, en van welk aspect van diens handelingen. Aangezien de gegevens opgeslagen (in een geautomatiseerd werk) of vastgelegd (op andere wijze opgeslagen) moeten zijn, betreft de bevoegdheid van art. 126nd Sv slechts historische gegevens, dat wil zeggen: gegevens die op het moment van de vordering al door de derde zijn verwerkt.

---

69 *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 8.
70 Mac Gillavry 2006, 'aant. 4 op art. 126nd Sv'.
71 Mac Gillavry 2006, 'aant. 4 op art. 126nd Sv'.
72 *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 24.
73 *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 8.

Een verschil met art. 126nc Sv is dat het daar gaat om 'bepaalde opgeslagen of vastgelegde identificerende gegevens van een persoon' terwijl 'van een persoon' voor art. 126nd Sv geen toepassingsvereiste is. De verklaring daarvoor ligt in de omstandigheid dat identificerende gegevens altijd direct gerelateerd zijn aan een (rechts)persoon terwijl art. 126nd Sv betrekking kan hebben op alle opgeslagen of vastgelegde gegevens, met uitzondering van gevoelige gegevens. Ook gegevens over bijvoorbeeld het gebruik van voertuigen en bedrijfsgegevens vallen onder de reikwijdte van art. 126nd Sv. Dat sluit ook naadloos aan bij het eerdergenoemde doel van de bepaling: zicht krijgen op bepaalde gebeurtenissen of het in kaart brengen van het gedrag of patroon van gedragingen van een persoon.[74] Heeft de vordering geen betrekking op personen of ziet zij op een onbepaalde groep personen, dan dient deze gespecificeerd te worden door bijvoorbeeld te vermelden over welke periode gegevens worden gevorderd.[75] Indien de vordering niet gericht is op een op voorhand bepaalde persoon dan kan de vraag toch gerechtvaardigd zijn als er een (ander concreet) aanknopingspunt is voor het opsporingsonderzoek.[76]

3.5 Andere dan identificerende gegevens (toekomstig)

De wetgever heeft ook de mogelijkheid in het leven geroepen om andere dan identificerende gegevens die (eventueel) in de toekomst bij de gegevenshouder ter beschikking zullen komen, te vorderen. Het betreft gegevens die op het moment van de vordering nog niet door de derde zijn verwerkt. Wat betreft de term 'verwerken' wordt volgens de MvT aangesloten bij de betekenis van dezelfde term in de Wbp: elke handeling die, na het ontstaan van een gegeven, met het gegeven wordt verricht, zoals ontvangen, opslaan, vastleggen, vernietigen, bewerken en verstrekken.[77] De bevoegdheid heeft in beginsel betrekking op dezelfde gegevens als die op basis van art. 126nd Sv gevorderd kunnen worden

---

74 Mac Gillavry 2006, 'aant. 11 op art. 126nd'.

75 In de zaak die leidde tot Rb. Haarlem 13 oktober 2008, *LJN* BF8365 was bij de Criminele Inlichtingen Eenheid (CIE) informatie binnengekomen dat een persoon vermoedelijk verdovende middelen zou invoeren. De CIE heeft vluchtgegevens opgevraagd o.g.v. een door de OvJ afgegeven algemene vordering op grond van art. 126nd/ue Sv, zonder enige aanduiding van de persoon op wie de vordering betrekking had. Het betrof derhalve een 'blanco vordering'. Gevolg van een dergelijke vordering is dat de CIE beoordeelt of van de vordering gebruik wordt gemaakt zonder toetsing door de OvJ. Dat is volgens de rechtbank in strijd met de bedoeling van de wetgever. De informatie is gedeeltelijk onrechtmatig verkregen.

76 *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 23.

77 *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 25.

(historische gegevens). Het verschil is slechts het moment van de eerste verwerking van de gegevens in relatie tot het moment van de vordering.

De voorwaarden die gesteld worden aan het vorderen van andere dan identificerende gegevens die toekomstig zijn, zijn identiek aan de voorwaarden uit art. 126nd Sv. De bevoegdheid van art. 126ne en art. 126ue Sv is in het leven geroepen zodat voorkomen kan worden dat de officier van justitie een vordering tot het verstrekken van gegevens telkens moet herhalen, bijvoorbeeld indien de officier van justitie elke week gegevens wil vorderen van de afgelopen week.[78] Van belang is nog dat de officier van justitie in de vordering de termijn moet vermelden waarbinnen de gegevens worden verstrekt. Deze termijn kan langer zijn dan de periode die de derde normaal hanteert om gegevens te bewaren in het kader van zijn normale activiteiten. Gezien het feit dat de derde ook kan kiezen de gegevens direct te verstrekken kan feitelijk niet (altijd) gesproken worden van een bewaarplicht.[79] De periode waarover de vordering zich uitstrekt is, ingevolge art. 126ne lid 1 Sv maximaal vier weken en kan telkens met vier weken worden verlengd.

Gevorderd kan worden dat gegevens direct na de eerste verwerking ervan door de derde worden verstrekt, omdat dat in het belang van het opsporingsonderzoek kan zijn. Te denken valt aan een onderzoek naar gestolen pinpassen, waarbij het zeer aan de waarheidsvinding kan bijdragen als van de derde directe verstrekking kan worden gevorderd van gegevens omtrent wanneer, waar en op welke wijze een pasje wordt gebruikt. Deze bevoegdheid kan voor de derde extra belastend zijn. Hij moet namelijk constant in de gaten houden of dergelijke gegevens worden ontvangen en deze dan onmiddellijk verstrekken. Deze handelingen zullen voor een derde doorgaans ook verder verwijderd zijn van het doel waartoe hij gegevens verwerkt in het kader van zijn normale activiteiten. Derhalve is in art. 126ne lid 3 Sv bepaald dat deze mogelijkheid slechts openstaat indien het belang van het onderzoek dit dringend vordert. Daarnaast kan de officier van justitie slechts directe verstrekking vorderen na een machtiging van de rechter-commissaris. De rechter-commissaris zal toetsen of er sprake is van een dringend onderzoeksbelang en of er geen onevenredige inspanning wordt gevraagd van de betreffende derde. Vereist is dat de gevraagde handelingen binnen het bereik van de normale activiteiten van de derde liggen. Verder zal aandacht worden besteed aan de concrete omstandigheden van het geval, de te vorderen gegevens *an sich* en de ernst van het op te sporen misdrijf.[80]

---

78 *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 9.

79 Mac Gillavry 2006, 'aant. 12 op art. 126ne'.

80 Ter vergelijking wordt opgemerkt dat in het kader van het opnemen van telecommunicatie (ex art. 126m Sv) en het opnemen van vertrouwelijke communicatie (ex art. 126l Sv)

De vordering betreft, getuige de in lid 1 van art. 126ne Sv opgenomen terugverwijzing naar art. 126nd Sv, slechts vooraf bepaalde gegevens die op een later tijdstip toch al zouden worden verwerkt. Gegevens die normaliter niet verwerkt zouden worden, vallen dus buiten de bevoegdheid. Dat zorgt ervoor dat de bevoegdheid tot het vorderen van toekomstige gegevens vooral van betekenis is indien de derde van wie de gegevens gevorderd worden deze vanwege zijn reguliere activiteiten verwerkt. Alleen dan kan immers redelijkerwijs worden vermoed dat gegevens op een later tijdstip verwerkt zullen gaan worden. Daarom kan deze bevoegdheid slechts worden toegepast ten aanzien van de derde die anders dan ten behoeve van persoonlijk gebruik gegevens verwerkt.[81]

Volgens Mac Gillavry betekent dit dat er in beginsel sprake moet zijn van een reeds bestaande (dienstverlenings)relatie tussen de derde en degene die onderwerp is van onderzoek. Hij stelt dat juist dan denkbaar is dat op gezette tijden nieuwe gegevens van een persoon worden ontvangen en geeft daarbij het voorbeeld van een persoon die een betalingsrekening heeft bij een bank. Er zullen dan regelmatig bedragen op de rekening bijgeboekt en afgeboekt worden. Hoewel niet op voorhand valt te zeggen wanneer die transacties zullen plaatsvinden, is het ontstaan van toekomstige transactiegegevens zeer waarschijnlijk gezien de aard van de dienstverleningsrelatie.[82]

De bevoegdheid van art. 126ne Sv kan volgens Mac Gillavry echter niet worden gebruikt om in zijn algemeenheid een of meer dienstverleners de verplichting op te leggen gegevens te verzamelen en te verstrekken van een bepaalde nieuwe klant. Bijvoorbeeld in het geval een of meer banken wordt verzocht het openen van een rekening door persoon X (als nieuwe klant) onverwijld te melden of als een aantal autoverhuurbedrijven wordt gevraagd het huren van een auto door een bepaalde persoon te melden op grond van art. 126ne lid 3 Sv. Als de betreffende geadresseerde van de vordering nooit eerder met deze persoon te maken heeft gehad, is deze vordering onverenigbaar met het in de wetsgeschiedenis verwoorde uitgangspunt dat het bij toepassing van deze bevoegdheid gaat om 'het vorderen van vooraf bepaalde gegevens die op een later tijdstip toch al

een beoordelingskader voor de zittingsrechter bestaat. De zittingsrechter moet oordelen of de rechter-commissaris in redelijkheid tot zijn oordeel omtrent de machtiging heeft kunnen komen. Zie HR 11 oktober 2005, *NJ* 2006, 625, HR 21 november 2006, *LJN* AY9673 en recenter, HR 30 maart 2010, *NJ 2010*, 201. Het instellen van een dergelijk beoordelingskader bij de bevoegdheid tot directe verstrekking van toekomstige andere dan identificerende gegevens zou een extra rechterlijke waarborg kunnen opleveren.

81 *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 10.

82 Mac Gillavry 2006.

zouden worden verwerkt'. Dat laatste is immers niet vooraf waarschijnlijk, zo stelt Mac Gillavry.[83]

Een ander argument dat hij aanvoert, houdt verband met het feit dat art. 126ne Sv voortbouwt op art. 126nd Sv. In dat laatste artikel wordt een redelijk vermoeden vereist dat bepaalde gegevens bij de derde beschikbaar zijn, wat ervoor zorgt dat deze voorwaarde ook van toepassing is bij art. 126ne Sv. Dat redelijke vermoeden kan volgens de wetsgeschiedenis ontstaan zijn door informatie die reeds beschikbaar is in het opsporingsonderzoek, bijvoorbeeld door gegevens die aan het licht zijn gekomen door een observatie. Indien er geen relatie is tussen de derde en de persoon die onderwerp is van onderzoek kan er van een redelijk vermoeden dat de gegevens bij de derde beschikbaar (zullen) komen, geen sprake zijn.

De bevoegdheid om toekomstige andere dan identificerende gegevens te vorderen in de gevallen waarin geen relatie bestaat tussen de derde en de persoon die onderwerp is van onderzoek is in de opvatting van Mac Gillavry derhalve beperkt. Voor art. 126ne lid 3 Sv heeft dit tot gevolg dat dit artikel slechts gebruikt kan worden indien men in het opsporingsonderzoek aanwijzingen heeft gevonden dat verdachte bijvoorbeeld mogelijk een rekening zal openen bij een bepaalde bank of een auto zal huren bij een bepaald bedrijf.[84]

De opvatting van Mac Gillavry laat zich als volgt samenvatten: er dient in beginsel sprake te zijn van een al bestaande (dienstverlenings)relatie tussen de derde en degene die onderwerp is van onderzoek alvorens men de bevoegdheid van art. 126ne Sv kan gebruiken. Indien een dergelijke relatie ontbreekt, is de toepassing van art. 126ne Sv beperkt, aangezien dan niet waarschijnlijk is dat de gegevens vooraf bepaald kunnen worden en op een later tijdstip zullen worden verwerkt. Daarnaast kan er van een redelijk vermoeden dat de gegevens bij de derde beschikbaar (zullen) komen, geen sprake zijn. Deze opvatting is in lijn met het feit dat de wetgever als het gaat om het vorderen van gegevens van derden *fishing expeditions* wil voorkomen en daardoor beperkingen stelt aan het aantal te bevragen gegevenshouders, uiteraard ook als het toekomstige gegevens betreft.

Desondanks kunnen er vraagtekens worden gezet bij de steekhoudendheid van deze opvatting. Uitgaande van een systeem van bevoegdheidstoedeling is namelijk niet ondubbelzinnig uit de wettekst af te leiden dat ten aanzien van art. 126ne Sv een reeds bestaande (dienstverlenings)relatie wordt vereist. Daarnaast is het de vraag of de beperking die Mac Gillavry stelt aan de toepassing

---

83 Mac Gillavry 2006.
84 Mac Gillavry 2006.

van art. 126ne Sv in het geval er geen bestaande relatie is tussen de derde en degene die onderwerp is van onderzoek niet te strikt is. De eis dat het slechts vooraf bepaalde gegevens mogen zijn die op een later tijdstip toch al zouden worden verwerkt, heeft met name betrekking op het feit dat het geen gegevens mogen zijn die normaliter niet verwerkt zouden worden. Het kunnen dus geen gegevens zijn die een derde vanwege zijn reguliere activiteiten niet verwerkt. Daarom kan deze bevoegdheid slechts toegepast worden ten aanzien van de derde die anders dan ten behoeve van persoonlijk gebruik gegevens verwerkt.[85] Indien een of meer banken wordt verzocht het openen van een rekening door persoon X (als nieuwe klant) onverwijld te melden, dan worden van hen vooraf bepaalde gegevens gevorderd die de bank in beginsel vanwege zijn reguliere activiteiten toch zou verwerken indien persoon X klant wordt.

3.6 Gevoelige gegevens

Art. 126nf en126uf Sv vormen de basis om gevoelige gegevens te vorderen. Voor de gegevens die als 'gevoelig' gekwalificeerd kunnen worden, is aansluiting gezocht bij art. 16 Wbp. Het betreft informatie over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven of iemands lidmaatschap van een vakvereniging.[86] Kortom: gegevens die vanwege hun aard indringend betrekking hebben op de persoonlijke levenssfeer. Het vorderen van gevoelige gegevens kan noodzakelijk zijn bij de opsporing van zedenmisdrijven (welke seksueel getinte webpagina's bekijkt iemand?) of van terroristische misdrijven (welke politieke of levensbeschouwelijke literatuur of informatie heeft iemand geraadpleegd op internet?).[87]

Het feit dat de gegevens een indringende inbreuk veroorzaken op de persoonlijke levenssfeer maakt dat er aan de toepassing van deze bevoegdheid

---

85 *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 10.

86 Zie ook Hof Arnhem 24 september 2009, *NJFS* 2009, 265 waarin door de raadsvrouw een beroep op bewijsuitsluiting werd gedaan aangezien het opvragen van een pasfoto bij de gemeentelijke reisdocumentenadministratie door opsporingsambtenaren onrechtmatig zou zijn. Een foto bevat volgens de raadsvrouw informatie over iemands ras en daardoor zou art. 126nf Sv van toepassing zijn. Het hof oordeelt dat het opvragen van de foto is toegestaan op grond van de Paspoortuitvoeringsregeling Nederland 2001 en dus niet op grond van de Wbvg, voor zover die gegevens noodzakelijk zijn voor de opsporing van strafbare feiten. In HR 3 maart 2009, *LJN* BG9218 overwoog de HR dat uit de identiteitsgegevens van personen die zich voor enige vorm van medische hulp of informatie bij een ziekenhuis hebben gemeld, indirect informatie over de gezondheid van de betreffende personen kan worden afgeleid en daarom gegevens zijn betreffende de gezondheid in de zin van art. 126nd lid 2, derde volzin Sv en dus gevoelige gegevens zijn.

87 Jongeneel-van Amerongen 2005, p. 958.

zware voorwaarden verbonden zijn. Zo dient de officier van justitie een machtiging te hebben van de rechter-commissaris voor hij kan ertoe kan overgaan. De informatie mag worden gevorderd van de derde van wie redelijkerwijs kan worden vermoed dat hij toegang heeft tot de gegevens. Deze laatste eis is ook van toepassing bij het vorderen van andere dan identificerende (historische) gegevens. Uit de wetsgeschiedenis ten aanzien van art. 126nd Sv blijkt dat het redelijke vermoeden gebaseerd moet zijn op concrete feiten en omstandigheden. Bij andere dan identificerende gegevens kan wanneer een redelijk vermoeden ontbreekt, maar er wel aanwijzingen aanwezig zijn, duidelijkheid worden verkregen omtrent de vindplaats van de gegevens door het vorderen van identificerende gegevens op basis van art. 126nc Sv (door middel van het stellen van zogenoemde ja/nee-vragen).[88] Dat maakt dat de eis van art. 126nd Sv in de praktijk niet veel voorstelt. Nu in art. 126nc en 126nd Sv gevoelige gegevens expliciet zijn uitgesloten, kan bij het ontbreken van een redelijk vermoeden dat de derde over gevoelige gegevens beschikt, niet via de bij art. 126nd Sv toegestane uitweg duidelijkheid worden gecreëerd over de vindplaats van de gevoelige gegevens.[89]

Aandacht verdient dat in art. 126nf en 126uf Sv, in tegenstelling tot bij de hiervoor besproken bevoegdheden tot het vorderen van identificerende en andere dan identificerende (historische) gegevens, niet gesproken wordt van 'opgeslagen of vastgelegde' gegevens. Uit de MvT is op te maken dat het doel van de toevoeging 'opgeslagen of vastgelegd' is het duiden op het feit dat de gegevens historisch moeten zijn. De gegevens moeten op het moment van de vordering al door de derde zijn verwerkt. Met opgeslagen gegevens worden, zoals hiervoor aan de orde kwam, gegevens in een geautomatiseerd werk bedoeld, terwijl vastgelegde gegevens op een andere wijze zijn vastgelegd, bijvoorbeeld op papier.[90] Gezien de aard en strekking van de Wbvg ligt het voor de hand dat art. 126nf Sv slechts ziet op opgeslagen of vastgelegde gegevens. Art. 126ne Sv is immers het enige artikel dat betrekking heeft op toekomstige gegevens en daar wordt dan ook expliciet gebruikgemaakt van de zinsnede 'gegevens die eerst na het tijdstip van de vordering worden verwerkt'.

In art. 126nf Sv wordt daarnaast niet vereist dat de derde de gegevens anders dan ten behoeve van persoonlijk gebruik dient te verwerken. Gevoelige gegevens die worden verwerkt voor persoonlijk gebruik kunnen dus in het kader van art. 126nf lid 1 Sv ook worden gevorderd.

---

88 *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 8.
89 Mac Gillavry 2006.
90 *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 7 en 23.

Vordering van gevoelige gegevens is verder slechts mogelijk in het geval het onderzoek dit dringend vordert en er sprake is van verdenking van een misdrijf als bedoeld in art. 67 lid 1 Sv, dat gezien zijn aard of de samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert, dan wel in geval van verdenking dat in georganiseerd verband misdrijven als omschreven in art. 67 lid 1 Sv worden beraamd of gepleegd die, gezien hun aard of de samenhang met andere misdrijven die in dat georganiseerde verband worden beraamd of gepleegd, een ernstige inbreuk op de rechtsorde opleveren. Daaronder vallen onder andere moord, drugshandel, zedendelicten, mensenhandel, wapenhandel en ernstige fraude. Minder ernstige misdrijven kunnen een ernstige inbreuk op de rechtsorde opleveren doordat zij in combinatie met andere misdrijven worden gepleegd.[91]

Zoals hiervoor aan de orde werd gesteld, zijn de gevoelige gegevens, vanwege hun aard en de daaruit volgende gevolgen voor de persoonlijke levenssfeer van de verdachte, expliciet uitgezonderd van de bevoegdheden tot het vorderen van identificerende en andere dan identificerende gegevens. Dat betekent dat van instellingen waarvan vooraf duidelijk is dat zij gevoelige gegevens beheren, slechts op basis van art. 126nf en 126uf Sv gegevens kunnen worden gevorderd. Te denken valt aan kerkgenootschappen of vakverenigingen. Het is echter niet altijd vooraf duidelijk dat een instelling gevoelige gegevens beheert. Indien de officier van justitie bijvoorbeeld gegevens vordert betreffende de financiële transacties van een bepaalde persoon in een bepaalde periode, dan dient hij de (algemene) bevoegdheid van art. 126nd Sv of art. 126ne Sv toe te passen. Reden hiervoor is dat financiële transacties geen gevoelige gegevens zijn en men van de derde (bijvoorbeeld een bank) niet kan verlangen voor de verstrekking alle gegevens (bijvoorbeeld bankafschriften) te screenen op gevoelige gegevens. Het kan dus niet worden uitgesloten dat in de gevorderde gegevens bijvoorbeeld donaties aan een kerkgenootschap of vakvereniging zijn terug te vinden. Die gegevens zijn (achteraf) aan te merken als gevoelige gegevens, maar kunnen wel gevorderd worden op basis van de bevoegdheid van art. 126nd Sv of art. 126ne Sv. Vooraf is dus, net als bij de toepassing van sommige andere opsporingsbevoegdheden, niet geheel te voorzien wat het resultaat zal zijn. Dat maakt de toepassing van de bevoegdheid niet achteraf onrechtmatig en het resultaat kan, indien relevant voor het opsporingsonderzoek, blijkens de wetsgeschiedenis verder worden verwerkt.[92]

---

91 *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 25.

92 *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 10-11 en Jongeneel-van Amerongen 2005, p. 958.

Tijdens de parlementaire behandeling vormde het voorgaande een punt van discussie, welke heeft geleid tot een nuancering. Toenmalig minister van Justitie Donner stelde uiteindelijk dat als het aannemelijk is dat de vordering op grond van art. 126nd Sv mede betrekking heeft op gevoelige gegevens, die bevoegdheid niet zal worden aangewend. Die aannemelijkheid kan onder andere worden afgeleid uit de periode waarop de vordering betrekking heeft. Worden bijvoorbeeld bankgegevens over ten minste een half jaar opgevraagd dan is de aanwezigheid van gevoelige gegevens aannemelijk. De minister stelt nadrukkelijk wel dat dit niet betekent dat als het maar enigszins mogelijk is dat mede gevoelige gegevens worden gevorderd de bevoegdheid van art. 126nd Sv niet kan worden gebruikt.[93]

Een ander voorbeeld waar de aannemelijkheid van het aantreffen van gevoelige gegevens een discussiepunt kan opleveren, betreft het vorderen van foto's. Op 23 maart 2010 oordeelde de Hoge Raad (HR) in een zaak waarin door de officier van justitie van Trans Link Systems B.V. gegevens waren gevorderd, waaronder foto's van personen. Met verwijzing naar de Wbp besliste de HR dat gegevens waaruit informatie over het ras van een persoon kan worden afgeleid, zoals foto's van personen, als gevoelige informatie wordt gezien waarvoor art. 126nf Sv geldt. Het feit dat met de vordering niet werd beoogd de desbetreffende informatie aan de foto's te ontlenen deed daar volgens de HR niet aan af omdat vooraf duidelijk was dat er gevoelige gegevens zouden kunnen worden verkregen en daarom diende art. 126nf Sv te worden gebruikt.[94]

Deze uitspraak roept de belangrijke vraag op of deze opvatting ook zonder meer geldt ten aanzien van camerabeelden. Inmiddels is uit recente (weliswaar lagere) jurisprudentie een nuancering op de opvatting van de HR af te leiden.[95] Zo oordeelde de Rechtbank Zutphen op 15 april 2010 in een zaak waarin camerabeelden van een bank waren gevorderd. De vordering tot het verstrekken van camerabeelden was naar het oordeel van de politierechter niet (zonder meer) op een lijn te stellen met een vordering tot het verstrekken van gevoelige persoonsgegevens, aangezien er geen sprake was van een (dienstverlenende) relatie tussen de onderhavige bank en de verdachte, uit hoofde waarvan de bank over de bewuste gegevens (beeldmateriaal) beschikte. 'Verdachte heeft

---

93 *Handelingen I* 2004/05, p. 14-819/820 en Mac Gillavry 2006.

94 HR 23 maart 2010, *LJN* BK6331.

95 Behalve in de uitspraken die hierna worden beschreven, is deze kwestie ook aan de orde gekomen in: Rb. Rotterdam 19 mei 2010, *LJN* BM5003, Rb. Amsterdam 5 juli 2010, *LJN* BN1699, Rb. Amsterdam 5 juli 2010, *LJN* BN1025, Rb. Rotterdam 22 juli 2010, *LJN* BN3336, Rb. Rotterdam 22 juli 2010, *LJN* BN3338, Rb. Arnhem 3 augustus 2010, *LJN* BN2280 en Rb. Alkmaar 5 augustus 2010, *LJN* BN3312.

zich als passant, op straat, binnen het bereik van deze (beveiligings-)camera bevonden.' De politierechter oordeelde dat het belang om zich onbespied op straat in de openbare ruimte te begeven niet het privacybelang is dat de regeling van art. 126nc e.v. Sv beoogt te beschermen. De vordering tot het verstrekken van de camerabeelden kon in dit geval dus wel op art. 126nd Sv worden gegrond. Als vervolgens, bij het bekijken van de beelden door de politie, zou blijken dat daarop personen voorkomen van wie (bijvoorbeeld) ook de huidskleur zichtbaar is, dan maakt dit in het onderhavige geval de toepassing van de bevoegdheid ex art. 126nd Sv achteraf niet onrechtmatig en staat het niet het gebruik van die beelden en de daarmee verkregen (gevoelige) informatie in de weg.[96]

Het Hof Den Haag hanteerde op 6 mei 2010 een vergelijkbare redenering in een zaak waar camerabeelden van een aantal casinobedrijven waren gevorderd. Het hof stelde dat 'het hierbij niet op voorhand de bedoeling is geweest om gegevens te vorderen om daaraan gevoelige informatie te ontlenen. De beelden zijn niet door de personen die daarop staan afgebeeld afgegeven, en zijn niet gekoppeld aan (door dezen in vertrouwen aan een instantie afgegeven) personalia. Het gaat bij dit type cameratoezicht enkel om de vastlegging van het beeld van degene die komt pinnen. Beoogd wordt hiermee de opsporing mogelijk te maken van diegenen die op onrechtmatige wijze gebruikmaken van pinpassen. Voor beelden, opgenomen in winkels en casino's ter bestrijding en voorkoming van winkeldiefstallen en andere criminaliteit geldt mutatis mutandis hetzelfde.'

Ook het Hof Arnhem kwam op 3 juni 2010 in een zaak waar beelden van een beveiligingscamera van een pinautomaat van een bank waren gevorderd op grond van art. 126nd/ud Sv tot eenzelfde uitspraak. Het hof gaf expliciet aan dat deze zaak (en daarmee ook de zaken van de Rechtbank Zutphen en het Hof Den Haag) op essentiële punten verschilden van de kwestie die aan de orde was in de Trans Link-zaak. 'Het gaat immers om beelden die (anders dan in het geval van de HR) niet aan de bank waren toevertrouwd, maar om een opname van een beveiligingscamera waarvan de aanwezigheid op allerlei plekken in de publieke ruimte en in het bijzonder bij pinautomaten van algemene bekendheid is. Van een (aan de beelden of de opnamen daarvan) voorafgegane verwerking van gevoelige persoonsgegevens als bedoeld in art. 16 Wbp, is bij deze registratie in de opvatting van het hof geen sprake. Het verbod van art. 18 van de wet doet zich daarom evenmin gelden'. Het hof kwam tot de conclusie dat het beeldmateriaal in kwestie daarom op grond van art. 12nd/ud Sv kon worden gevorderd en om die reden kon en mocht worden gebruikt voor het bewijs.[97]

---

96 Rb. Zutphen 15 april 2010, *LJN* BM1196.
97 Hof Arnhem 3 juni 2010, *LJN* BM6941.

De Rechtbank Haarlem onderschreef de uitspraken van het Hof Arnhem, het Hof Den Haag en de Rechtbank Zutphen op 11 juni 2010. De rechtbank wees op art. 8 Wbp, art. dat bedrijven toestaat beveiligingscamera's te gebruiken ter beveiliging van hun bedrijf. 'Aangezien niet identificatie maar beveiliging het achterliggende doel is, er worden immers geen namen aan de beelden gekoppeld, vindt de verwerking tegen een geheel andere achtergrond plaats dan wanneer het gaat om foto's in een leden- of personeelsadministratie dan wel registratiesysteem voor houders van bepaalde passen. Er wordt niet vanuit gegaan dat uit camerabeelden zonder meer gevoelige gegevens als ras kunnen worden afgeleid, ook al niet omdat vooraf onbekend is van welke personen beelden worden gemaakt. Vaak achteraf zal pas blijken wat uit de beelden valt af te leiden, of wat daarop al dan niet zichtbaar is. In dat opzicht kan de vergelijking gemaakt worden met het opvragen van de in de MvT als voorbeeld genoemde financiële gegevens. In de MvT is expliciet vermeld dat deze op basis van de algemene bevoegdheid opgevraagd kunnen worden, ook al zou naderhand blijken dat er gevoelige gegevens tussen zaten, en vervolgens verwerkt kunnen worden. Daar komt bij dat deelname aan het maatschappelijk verkeer een zekere inbreuk op de privacy met zich meebrengt, waarbij niet altijd sprake is van schending van een *Schutznorm*. Naar het oordeel van de politierechter is daarvan sprake bij beelden van een camera door een bedrijf ter beveiliging van dat bedrijf geplaatst. Eén en ander kan anders zijn indien voorzienbaar is dat er gevoelige gegevens zijn geregistreerd. Gelet op het voorgaande gaat het echter te ver er op voorhand vanuit te gaan dat camerabeelden, zoals hiervoor bedoeld, gevoelige gegevens zouden bevatten en dus onder het regime van art. 126nf Sv vallen. Daarmee zou ook het evenwicht tussen de diverse belangen, zoals het individuele belang bij bescherming van de persoonlijke levenssfeer en het algemene belang van de opsporing van strafbare feiten, verstoord zijn.'[98]

Discussies over de vraag of een gegeven als gevoelig moet worden gekwalificeerd, komen, ondanks het feit dat de categorieën van gevoelige gegevens limitatief zijn opgesomd in art. 126nc lid 3 en 126nd lid 2 Sv, blijkens de hiervoor beschreven zaken regelmatig voor.[99] Het op de wetsgeschiedenis van de Wbp gebaseerde criterium van de HR, dat gegevens waaruit informatie over

---

98 Rb. Haarlem 10 juni 2010, *LJN* BM7440.

99 De categorieën gegevens die de Wbvg als gevoelige gegevens aanduidt, zijn gebaseerd op art. 16 van de Wet bescherming persoonsgegevens. De categorieën uit de Wbp vinden op hun beurt blijkens de MvT hun grondslag in Europese regelgeving, te weten het Dataprotectieverdrag van de Raad van Europa (1981) en de Europese richtlijn bescherming persoonsgegevens (richtlijn 95/46/EG (*PbEG* 1995, L 281)). Zie o.a. *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 100.

het ras van een persoon kan worden afgeleid, moeten worden gezien als gevoelige informatie, is in zijn algemeenheid als te strikt te kwalificeren. De opvatting van de HR dat bij het vorderen van de foto's in de Trans Link-zaak gekozen had moeten worden voor een vordering ex art. 126nf Sv is evenwel plausibel, nu in dat geval door het opvragen van de naam en adresgegevens met de daarbij behorende foto gevoelige gegevens als ras direct aan een betrokkene konden worden gekoppeld. Dan ligt een vordering ex art. 126nf Sv in de rede.

Dit is anders in het geval van camerabeelden. Lagere rechters hebben inmiddels terecht in recente uitspraken geoordeeld dat camerabeelden niet zonder meer op een lijn zijn te stellen met gevoelige gegevens die dienen te worden gevorderd op grond van art. 126nf Sv. Als belangrijkste argument in deze discussie geldt dat camerabeelden niet direct kunnen worden gekoppeld aan een persoon. Daarmee verschillen ze fundamenteel van foto's die gekoppeld zijn aan personalia, die in de zaak Trans Link bovendien ook nadrukkelijk in combinatie waren gevorderd.

Daarnaast worden beveiligingscamera's niet ingezet met identificatie of het verkrijgen van gevoelige gegevens als doel. Bij camerabeelden is, in tegenstelling tot bij foto's, informatie over etniciteit derhalve een bijvangst. Deze situatie moet worden onderscheiden van die waarin gericht om gevoelige gegevens wordt gevraagd.[100]

Bovendien valt het belang om zich onbespied op straat te kunnen begeven niet onder het privacybelang dat de Wbvg beoogt te beschermen. De beelden zijn immers niet door de afgebeelde personen toevertrouwd aan een instelling of instantie, zoals dat bij foto's doorgaans wel het geval is. Dat rechters waarde hechten aan het feit dat foto's die gekoppeld zijn aan personalia door een betrokkene aan een instelling of instantie zijn afgestaan met een ander doel dan waarvoor zij door de officier van justitie worden gevorderd, is derhalve niet meer dan logisch.

Het criterium van de HR zou in het licht van bovenstaande argumenten genuanceerd moeten worden zodat slechts gegevens, door een persoon toevertrouwd aan een instelling of instantie, waaruit informatie over het ras van een

[100] Ter vergelijking: het OM stelde zich in de Trans Link-zaak ook op het standpunt dat er sprake was van een bijvangst nu het doel niet was het verkrijgen van privacygevoelige informatie (zoals gevoelige informatie als ras), maar het verkrijgen van informatie omtrent reisbewegingen. Er dient echter opgemerkt te worden dat in de Trans Link-zaak een koppeling werd gemaakt van de foto's en de identiteitsgegevens waardoor van bijvangst geen sprake meer is.

persoon kan worden afgeleid én die direct gekoppeld kunnen worden aan de betreffende persoon, aangemerkt worden als gevoelige informatie.[101]

3.7 Ontsleutelen van versleutelde gegevens

Een vordering tot gegevensverstrekking impliceert dat de gegevens ontsleuteld verstrekt dienen te worden door de gegevenshouder. Het kan echter voorkomen dat de gegevens die gevorderd worden op basis van de hiervoor beschreven bevoegdheden beveiligd zijn met behulp van een code, terwijl de gegevensverstrekker niet zelf over de code beschikt waarmee de gegevens ontsleuteld kunnen worden. Aangezien het opsporingsbelang er belang bij kan hebben dat deze beveiliging wordt doorbroken is in art. 126nh en in art. 126uh Sv de bevoegdheid opgenomen voor het ontsleutelen van versleutelde gegevens.

De officier van justitie kan degene van wie redelijkerwijs wordt vermoed dat hij kennis draagt van de wijze van versleuteling van de gevorderde gegevens, bevelen medewerking te verlenen aan het ontsleutelen van de gegevens door de versleuteling ongedaan te maken, dan wel deze kennis ter beschikking te stellen. Deze bevoegdheid kan worden aangewend indien het onderzoek dit vordert en zij kan plaatsvinden bij of terstond na de toepassing van de bevoegdheden om gegevens te vorderen. De MvT vermeldt dat beveiligingscodes en encryptiesleutels die zijn opgeslagen of vastgelegd, kunnen worden aangemerkt als gegevens die vallen binnen het bereik van art. 126nd Sv. Zij zouden derhalve door de officier van justitie, met toepassing van de bevoegdheid tot het vorderen van gegevens op grond van art. 126nd Sv, kunnen worden gevorderd. Uitgangspunt dient evenwel te zijn dat dergelijke codes op grond van de speciale bevoegdheid van art. 126nh Sv gevorderd worden.[102] Eenzelfde bevoegdheid als in art. 126nh Sv is vervat in art. 125k Sv. Daar betreft het de situatie dat men in het kader van een doorzoeking stuit op versleutelde gegevens.

3.8 Doorzoeking ter vastlegging van gegevens

In art. 125i Sv is neergelegd dat de rechter-commissaris, de officier van justitie, de hulpofficier van justitie en de opsporingsambtenaar op gelijke voet met de hun toekomende bevoegdheden tot doorzoeking ter inbeslagneming, bevoegd

---

[101] Voor een verdere bespreking van de consequenties van het Trans Link-arrest voor de opsporingspraktijk en het standpunt van prof. dr. Mevis in dezen, wordt verwezen naar paragraaf 7.3.6.

[102] *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 11.

zijn tot doorzoeking van een plaats ter vastlegging van gegevens die op deze plaats op een gegevensdrager zijn opgeslagen of vastgelegd. Een doorzoeking die uitsluitend bedoeld is om gegevens vast te leggen is dus toegestaan.

Tijdens een doorzoeking kunnen verschillende activiteiten worden verricht: het onderzoek doen naar, inzage krijgen in en een kopie maken van gegevens die, hetzij op papier, hetzij op enige andere gegevensdrager, daaronder begrepen een geautomatiseerd werk, zijn opgeslagen.[103]

Aangezien het bij een doorzoeking vooraf vaak niet precies duidelijk is wat voor gegevens men zal aantreffen, is het onderscheid naar categorieën gegevens (identificerende, andere dan identificerende en gevoelige) moeilijk hanteerbaar. Uitgangspunt (van subsidiariteit) bij de doorzoeking is dat deze bevoegdheid pas wordt toegepast als het niet effectief is om andere bevoegdheden, zoals het vorderen van gegevens of het vorderen van de uitlevering van een voorwerp ter inbeslagneming, te gebruiken. Dit is onder meer het geval als verwacht kan worden dat de derde geen medewerking zal verlenen aan het verstrekken van gegevens, dan wel indien er een risico bestaat dat gegevens of voorwerpen worden weggemaakt.[104] De zwaardere bevoegdheid (tot in dit geval doorzoeking) komt derhalve pas in beeld als de lichtere bevoegdheden niet (kunnen) werken.[105]

Op grond van art. 96b Sv is een opsporingsambtenaar bevoegd om een vervoermiddel (met uitzondering van het woongedeelte) te doorzoeken ter inbeslagneming. De (hulp)officier van justitie kan op grond van art. 96c Sv een andere plaats dan een woning en een kantoor van een verschoningsgerechtigde doorzoeken ter inbeslagneming en is bij dringende noodzakelijkheid, en indien het optreden van de rechter-commissaris niet kan worden afgewacht, bevoegd om ook een woning en een kantoor van een verschoningsgerechtigde te doorzoeken op grond van art. 97 Sv. De rechter-commissaris is tot slot bevoegd op grond van art. 110 Sv om elke plaats te doorzoeken (op vordering van de officier van justitie en in het gerechtelijk vooronderzoek ambtshalve). Voor bovengenoemde functionarissen bepaalt art. 125i Sv dat de doorzoeking ook kan plaatsvinden in het kader van de vastlegging van gegevens.

Indien de genoemde functionaris bij de doorzoeking ter vastlegging van gegevens stuit op een beveiligd geautomatiseerd werk, dan kan hij op basis van art. 125k Sv, indien het belang van het onderzoek dit bepaaldelijk vordert, degene van wie redelijkerwijs kan worden vermoed dat hij kennis draagt van de wijze van de beveiliging, bevelen toegang te verschaffen tot de aanwezige geauto-

---

103 *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 12.
104 *Kamerstukken II* 2003/04, 29 441, nr. 6, p. 10.
105 *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 12.

matiseerde werken (of delen ervan) of de kennis omtrent de beveiliging ter beschikking te stellen. Dat geldt ook indien in een geautomatiseerd werk versleutelde gegevens worden aangetroffen.

Vindt een doorzoeking ter vastlegging van gegevens plaats bij een aanbieder van een openbaar telecommunicatienetwerk of een openbare telecommunicatiedienst, dan kunnen gegevens worden aangetroffen die niet voor deze bestemd of van deze afkomstig zijn. Dit betreft de gegevens in e-mails die zijn opgeslagen bij een internetaanbieder en die niet voor de internetaanbieder bestemd is of van deze afkomstig is, met andere woorden: e-mails van abonnees.[106] Deze categorie gegevens is in een aparte bepaling opgenomen om een e-mail een soortgelijke bescherming te verlenen als een andere vorm van vertrouwelijke informatie: poststukken.[107] Op basis van art. 125la Sv kan de officier van justitie slechts bevelen van deze gegevens kennis te nemen en deze vast te leggen 'voor zover zij klaarblijkelijk van de verdachte afkomstig zijn, voor hem bestemd zijn, op hem betrekking hebben of tot het begaan van het strafbare feit hebben gediend, ofwel klaarblijkelijk met betrekking tot die gegevens het strafbare feit is gepleegd'. Een voorafgaande machtiging van de rechter-commissaris is noodzakelijk.

Bij vergelijking van hiervoor genoemde bevoegdheden met de bevoegdheden tot het vorderen van gegevens valt op dat de laatste groep in enkele gevallen zwaardere voorwaarden kent voor toepassing dan de bevoegdheden tot doorzoeking. Zo zijn de voorwaarden voor het vorderen van andere dan identificerende gegevens (door de officier van justitie) bijvoorbeeld zwaarder dan de bevoegdheid tot doorzoeking van een vervoermiddel (door een opsporingsambtenaar). Het levert volgens de MvT echter misbruik van bevoegdheid op als de opsporingsambtenaar een vervoermiddel zou doorzoeken om de beschikking te krijgen over andere dan identificerende gegevens, terwijl deze eigenlijk door toepassing van art. 126nd Sv door de officier van justitie verkregen zouden moeten worden.[108]

Tot slot biedt art. 125j Sv de mogelijkheid om in geval van doorzoeking onderzoek te verrichten in computersystemen die vanuit de locatie waar de doorzoeking plaatsvindt (via telecommunicatie) toegankelijk zijn, maar zich fysiek op een andere plaats bevinden.

---

106 *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 19.

107 Wiemans 2006.

108 *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 12. Zoals aangegeven is de bevoegdheid van art. 125i Sv echter nodig als bijvoorbeeld verwacht kan worden dat de derde geen medewerking zal verlenen aan het verstrekken van gegevens, dan wel indien er een risico bestaat dat gegevens of voorwerpen worden weggemaakt. Zie Wiemans 2006.

3.9 Besluit

In dit hoofdstuk is de systematiek van de Wbvg geschetst en zijn de afzonderlijke wetsartikelen de revue gepasseerd. De Wbvg is gebaseerd op twee afzonderlijke stelsels van bevoegdheden. Het eerste stelsel kent zijn neerslag in art. 126nc-126nh Sv en het tweede stelsel in art. 126uc-126uh Sv. Slechts het toepassingsbereik van beide stelsels verschilt. Zo is het eerste stelsel neergelegd in de titel rondom de bijzondere bevoegdheden tot opsporing (titel IVa) en het tweede stelsel in titel V (bijzondere bevoegdheden tot opsporing voor het onderzoek naar het beramen of plegen van ernstige misdrijven in georganiseerd verband).

De Wbvg bevat een driedeling in bevoegdheden naar de aard van de gegevens: identificerende gegevens, andere dan identificerende gegevens (historisch en toekomstig, niet zijnde gevoelige gegevens) en gevoelige gegevens. Voor de bevoegdheden geldt: al naar gelang de categorie gegevens ingrijpender is voor de persoonlijke levenssfeer en/of naarmate meer handelingen van een derde worden gevraagd, gelden zwaardere voorwaarden voor toepassing. Naast deze bevoegdheden behoren ook het vorderen medewerking te verlenen aan het ontsleutelen van versleutelde gegevens en de doorzoeking ter vastlegging van gegevens tot de bevoegdheden van de Wbvg.

De verdachte en verschoningsgerechtigde blijven buiten het bereik van de Wbvg in die zin dat de vordering niet gericht kan worden tot de verdachte en de verschoningsgerechtigde geen medewerking hoeft te verlenen aan de vordering. Niet alleen over de verdachte, maar ook over andere personen kunnen gegevens worden gevorderd indien dat in het belang van het onderzoek is. Beklag tegen een vordering staat (achteraf) open op grond van art. 552a Sv.

Ten eerste kunnen identificerende gegevens (art. 126nc en 126uc Sv), grofweg NAW-gegevens, in het belang van het onderzoek worden gevorderd door een opsporingsambtenaar van degene die daarvoor redelijkerwijs in aanmerking komt en die de gegevens verwerkt vanwege een functie of beroep. Van belang is dat de bevoegdheid ook gebruikt kan worden om van de derde te vorderen of hij over gegevens over de betreffende persoon beschikt, de zogenoemde ja/nee-vragen.

In de tweede plaats kunnen andere dan identificerende gegevens (art. 126nd en 126ud Sv) worden gevorderd. Dit betreft alle gegevens, met uitzondering van gevoelige gegevens. Het dient wel te gaan om historische gegevens: de informatie dient opgeslagen of vastgelegd te zijn. De bevoegdheid deze gegevens te vorderen valt toe aan de officier van justitie.

De derde categorie gegevens in de Wbvg betreft 'toekomstige andere dan identificerende gegevens' (art. 126ne en 126ue Sv). De voorwaarden die gesteld worden aan deze bevoegdheid zijn gelijk aan die gelden voor art. 126nd Sv.

In de vierde plaats biedt de Wbvg de mogelijkheid gevoelige gegevens (art. 126nf en 126uf Sv), bijvoorbeeld informatie omtrent iemands godsdienst, ras, politieke gezindheid, gezondheid en seksuele leven, te vorderen. De officier van justitie dient hiervoor te beschikken over een machtiging van de rechter-commissaris; er moet een dringend onderzoeksbelang zijn en er moet sprake zijn van een 'voorlopige hechtenis-feit' dat een ernstige inbreuk op de rechtsorde oplevert of van een dergelijk feit dat in georganiseerd verband wordt beraamd of gepleegd. Aandachtspunt betreft de huidige ontwikkeling in de jurisprudentie met betrekking tot de vraag of foto's en camerabeelden zijn aan te merken als gevoelige gegevens.

De officier van justitie kan, ten vijfde, degene van wie redelijkerwijs wordt vermoed dat hij kennis draagt van de wijze van versleuteling van de gevorderde gegevens bevelen medewerking te verlenen aan het ontsleutelen van de gegevens door de versleuteling ongedaan te maken, dan wel deze kennis ter beschikking te stellen (art. 126nh en 126uh Sv).

De laatste bevoegdheid uit de Wbvg is de doorzoeking ter vastlegging van gegevens (art. 125i Sv). Het biedt de mogelijkheid om ter plaatse onderzoek te verrichten in computersystemen, in plaats van de gegevensdragers eerst middels inbeslagneming ter beschikking te hoeven krijgen.

4 De verhouding van de Wbvg tot andere bevoegdheden

4.1 Inleiding

De Wbvg ziet toe op het vorderen van gegevens in algemene zin. Opsporingsinstanties hebben echter ook nog andere mogelijkheden om informatie van derden te verkrijgen. Het is daarom goed om te schetsen hoe die in verhouding staan tot de uit de Wbvg voortvloeiende bevoegdheden. Concreet gaat het daarbij ten eerste om de bevoegdheden tot het vorderen van gegevens van aanbieders van telecommunicatie. Deze mogelijkheden komen in paragraaf 4.2 aan de orde. In de tweede plaats kunnen ook voorwerpen in beslag worden genomen op grond van art. 94-105 Sv. Deze voorwerpen, zoals papier of harde schijven uit computers, kunnen echter ook gegevens bevatten. In paragraaf 4.3 wordt hierop nader ingegaan. Vervolgens komen in paragraaf 4.4 de bevoegdheden tot het vorderen van gegevens in het kader van ontnemingsvorderingen, onder andere op grond van art. 126a Sv, aan bod. Ten vierde kunnen bevoegdheden van de Algemene wet bestuursrecht (Awb), in casu art. 5:16-5:20 Awb, worden aangewend om informatie van derden te verkrijgen. In paragraaf 4.5 worden deze nader beschreven. In paragraaf 4.6 wordt aandacht besteed aan de bevoegdheden tot gegevensvergaring in enkele bijzondere wetten, te weten de Algemene wet inzake rijksbelastingen (Awr) en de Wet op de economische delicten (WED). [109] Paragraaf 4.7 besluit dit hoofdstuk met een korte samenvatting van de bevindingen.

4.2 Het vorderen van gegevens van aanbieders van telecommunicatie

Al voor de inwerkingtreding van de Wbvg kende het WvSv bevoegdheden tot het vorderen van verkeersgegevens en gebruikersgegevens van de aanbieders van openbare telecommunicatienetwerken en -diensten.[110] In art. 126la Sv wordt aangegeven dat onder een aanbieder van een communicatiedienst wordt verstaan: de natuurlijke persoon of rechtspersoon die in de uitoefening van een beroep of bedrijf aan de gebruikers van zijn dienst de mogelijkheid biedt te communiceren met behulp van een geautomatiseerd werk, of gegevens verwerkt of opslaat ten behoeve van een zodanige dienst of de gebruikers van die dienst.

Van de aanbieders kunnen gegevens worden gevorderd betreffende de gebruiker van een communicatiedienst en het communicatieverkeer met betrek-

---

[109] Als aanvulling wordt nog gewezen op de mogelijkheid om in het kader van de Wet Werk en Bijstand gegevens te vorderen.

[110] Zie o.a. Smits 2006.

king tot die gebruiker (art. 126n Sv).[111] Bij verkeersgegevens gaat het om de uiterlijke kenmerken van de telecommunicatie en niet om de inhoud van hetgeen via het communicatieverkeer wordt uitgewisseld. Voorbeelden daarvan zijn de betrokken nummers, de gebruikte apparatuur en het tijdstip van de aanvang en de duur van het verkeer.[112] In het geval gebruik wordt gemaakt van mobiele telefoons kunnen ook locatiegegevens, aan de hand van de zendmasten waarlangs communicatie heeft plaatsgevonden, worden opgevraagd. In art. 126n Sv is opgenomen dat de vordering slechts betrekking kan hebben op gegevens die bij algemene maatregel van bestuur zijn aangewezen.[113] Gebruikersgegevens (art. 126na Sv) betreffen naam, adres, woonplaats, nummer en soort dienst. Deze laatste gegevens lijken erg op identificerende gegevens, maar dienen op basis van de speciale bevoegdheid van art. 126na Sv gevorderd te worden.[114]

De wet voorziet via art. 126ng en art. 126ug Sv ook in de bevoegdheid om gegevens te vorderen bij communicatiediensten.[115] De reeds bestaande bevoegdheden tot het vorderen van verkeersgegevens en gebruikersgegevens zijn echter gehandhaafd na invoering van de Wbvg. Art. 126ng en 126ug Sv bepalen dan ook dat een vordering tot gegevensverstrekking slechts gericht kan worden tot communicatiediensten voor zover zij betrekking heeft op andere gegevens dan die welke gevorderd kunnen worden door de toepassing van art. 126n en 126na Sv.[116] Kortom: verkeers- en gebruikersgegevens kunnen niet via art. 126nc, 126nd of 126ne Sv worden gevorderd. De MvT noemt als voorbeeld een geval waarin, in het kader van de opsporing van fraude met betalingen van (telefoon)rekeningen, van de aanbieder van telecommunicatie gegevens over de betaling van de rekeningen worden gevorderd. De rechtsbasis is gelegen in art. 126nd Sv omdat het gegevens betreft die niet vallen onder art. 126n en 126na Sv.[117]

In art. 126ng lid 1 Sv zijn gegevens die zijn opgeslagen in het geautomatiseerde werk van de aanbieder en die niet voor deze bestemd of afkomstig

---

111 Onder een gebruiker van een communicatiedienst verstaat art. 126la Sv: de natuurlijke persoon of rechtspersoon die met de aanbieder van een communicatiedienst een overeenkomst is aangegaan met betrekking tot het gebruik van die dienst of die feitelijk gebruik maakt van een zodanige dienst.

112 Blom 2009.

113 Het betreft het Besluit vorderen gegevens telecommunicatie (*Stb.* 2004, 394).

114 *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 26.

115 Zie *Kamerstukken II* 2007/08, 31 391, nr. 2 waar wordt voorgesteld in art. 126ng lid 1 Sv, art. 126ne lid 3 en 126nf lid 1 Sv op te nemen.

116 Op grond van art. 126ng lid 3 Sv kan de vordering niet worden gericht tot de verdachte. Een verschoningsgerechtigde is op grond van art. 96a lid 3 Sv niet verplicht mee te werken aan de vordering.

117 *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 26.

zijn ook uitgezonderd van de mogelijkheid om op grond van de Wbvg te worden gevorderd. Met deze laatste categorie gegevens wordt gedoeld op informatie betreffende een e-mail die is opgeslagen bij de internetaanbieder. Hierboven werd al aangegeven dat de wetgever e-mails van abonnees een soortgelijke bescherming wil verlenen als een andere vorm van vertrouwelijke informatie: poststukken.[118] Dit heeft ertoe geleid dat de gegevens betreffende een e-mail op basis van art. 126ng lid 2 Sv enkel gevorderd kunnen worden voor zover zij klaarblijkelijk van de verdachte afkomstig zijn, voor hem bestemd zijn, op hem betrekking hebben of tot het begaan van het strafbare feit hebben gediend, of klaarblijkelijk met betrekking tot die gegevens het strafbare feit is gepleegd. De officier van justitie is bevoegd deze gegevens te vorderen, na machtiging van de rechter-commissaris, en slechts indien het belang van het onderzoek dit dringend vordert. Daarnaast moet het gaan om een misdrijf als omschreven in art. 67 lid 1 Sv, dat gezien zijn aard of de samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert.

4.3 De bevoegdheden tot inbeslagneming van voorwerpen

Gegevens kunnen ook ter beschikking komen aan de met opsporing belaste instanties door gebruik te maken van de bevoegdheden tot inbeslagneming van voorwerpen en tot het vorderen van uitlevering van voorwerpen ter inbeslagneming. Door deze bevoegdheden kunnen gegevensdragers zoals documenten, boeken, ordners, computers en usb-sticks in beslag worden genomen. Wanneer het gaat om de gegevensvergaring bestaat de mogelijkheid dat het in beslag nemen van een computer disproportioneel is wanneer de inbeslagneming zeer ingrijpende gevolgen heeft voor de beslagene. Aan de Wbvg ligt de gedachte ten grondslag dat de bevoegdheden tot inbeslagneming niet gebruikt mogen worden als kan worden volstaan met de (lichtere) bevoegdheden tot het vorderen van gegevens. Er kan slechts nog worden overgegaan tot inbeslagneming van de gehele gegevensdrager indien de omstandigheden daartoe aanleiding geven. Te denken valt daarbij aan een zaak waarbij langdurig onderzoek in omvangrijke dossiers nodig is voordat men überhaupt weet welke gegevens voor het opsporingsonderzoek van belang zijn.[119]

---

[118] Ondanks het feit dat e-mails in de Wbvg op eenzelfde wijze worden beschermd als gevoelige gegevens gaat het te ver om e-mails te kwalificeren als gevoelige gegevens. Reden hiervoor is dat e-mails onder het briefgeheim en daarmee de bescherming van art. 13 van de Grondwet vallen en de bescherming van de categorieën gevoelige gegevens in de Wbvg een geheel andere oorsprong kent.

[119] *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 12.

4.4 Bevoegdheden in het kader van ontnemingsvorderingen

In art. 126a Sv was al voor de inwerkingtreding van de Wbvg een bevoegdheid opgenomen om in het kader van het Strafrechtelijk Financieel Onderzoek (hierna verder: SFO) gegevens te vergaren. Op basis van lid 1 van dat artikel is de opsporingsambtenaar die met het SFO belast is, op vertoon van een afschrift van de door de rechter-commissaris verleende machtiging tot instelling van het SFO, bevoegd gegevens te vorderen. Het doel van de gegevensvergaring is het verkrijgen van inzicht in de vermogenspositie van degene tegen wie het onderzoek is gericht. De opsporingsambtenaar kan de vordering richten tot eenieder, met uitzondering van degene tegen wie het SFO is gericht en verschoningsgerechtigden. Gevoelige gegevens zijn expliciet uitgezonderd en kunnen dus enkel gevorderd worden in het kader van art. 126nf Sv, ook als een SFO is ingesteld. De bevoegdheden die neergelegd zijn in art. 126nc en 126nd Sv bieden voor het SFO dus geen nieuwe mogelijkheden. Art. 126ne Sv heeft die echter wel uitgebreid omdat daarmee voortaan ook toekomstige gegevens kunnen worden gevorderd als een SFO is ingesteld.[120]

In vergelijking met de bevoegdheden van de Wbvg is art. 126a Sv deels ruimer aangezien de opsporingsambtenaar bevoegd is gegevens te vorderen, terwijl dat in de Wbvg vaak de officier van justitie is, en deels beperkter gezien het feit dat de opsporingsambtenaar altijd optreedt krachtens een machtiging van de rechter-commissaris op grond waarvan het SFO is ingesteld. Daar komt nog bij dat in het kader van een SFO slechts gegevens gevorderd kunnen worden om inzicht te krijgen in iemands vermogenspositie.[121]

De toenmalige minister van Justitie Hirsch Ballin heeft een wetsvoorstel ingediend ter verbetering van de toepassing van de maatregel ter ontneming van wederrechtelijk verkregen voordeel (verruiming mogelijkheden voordeelontneming).[122] In het wetsvoorstel wordt voorzien in de bevoegdheid om een onderzoek in te stellen naar het vermogen van de veroordeelde indien hij verzuimt te voldoen aan een onherroepelijk opgelegde ontnemingsmaatregel ex art. 36e Sr. Uit het onderzoek kan bijvoorbeeld blijken waar voorwerpen van de veroordeelde zich bevinden zodat daarop verhaal kan worden genomen.[123]

---

120 *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 13.
121 *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 13.
122 *Kamerstukken II* 2009/10, 32 194, nr. 2. Zie daarover Borgers en Kooijmans 2010.
123 *Kamerstukken II* 2009/10, 32 194, nr. 3, p. 14.

Het wetsvoorstel beoogt na art. 577b Sv een zestal artikelen in te voegen die de bevoegdheden beschrijven. Is de termijn voor volledige betaling verstreken, de hoogte van de resterende betalingsverplichting 'van aanzienlijk belang' en zijn er aanwijzingen dat aan de veroordeelde voorwerpen toebehoren waarop krachtens art. 577b Sv verhaal kan worden genomen, dan kan de officier van justitie, na machtiging van de rechter-commissaris, een onderzoek naar het vermogen van de veroordeelde instellen op basis van art. 577ba Sv. De bevoegdheden die tijdens het onderzoek kunnen worden gehanteerd, worden opgesomd in art. 577bb Sv. De navolgenart. bieden hierop aanvullende voorzieningen.

Een deel van de voorgestelde bevoegdheden is gericht op het verkrijgen van gegevens van anderen. Zo bestaat de mogelijkheid, ontleend aan art. 126a Sv, om van derden van wie wordt vermoed dat zij vermogensbestanddelen van de veroordeelde onder zich hebben of hebben gehad, te vorderen dat zij daarvan opgave doen. De overige mogelijkheden tot het vorderen van gegevens zijn gebaseerd op art. 126nc tot en met 126ne Sv.[124] Opvallend is dat het vorderen van gegevens op basis van de Wbvg slechts kan plaatsvinden in het kader van de opsporing. De voorgestelde nieuwe bevoegdheden met betrekking tot verbetering van de toepassing van de maatregel ter ontneming van wederrechtelijk verkregen voordeel vinden plaats in het kader van de tenuitvoerlegging van de maatregel.

4.5 De bevoegdheden van de Algemene wet bestuursrecht

Het vorderen van gegevens langs bestuurlijke weg dient in beginsel te worden onderscheiden van het vorderen van gegevens langs strafvorderlijke weg. De Algemene wet bestuursrecht (Awb) kent toezichthouders in onder andere art. 5:16, 5:17 en 5:20 bevoegdheden toe in het kader van de naleving van regelgeving.[125] Het betreft respectievelijk het vorderen van inlichtingen, het vorderen van inzage in zakelijke gegevens en het eenieder verplichten alle medewerking te verlenen. Een toezichthouder kan via de ruim geformuleerde bevoegdheden van de Awb derhalve gegevens vorderen die ook vallen onder de reikwijdte van de Wbvg. Voor toepassing van de toezichthoudende bevoegdheden is echter wel een bestuursrechtelijk doel nodig, te weten toezicht op naleving van bestuurswetten. In het licht van de wetsgeschiedenis is een toezichthouder niet bevoegd langs bestuurlijke weg gegevens te vorderen als strafrechtelijke afdoening het

---

124 *Kamerstukken II* 2009/10, 32 194, nr. 3, p. 15.

125 In art. 5:11 Awb is neergelegd wie als toezichthouder kunnen worden aangemerkt.

uitsluitende doel is.[126] Art. 1:6 sub a Awb stelt namelijk dat de wet niet van toepassing is op de opsporing en vervolging van strafbare feiten. Dat sluit niet uit dat als er een bestuursrechtelijk traject loopt en er een verdenking ontstaat op grond van art. 27 Sv, men naast het bestuursrechtelijk traject een strafvorderlijk traject kan starten. Zolang het bestuursrechtelijk en strafvorderlijk doel aanwezig blijven, kunnen beide trajecten naast elkaar bestaan. Het is dus de vraag in hoeverre de trajecten (bestuursrecht versus strafrecht) in de praktijk overlappen.[127]

4.6 De bevoegdheden in enkele bijzondere wetten

Tot slot dient aandacht te worden besteed aan enkele bijzondere wetten op grond waarvan gegevens kunnen worden verkregen. Een opsporingsmedewerker van de FIOD kan, naast van de bevoegdheden van de Wbvg, gebruikmaken van de bevoegdheid van art. 81 Awr. Dit artikel bepaalt dat de ambtenaren belast met het opsporen van bij de belastingwet strafbaar gestelde feiten, te allen tijde bevoegd zijn tot inbeslagneming van de ingevolge het Wetboek van Strafvordering voor inbeslagneming vatbare voorwerpen.[128] Zij kunnen daartoe hun uitlevering vorderen. Opvallend is dat, getuige de zinsnede 'te allen tijde', geen verdenking nodig is voor toepassing van art. 81 Awr. Daarnaast kan de opsporingsambtenaar deze bevoegdheid zelfstandig aanwenden, dus zonder tussenkomst van het openbaar ministerie. Als beperking van art. 81 Awr geldt dat het moet gaan om een fiscaal delict.

De strafvorderlijke tegenhanger van art. 81 Awr is art. 96a Sv, waarin de bevoegdheid tot inbeslagneming van voorwerpen is neergelegd. De bevoegdheid van art. 81 Awr gaat in twee opzichten verder dan de strafvorderlijke bevoegdheden. In de eerste plaats kan de bevoegdheid van art. 81 Awr te allen tijde worden uitgeoefend, terwijl opsporingsambtenaren bij de bevoegdheid tot inbeslagneming blijkens art. 96 Sv beperkt zijn tot heterdaadgevallen en misdrijven in de zin van art. 67 lid 1 Sv. Als tweede verschil kan worden opgemerkt dat art. 81 Awr ook tot een verdachte en verschoningsgerechtigde kan worden gericht.[129]

In geval van verdenking van een economisch delict, biedt art. 19 WED aan opsporingsambtenaren de bevoegdheid gegevens en bescheiden in te zien en

---

126 *Kamerstukken I* 1995/96, 23 700, nr. 188b, p. 1.
127 Voor de verhouding tussen bestuursrecht en strafrecht zie nader Knigge 2009 en Michiels 2009.
128 Zie art. 94 lid 1 Sv.
129 Smits 2008.

daarvan kopieën te maken. Ook voor de toepassing van deze bevoegdheid wordt een ruim opsporingsbegrip gehanteerd. Er hoeft geen sprake te zijn van een concrete verdenking in de zin van art. 27 Sv, 'concrete aanwijzingen' dat een WED-voorschrift is overtreden, is voldoende. Bovendien kan deze bevoegdheid worden ingezet tegen de verdachte. Dat alles maakt dat, net als de bevoegdheid van de Awr, de bevoegdheid van art. 19 WED zeer ruim toepasbaar lijkt, in ieder geval ruimer dan de bevoegdheden van de Wbvg (die niet mogen worden ingezet tegen de verdachte en waarbij sprake moet zijn van een verdenking). De enige beperking is dat het moet gaan om een economisch delict, dat is strafbaar gesteld in art. 1 en 1a WED.

4.7 Besluit

Voordat de Wbvg in werking trad, kende het Wetboek van Strafvordering al bevoegdheden tot het vorderen van verkeersgegevens en gebruikersgegevens van de aanbieders van openbare telecommunicatienetwerken en -diensten. De Wbvg voorziet in art. 126ng Sv en 126ug Sv ook in de bevoegdheid om (verkeers)gegevens te vorderen bij communicatiediensten. Verkeersgegevens en gebruikersgegevens kunnen niet via art. 126nc Sv, 126nd Sv, 126ne Sv of 126ng Sv worden gevorderd. Ook de gegevens die zijn opgeslagen in het geautomatiseerde werk van de aanbieder, maar die geen verkeers- of gebruikersgegevens zijn, zijn uitgezonderd. Het betreft hier bijvoorbeeld e-mails van de abonnees.

In de tweede plaats kunnen gegevens worden verkregen door toepassing van de bevoegdheden tot inbeslagneming van een voorwerp en tot het uitleveren van een voorwerp. De bevoegdheden tot inbeslagneming mogen niet worden gebruikt als volstaan kan worden met de lichtere bevoegdheden uit de Wbvg. Hier ligt echter wel een kiem van onduidelijkheid: wanneer een gegevenshouder originele stukken, bijvoorbeeld op papier, aanlevert op grond van een vordering ex de Wbvg, heeft de opsporingsinstantie deze dus eveneens ter beschikking, ofschoon ze niet in beslag zijn genomen.

In de derde plaats kunnen in het kader van het SFO gegevens worden gevorderd (art. 126a Sv). De bevoegdheden van de Wbvg bieden, behalve waar het gaat om art. 126ne Sv, geen nieuwe mogelijkheden in relatie tot een SFO.

Daarnaast biedt ook de Algemene wet bestuursrecht mogelijkheden om gegevens te vorderen die vallen onder de reikwijdte van de Wbvg. Toezichthouders kunnen op grond van art. 5:16, 5:17 en 5:20 Awb inlichtingen en inzage in zakelijke gegevens vorderen en eenieder verplichten alle medewerking te verlenen in het kader van de naleving van regelgeving. Art. 1:6 sub a Awb stelt echter dat de Awb niet van toepassing is op de opsporing en vervolging van strafbare feiten. In het licht van de wetsgeschiedenis is een toezichthouder niet bevoegd

langs bestuurlijke weg gegevens te vorderen als strafrechtelijke afdoening het uitsluitende doel is.

Tot slot is aandacht besteed aan enkele bijzondere wetten op grond waarvan gegevens kunnen worden verkregen. Zo kan een opsporingsmedewerker van de FIOD gebruikmaken van de bevoegdheid van art. 81 Awr. Dit artikel bepaalt dat de ambtenaren belast met het opsporen van bij de belastingwet strafbaar gestelde feiten, te allen tijde bevoegd zijn tot inbeslagneming van de ingevolge het Wetboek van Strafvordering voor inbeslagneming vatbare voorwerpen.[130] Zij kunnen daartoe hun uitlevering vorderen. In geval van verdenking van een economisch delict, biedt art. 19 WED aan opsporingsambtenaren de bevoegdheid gegevens en bescheiden in te zien en daarvan kopieën te maken.

[130] Zie art. 94 lid 1 Sv.

5 Het opsporingsproces in relatie tot de Wbvg

5.1 Inleiding

Elk opsporingsonderzoek is uniek en stelt derhalve eigen eisen aan de informatie die benodigd is om de bewijsvoering rond te krijgen. Toch zijn er ook grote lijnen te onderscheiden die op hun beurt gevolgen hebben voor het gebruik van de bevoegdheden uit de Wbvg. Voor een goed begrip van de uitkomsten die in de navolgende hoofdstukken 6-8 zullen worden gepresenteerd, is het dan ook aangewezen om eerst de organisatie en de uitvoering van het opsporingproces te schetsen. Uiteraard beperken we ons daarbij tot de hoofdlijnen.

In paragraaf 5.2 wordt, om te beginnen, zeer beknopt aandacht besteed aan de organisatie van het opsporingsproces en de rol die de verschillende partijen – het openbaar ministerie, de politie, de KMAR en de BOD'en daarin spelen. In paragraaf 5.3 komt aan de orde hoe een opsporingsonderzoek globaal verloopt. Hierin zullen ook enkele voorbeelden worden gegeven van zaken waarin vorderingen op grond van de Wbvg zijn gedaan, die in het kader van de onderhavige studie zijn bestudeerd in de verdiepende dossieranalyse. Paragraaf 5.4 besluit dit hoofdstuk.

5.2 De organisatie van het opsporingsproces

5.2.1 De rol van het openbaar ministerie

Het Nederlandse openbaar ministerie oefent, in de persoon van de officier van justitie, het gezag uit over concrete opsporingsonderzoeken. Deze is verantwoordelijk voor de dagelijkse leiding van het opsporingsonderzoek. Dit betekent (onder meer) dat hij aanwijzingen geeft aan de politie, en erover waakt dat de politie bij de opsporing de rechtsregels en de rechtsbeginselen in acht neemt.[131]

Daarnaast kan de officier van justitie bevelen dwangmiddelen toe te passen jegens een verdachte. In sommige gevallen, zoals ook in het kader van de Wbvg, heeft de officier van justitie daarbij voorafgaande toestemming van de rechter-commissaris nodig. Een officier van justitie is ook bevoegd in een strafzaak te vorderen dat de rechter-commissaris een Gerechtelijk Vooronderzoek (GVO) instelt. De ontwikkeling van de laatste jaren, waarin de officier van justitie steeds meer bevoegdheden gekregen heeft (bijvoorbeeld met betrekking tot

---

[131] Van Daele en Van Geebergen 2007, p. 137-138.

het bevelen van dwangmiddelen), heeft er echter voor gezorgd dat een GVO in steeds minder zaken wordt gevorderd.

5.2.2 De organisatie van de opsporing bij de politie

De Nederlandse politie is georganiseerd in 25 zelfstandige regionale politiekorpsen en, op nationaal niveau, het Korps Landelijke Politiediensten (KLPD). De politieregio's zijn in de regel nader verdeeld in districten, die op hun beurt een of meer basisteams omvatten.[132] Binnen deze structuur vindt op verschillende niveaus opsporingswerk plaats.

Op het laagste organisatorische niveau binnen de politie, het basisteam, wordt kleinschalig opsporingswerk verricht. Dit vormt doorgaans een onderdeel van de generale taakstelling van de (operationele) politiefunctionarissen: naast het recherchewerk vervullen zij ook andere taken, zoals het surveilleren op straat en het bieden van noodhulp. Het gaat bij het opsporingswerk op basisteamniveau dan ook om eenvoudige en niet-ernstige zaken, waaraan hooguit enkele dagen wordt gewerkt. Te denken valt bijvoorbeeld aan een eenvoudige diefstal of inbraak, of aan een vechtpartij waarbij het slachtoffer geen (ernstig) letsel heeft opgelopen. Wanneer de zaak niet binnen een kort tijdsbestek kan worden afgerond, of anderszins te complex blijkt te zijn om door een basisteam te worden behandeld, zal het onderzoek worden opgelegd, eventueel in afwachting van overdracht naar een rechercheteam dat over meer tijd en middelen beschikt.

Wanneer bijvoorbeeld binnen het werkgebied van een basisteam, of breder binnen een district of een politieregio, sprake is van een golf van gelijksoortige delicten, zoals woninginbraken, straatroven, inbraken in voertuigen, kan worden besloten een ad-hocrechercheteam op te richten. Zo'n team, dat doorgaans wordt samengesteld uit personeel dat afkomstig is van verschillende onderdelen van de organisatie, onder leiding van enkele meer ervaren rechercheurs, krijgt dan tot taak de seriematige daders of dadergroepen te identificeren en aan te houden. Wanneer de doelstelling, het terugbrengen van het aantal feiten in een bepaald gebied, gerealiseerd is, wordt het team weer opgeheven.

In het geval er sprake is van een ernstig feit, zoals een levensdelict of een ontvoering, wordt eveneens een ad-hocteam gevormd, een zogeheten Team Grootschalige Opsporing (TGO). Een dergelijk team zal in de eerste dagen nadat het feit is gepleegd veelal uit enkele tientallen politiemensen bestaan, die bij-

[132] Voor basisteams kunnen ook andere benamingen worden gehanteerd. De aard van de werkzaamheden die binnen een dergelijk team worden verricht, zijn over het algemeen echter gelijk.

voorbeeld uitgebreid buurtonderzoek verrichten en andere aanwijzingen natrekken. Na deze eerste fase wordt het TGO afgeschaald naar een kleinere omvang, al naargelang de hoeveelheid werk die voorhanden is. Wanneer verdachten zijn aangehouden en veroordeeld, houdt het team op te bestaan. Indien de zaak niet kan worden opgelost, kan het TGO op papier blijven voortbestaan. Indien nodig, bijvoorbeeld wanneer nieuwe informatie voorhanden komt, kan het weer worden gereactiveerd.

Behalve deze ad-hocrechercheteams beschikken de politieregio's ook over vaste rechercheteams, die bestaan uit gespecialiseerde rechercheurs. Om te beginnen houden districtsrecherches zich bezig met onderzoeken naar zware geweldsdelicten, met uitzondering van levensdelicten, en met opsporingsonderzoeken naar andere vormen van misdaad, zoals straatroven, seriematige vermogensdelicten en drugshandel. De opsporingsonderzoeken hebben in de regel een doorlooptijd van drie tot zes maanden.

Daarnaast doen de regionale recherches onderzoek naar de zwaarste vormen van criminaliteit in de politieregio. Doorgaans betreft het vormen van georganiseerde misdaad. Hierbij kan het gaan om onderzoek naar aanleiding van geconstateerde strafbare feiten, maar ook om planmatige, proactieve, opsporingsonderzoeken. Te denken valt aan een onderzoek naar een organisatie die verdovende middelen exporteert of produceert, waarover criminele inlichtingen zijn verkregen. Zulke opsporingsonderzoeken vergen in de regel al gauw een jaar recherchewerk en worden uitgevoerd door teams van ongeveer tien rechercheurs.

Bij de toedeling van opsporingsonderzoeken spelen niet alleen zwaartecriteria een rol, maar ook territoriale aspecten. Wanneer dezelfde daders strafbare feiten niet alleen in het werkgebied van een basisteam plegen, maar ook elders kan ervoor worden gekozen het onderzoek op het districtelijke niveau uit te laten voeren. Hetzelfde geldt, *mutatis mutandis*, voor zaken die de districtsgrenzen overschrijden. Indien een dadergroep bovendien in meerdere politieregio's actief is, kan het onderzoek worden toebedeeld aan de Bovenregionale Recherche (BR) of de Nationale Recherche (NR).

De NR is verantwoordelijk voor onderzoeken naar zware en georganiseerde misdaad met een nationale of internationale dimensie. De NR is onderdeel van het KLPD. De NR is onderverdeeld in units in verschillende delen van het land, maar de opsporingsonderzoeken die deze uitvoeren, zijn niet territoriaal gebonden.

Het takenpakket van de BR omvat regiogrensoverschrijdende opsporingsonderzoeken die qua ernst worden getypeerd als middencriminaliteit of als zware (georganiseerde) criminaliteit. Daarnaast houdt de BR zich bezig met onderzoeken naar zogenoemde 'horizontale' fraude, oftewel fraudes waarvan bur-

gers of bedrijven slachtoffer worden. [133] De BR heeft een sterkte van een procent van het personeel van de politieregio's en omvat zes territoriale eenheden.[134]

5.2.3 De opsporingstaken van de Koninklijke Marechaussee

Naast de politie heeft ook de Koninklijke Marechaussee (KMAR) een eigenstandige opsporingstaak. De KMAR maakt deel uit van het ministerie van Defensie. De marechaussee verricht in de eerste plaats de militaire politietaken. Dit betreft de politiezorg in relatie tot militaire installaties en personeel, zowel in Nederland als in het buitenland. Ook het eventuele recherchewerk dat daarbij noodzakelijk is, wordt door de KMAR verricht. In de tweede plaats is de marechaussee verantwoordelijk voor de politiezorg op de burgerluchthavens. En in de derde plaats behoort de uitvoering van het Mobiel Toezicht Vreemdelingen (MTV) aan de landsgrenzen tot het takenpakket. Daarbij gaat het primair om de controle op mensensmokkel en -handel.

5.2.4 De opsporingstaken van de Bijzondere Opsporingsdiensten

Tot slot kent Nederland vier BOD'en, die een eigenstandige (specialistische) opsporingstaak hebben. Deze opsporingsdiensten zijn op nationaal niveau georganiseerd en gedeconcentreerd over verschillende locaties in Nederland.

Om te beginnen doet de Fiscale Inlichtingen- en Opsporingsdienst Economische Controledienst (FIOD), onderzoek naar (verticale) fraudedelicten. Ook controles en opsporingsonderzoeken in het kader van de Wet Voorkoming Misbruik Chemicaliën (WVMC) behoort tot de verantwoordelijkheid van de FIOD. Deze dienst verricht, zo nodig, tevens nader opsporingsonderzoek naar strafbare feiten die door de Douane zijn vastgesteld. De FIOD ressorteert onder het ministerie van Financiën en bestaat in zijn huidige vorm sinds 1999.

In de tweede plaats is de Sociale Inlichtingen- en Opsporingsdienst (SIOD) verantwoordelijk voor de bestrijding van sociale fraude. Deze dienst valt onder het ministerie van Sociale Zaken en Werkgelegenheid. De SIOD is op 1 januari 2002 opgericht. De instantie verricht bijvoorbeeld onderzoek naar sociale fraude, malafide uitzendbureaus en illegale tewerkstelling.

---

[133] Het begrip 'verticale fraude' heeft betrekking op fraudes waarvan overheidsinstanties slachtoffer worden.

[134] Het gaat om de teams Zuid-Nederland, Noord- en Oost-Nederland, Noord-, Midden- en West-Nederland, Amsterdam, Rotterdam-Dordrecht en Haaglanden.

De derde BOD is de Algemene Inspectiedienst (AID), die viel onder het voormalige ministerie van Landbouw, Natuur en Voedselkwaliteit, en sinds oktober 2010 onder het ministerie van Economische Zaken, Landbouw en Innovatie. De AID verricht opsporingsonderzoeken in relatie tot natuur, milieu en de voedselveiligheid. Onderwerpen waar de dienst zich mee bezighoudt, zijn bijvoorbeeld dierenverwaarlozing, de naleving van de regels die aan de intensieve veehouderij zijn gesteld, en het gebruik van verboden groeihormonen. In 2008 rondde de AID in totaal 21 opsporingsonderzoeken af.[135] Het is voorgenomen dat de dienst per 1 januari 2012 zal opgaan in de fusieorganisatie Nieuwe Voedsel en Warenautoriteit (nVWA).

Tot slot richt de Inlichtingen- en Opsporingsdienst (IOD) zich op de veiligheid van de leefomgeving in brede zin. Daarbij kan worden gedacht aan de controle op afvaltransporten, en de opsporing van illegaal vuurwerk. Deze dienst viel tot oktober 2010 onder het ministerie van Volkshuisvesting, Ruimtelijke Ordening en Milieu (VROM) en thans onder het ministerie van Infrastructuur en Milieu.

Het zal geen verbazing wekken dat de bijzondere opsporingsdiensten, gezien hun specifieke takenpakket, een andersoortige informatiebehoefte kunnen hebben dan gemiddeld in een opsporingsonderzoek van de politie benodigd is. In een geval van fiscale fraude, bijvoorbeeld, spelen geldstromen een grote rol.[136] De FIOD is daarbij, zo blijkt uit interviews met functionarissen van deze dienst ten behoeve van de onderhavige evaluatie, 'grootverbruiker' van gegevens van banken en geldinstellingen. Het kan gaan om tientallen rekeningen en duizenden transacties waarover informatie wordt gevraagd.

Ook de SIOD rechercheert regelmatig, bijvoorbeeld in onderzoeken naar illegale arbeid, op financiële stromen, waarbij eveneens gegevens van banken en financiële instellingen een grote rol spelen. De AID en de IOD hebben bijvoorbeeld vaker dan andere opsporingsdiensten informatie nodig van bedrijven in de sectoren waar hun takenpakket zich op richt, zoals de visserijbranche of de transportbranche.

5.3 Uitvoering van opsporingsonderzoek

Strafbare feiten kunnen zich op verschillende manieren aandienen bij de opsporingsinstanties. Om te beginnen kan sprake zijn van strafbare feiten die onom-

135 AID 2008, p. 29.

136 Dat geldt overigens ook voor financieel-economische onderzoeken die door gespecialiseerde afdelingen binnen de politie worden verricht.

stotelijk hebben plaatsgevonden. Het is echter ook mogelijk dat er wel aanwijzingen zijn dat er strafbare feiten worden gepleegd, die voldoende zijn om tot verdenking te kunnen komen, maar dat de precieze aard en omvang van de illegale activiteiten nog niet duidelijk is.

In het eerste geval wordt het opsporingsonderzoek dat volgt, gedefinieerd als 'reactief'. Er is bijvoorbeeld een slachtoffer dat gewond is of erger; er is een inbraak gepleegd; er heeft zich een explosie voorgedaan in een laboratorium waar synthetische drugs werden vervaardigd; er is een zending beschermde dieren onderschept, enzovoort. De taak voor de opsporingsinstanties is in zo'n geval primair de gebeurtenissen die zich hebben afgespeeld te reconstrueren, de verdachten en hun rol te identificeren, en het bewijsmateriaal te verzamelen dat tot een veroordeling kan leiden.

In het tweede geval wordt gesproken van een 'proactief' opsporingsonderzoek. Informanten hebben bijvoorbeeld de politiefunctionarissen van de Criminele Inlichtingeneenheid (CIE) laten weten dat bepaalde personen bezig zijn met drugshandel, BTW-fraude of met het plegen van andere strafbare feiten. Die aanwijzingen kunnen ook afkomstig zijn uit het buitenland, wanneer bijvoorbeeld in een internationaal rechtshulpverzoek informatie wordt gevraagd omtrent personen die in Nederland bij de politie onbekend zijn, maar elders onderwerp van opsporingsonderzoek.

In de praktijk worden per politieregio jaarlijks maar een klein aantal proactieve opsporingsonderzoeken gestart. De regionale recherche voert in een gemiddelde politieregio jaarlijks 1 à 2 van dergelijke onderzoeken uit, die doorgaans ook een jaar, of langer, kosten om te worden gecompleteerd. Op districtsniveau kan eveneens sprake zijn van proactieve opsporingsonderzoeken, die meestal echter als reactief onderzoek beginnen. Het onderzoek kan bijvoorbeeld worden gestart op grond van gepleegde feiten, bijvoorbeeld een overval of een reeks inbraken, en dan een proactief karakter krijgen omdat het gaat om een dadergroep die nog altijd actief is met het plegen van misdrijven. De BR en de NR verrichten ook vooral proactieve opsporingsonderzoeken. Over het algemeen geldt echter dat het leeuwendeel van de door de politie uitgevoerde opsporingsonderzoeken reactief is.

5.3.1 Reactief opsporingsonderzoek

De praktijk van reactieve opsporingsonderzoeken is uitgebreid onderzocht door De Poot e.a. en in 2004 gepubliceerd in het boek Rechercheportret.[137] De navol-

[137] De Poot e.a. 2004.

gende bevindingen zijn dan ook voor een belangrijk deel aan dat werk ontleend. Het laat zien dat opsporingsinstanties kunnen kiezen uit een palet van methoden om bewijsmateriaal te verzamelen. De Poot e.a. hebben zeven clusters van opsporingsmethoden onderscheiden.[138]

Het eerste cluster is het getuigenonderzoek, waaronder bijvoorbeeld een buurt- of passantenonderzoek kunnen vallen.

Een tweede cluster is het technische onderzoek, waaronder bijvoorbeeld het nemen van foto's van de plaats delict of het veiligstellen van sporen kan vallen. Ook de doorzoeking van voertuigen of woningen wordt hieronder begrepen.

Het derde cluster dat De Poot e.a. identificeren, is politiekennis. Daaronder valt allerlei uiteenlopende informatie die reeds binnen de organisatie bekend is, op papier of in de hoofden van mensen, die bijvoorbeeld gaat over verdachten of locaties. Ook signalering, bijvoorbeeld van een gestolen voertuig, wordt hieronder geschaard.

In de vierde plaats kan de politie door middel van eigen acties bewijsmateriaal verzamelen. Een dader kan bijvoorbeeld op heterdaad worden aangehouden. Hieronder wordt ook begrepen het opvragen van gegevens van andere partijen, zoals historische gegevens van telefoon- en faxverkeer, maar ook van informatie waarop de Wbvg doelt.

Ten vijfde kunnen herkenningsmethoden als opsporingsmethode worden onderscheiden. Gangbaar in dit geval zijn bijvoorbeeld foto- of spiegelconfrontaties, maar het kan bijvoorbeeld ook gaan om geursorteerproeven of stemherkenning.

Ten zesde kan informatie worden verkregen van het slachtoffer, zoals een signalement van de dader of andere informatie die aanknopingspunten biedt waarop rechercheurs kunnen voortbouwen.

Tot slot wordt het verdachtenverhoor gezien als een afzonderlijk cluster van opsporingsmethoden.

Dit alles illustreert dat de politie, en hetzelfde geldt voor de andere opsporingsdiensten die in de vorige paragraaf werden beschreven, in principe over een breed palet van opsporingsmethoden beschikt. Welke methoden daadwerkelijk worden toegepast, is enerzijds afhankelijk van de zwaarte van het strafbare feit en anderzijds van de aard van de zaak en de keuzes van de betrokken opsporingsambtenaren. De Poot e.a. hebben ook daar nader onderzoek naar gedaan. Zij zijn in 814 dossiers van opsporingsonderzoeken nagegaan welke clusters van

138 De Poot e.a. 2004, p. 68-69.

opsporingsmethoden werden toegepast om het bewijsmateriaal te verzamelen.[139] Op grond daarvan komen zij tot een onderscheid in vier categorieën zaken.[140]

De eerste variant zijn *klip- en klaarzaken*, waarin de politie iemand op het heterdaad betrapt, waarin de verdachte zichzelf aangeeft, of waarin hij of zij direct kan worden aangehouden op of in de omgeving van de plaats delict. In zulke gevallen wordt het merendeel van het bewijsmateriaal door politieacties zelf gegenereerd. De politiefunctionarissen zijn in een situatie van heterdaad immers zelf waarnemer van het strafbare feit, verrichten de aanhouding en leggen dit alles vast in een proces-verbaal. Andere clusters van opsporingsmethoden die bij dit type zaak veel worden toegepast, zijn getuigenonderzoek (74% van de gevallen), informatie van het slachtoffer (52%) en technisch onderzoek (43%).

Het ligt voor de hand dat in klip en klaarzaken niet of nauwelijks behoefte is aan het vorderen van gegevens. Dat blijkt ook uit de 31 dossiers die in het kader van de onderhavige evaluatie diepgaander werden onderzocht: daarin kwamen situaties van heterdaad nauwelijks voor. Wel kunnen heterdaadzaken een vervolg krijgen. In een voorbeeld, waarin een overvaller op heterdaad werd betrapt, werden camerabeelden van andere voorvallen waarbij de dader op dezelfde wijze te werk was gegaan wederom bestudeerd om na te gaan of de aangehouden verdachte op die beelden te zien was. Deze camerabeelden waren echter reeds opgevraagd in de desbetreffende onderzoeken, en hoefden dus niet opnieuw te worden gevorderd.

De tweede categorie zaken die de makers van het boek *Rechercheportret* hebben onderscheiden, zijn *verificatiezaken*. In die gevallen is de identiteit van de verdachte bekend en tevens wat zich heeft afgespeeld. Daarvan is bijvoorbeeld sprake wanneer een slachtoffer aangifte doet en de (vermeende) dader daarbij kan noemen, zoals in een zaak van huiselijk geweld. Een andere mogelijkheid is dat een getuige deze informatie aanreikt. Bij dit type zaken is informatie van het slachtoffer het meest van belang (91%) alsmede ook getuigenonderzoek (72%). Acties van de politie zijn echter slechts in 14% van de gevallen nodig om het bewijsmateriaal te completeren.

In de casuïstiek in relatie tot de Wbvg komt dit type zaken met enige regelmaat naar voren. Een voorbeeld is een zaak waarin een medewerker van de klantenservice van een bedrijf verrekeningen ten voordele van klanten niet terugstortte, maar naar andere rekeningen overmaakte waarvan hij zelf de begunstigde was. Om de gang van zaken te bewijzen was, behalve het feit dat geldbe-

139 De Poot e.a. 2004, p. 82.
140 De Poot e.a. 2004, p. 50.

dragen verdwenen, ook informatie nodig van banken om te achterhalen naar welke rekeningen het verduisterde geld was overgemaakt, en op wiens naam die stonden. Aangezien de verdachte zo 'handig' was om voortdurend van rekening te wisselen, betroffen de verzoeken een fors aantal rekeningen.

Een ander voorbeeld van een verificatiezaak had betrekking op een vrouw die aangifte deed van mensenhandel en daarbij de naam van degene die haar tot prostitutie had gedwongen, kende. In dit geval werd door de politie allerlei uiteenlopende informatie opgevraagd waarmee het verhaal van de aangever kon worden gecontroleerd en de bewijsvoering onderbouwd. Zo werd bij een bordeel informatie gevorderd of de aangever daar inderdaad had gewerkt in de perioden waarover zij had verklaard. Zij vertelde ook over het feit dat het verdiende geld via *money transfers* en bepaalde bankrekeningen naar het buitenland was verzonden, respectievelijk overgemaakt. Om die reden werden bij de bewuste geldinstellingen vorderingen gedaan om dit te verifiëren. Ook allerlei andere informatie werd, uiteraard, nagetrokken, zoals historische verkeersgegevens van de telefoons waarvan gebruik was gemaakt om contact met de pooier te onderhouden.

In de derde plaats kan sprake zijn van een *opsporingszaak*. In zulke gevallen is wel bekend wat zich heeft afgespeeld, maar zijn het slachtoffer of getuigen niet bekend met de identiteit van de dader. In dergelijke zaken werd in 23% van de gevallen bewijsmateriaal verkregen door middel van eigen acties van de politie. Ook al aanwezige kennis binnen de politieorganisatie speelde een belangrijke rol (69%). Informatie van het slachtoffer (94%) en van getuigen (75%) waren wederom echter het meest belangrijk.

In de casuïstiek met betrekking tot de Wbvg blijkt het in opsporingszaken regelmatig te gaan om overvallen of straatroven. Bij een straatroof in de Amsterdamse binnenstad werden bijvoorbeeld beelden van een vijftal bedrijven gevorderd, waar camera's aan de gevel hingen die mogelijk ook de daders op hun vlucht hadden opgenomen.

Een ander voorbeeld betrof een woninginbraak die uitliep op een overval toen de bewoonster onverwacht thuiskwam. In plaats van op de vlucht te gaan, overweldigden de inbrekers de bewoner, bonden haar vast en maakten haar onder bedreiging met een pistool de pincodes van de bankpassen afhandig. Het slachtoffer wist zich korte tijd later te bevrijden en de politie te contacteren. In dit geval werd vanzelfsprekend het slachtoffer gehoord. Daarnaast werd uitgebreid forensisch onderzoek gedaan in de woning en in de buurt. Ook vond buurtonderzoek plaats waarbij een getuige werd gevonden die twee mannen uit de woning had zien komen en hen in een auto had zien wegrijden waarvan hij tevens het merk, de kleur en het kenteken kon noemen. Tijdens het onderzoek werd via een vordering aan de bank nagegaan of met de bankpas geld was opge-

nomen en waar dat was gebeurd. Vervolgens werden van die locaties camerabeelden opgevraagd.

In de vierde plaats kunnen *zoekzaken* worden onderscheiden. Hierin is niet (precies) bekend wat zich heeft afgespeeld en is evenmin bekend wie voor het strafbare feit verantwoordelijk is geweest. Dit kan aan de orde zijn wanneer een slachtoffer geen verklaring kan afleggen omtrent wat er is gebeurd, bijvoorbeeld omdat hij of zij is vermoord. In zoekzaken ligt de nadruk op getuigenonderzoek (78%) en politiekennis (76%), alsmede op technisch onderzoek (60%). Slechts in 24% van de gevallen volgden echter politieacties.

Een voorbeeld van een zoekzaak in de door ons bestudeerde dossiers was een geval waarin op straat een slachtoffer werd aangetroffen dat was neergeschoten en overleden. In de kleding van het slachtoffer werden attributen gevonden die iemand normaal gesproken altijd op zak heeft, zoals sleutels en een mobiele telefoon. Dit waren dan ook in eerste instantie de aanwijzingen waarop het opsporingsonderzoek zich richtte. Tevens werden camerabeelden gevorderd van bedrijven in de omgeving van de plaats waar de schietpartij had plaatsgevonden, om na te gaan of deze iets hadden geregistreerd. Dit leverde echter geen bruikbare informatie op. Uit het buurtonderzoek werd duidelijk dat het slachtoffer vlak bij de plaats delict woonde. Ook werd in de buurt de auto gevonden waarin het slachtoffer reed. De woning en de auto werden doorzocht, waaruit weer nieuwe aanknopingspunten naar voren kwamen, zoals over een verblijf in een hotel, over een *money transfer*, en over een bezoek aan een vestiging van Holland Casino. Ook hier werden gegevens gevorderd. Vervolgens werd uit informatie die reeds bij de politie voorhanden was, en uit gegevens die van buitenlandse politiediensten werd verkregen, duidelijk dat het slachtoffer zeer waarschijnlijk deel uitmaakte van een internationaal crimineel samenwerkingsverband dat bezig was met de import van verdovende middelen. De opsporing van een dergelijke dadergroep werd daarmee te complex voor het TGO. Het onderzoek werd dan ook tijdelijk gestaakt in afwachting van overname door een team van de regionale recherche of de NR.

Het is duidelijk dat een rechercheteam met name in zoekzaken niet altijd gemakkelijk nauw afgebakende gegevensvorderingen kan doen. In eerste instantie kan een verzoek om camerabeelden in de omgeving van de plaats delict bijvoorbeeld nog worden afgebakend tot een tijdsperiode waarin het strafbare feit waarschijnlijk is gepleegd. Het trekken van een grens omtrent welke camera's mogelijk iets van belang hebben vastgelegd, wordt hier echter al moeilijker. Ook voor andere informatie geldt dat hoe vager het gegeven is, hoe lastiger een tijdvak of een zoekvraag valt af te bakenen.

5.3.2 Proactief opsporingsonderzoek

Het startpunt van een proactief opsporingsonderzoek verschilt, zoals hiervoor werd beschreven, van dat van een reactief onderzoek. Het gaat hier bovendien niet om het leveren van het bewijs dat een bepaalde verdachte (mede)verantwoordelijk is geweest voor een voltooid delict dat ter kennis is gekomen van de politie, maar om het aantonen van betrokkenheid bij lopende strafbare feiten.

In een proactief opsporingsonderzoek wordt dus allereerst vooruitgekeken in plaats van achteruit. De politie beschikt bijvoorbeeld over informatie dat een bepaalde groepering bezig is met het produceren van synthetische drugs. De doelstelling van het onderzoek kan dan worden geformuleerd in termen van het vinden van de productielocatie en het leveren van het bewijs van de betrokkenheid van specifieke personen.[141] Wanneer een groep wordt verdacht van het illegaal exporteren van afval vanuit Nederland, is een logische doelstelling het volgen en onderscheppen van deze ladingen, eveneens in combinatie met het verzamelen van voldoende bewijsmateriaal om de verantwoordelijken succesvol te kunnen vervolgen.

Aangezien het bij een proactief onderzoek gaat om lopende of toekomstige gebeurtenissen spelen heimelijke opsporingsmethoden een wezenlijke rol.[142] In de Nederlandse context gaat het daarbij allereerst om het afluisteren van telefoons of andere communicatiehulpmiddelen, in de regel in combinatie met het (statisch en dynamisch) observeren van subjecten. Indien deze opsporingsbevoegdheden zonder resultaat blijven, kan worden gekozen voor het zwaarder geachte middel van 'opnemen van vertrouwelijke communicatie met een technisch hulpmiddel (OVC)' oftewel het installeren van opnameapparatuur in iemands voertuig, binnen bedrijfspanden waarvan hij gebruikmaakt, of zelfs,

---

141 Uiteraard bestaat ook de mogelijkheid dat een proactief en reactief onderzoek vermengd worden. Een voorbeeld is een zaak waarin een bankoverval werd gepleegd en waarin de politie, toen de vermoedelijke daders eenmaal waren geïdentificeerd, beoogde hen op heterdaad te betrappen wanneer zij een nieuw feit zouden plegen. Ook kan wisselwerking tussen een proactief opsporingsonderzoek en een reactief onderzoek ontstaan. Een voorbeeld hiervan is een zaak waarin een XTC-laboratorium van een groep die onderwerp was van een proactief opsporingsonderzoek explodeerde. Een ander rechercheteam voerde daarbij het onderzoek naar deze ontploffing uit.

142 Spapens 2006.

in incidentele gevallen, in iemands woning. Een andere optie is het organiseren van een pseudokoop of een infiltratietraject door een politiefunctionaris.[143]
Behalve deze bijzondere opsporingsbevoegdheden worden tijdens proactieve onderzoeken vanzelfsprekend ook andere dwangmiddelen toegepast. Wanneer er op heimelijke wijze voldoende bewijsmateriaal is verzameld om tot succesvolle vervolging te kunnen komen, worden aangehouden verdachten ook uitgebreid verhoord, vinden doorzoekingen plaats in woningen, bedrijfspanden of voertuigen en zo nodig ook forensisch onderzoek. Met de aanhouding van de verdachten is de heimelijke fase, waarin zij niet wisten dat zij onderwerp van opsporingsonderzoek waren, beëindigd.[144]

Zo nodig worden echter ook al tijdens de heimelijke fase van het opsporingsonderzoek gegevens verzameld door middel van niet-bijzondere opsporingsbevoegdheden. Dit gebeurt ten eerste om informatie die, bijvoorbeeld middels het aftappen van telefoons of observaties, is verkregen te kunnen onderbouwen of daaruit weer nieuwe aanknopingspunten te verkrijgen. Een voorbeeld is een observatieactie waarbij wordt gezien dat twee personen die onderwerp van opsporingsonderzoek zijn in een auto rijden, onderweg stoppen bij een benzinestation om te tanken en daarbij elektronisch betalen, vervolgens nog een stop maken bij een telefooncel om te telefoneren en daarna stoppen bij een hotel waar zij een ontmoeting hebben met twee andere personen. Na deze actie zou de politie bijvoorbeeld bij het benzinestation en het hotel camerabeelden kunnen opvragen – als het observatieteam die niet zelf al had kunnen maken – maar bijvoorbeeld ook een kopie van de geobserveerde transactie om rekeninggegevens te kunnen achterhalen, alsmede verkeersgegevens van de telefooncel om na te kunnen gaan met welk nummer is gebeld.

Op basis van informatie die is verkregen door middel van heimelijke opsporingsmethoden kunnen ook aanvullende gegevens worden gevorderd. Zo kan iemand aan de telefoon vertellen dat hij op een bepaald tijdstip een vlucht naar het buitenland heeft gemaakt, waarna bij de luchtvaartmaatschappij kan worden geverifieerd of hij inderdaad op de passagierslijst staat. Er kunnen uiteraard ook toekomstgerichte vorderingen worden gedaan, bijvoorbeeld wanneer bekend wordt dat iemand van plan is op een bepaalde datum naar een bepaalde bestemming te vliegen.

In de heimelijke fase van een proactief opsporingsonderzoek dient de integriteit van de gegevensverstrekker voortdurend in overweging te worden

---

143 Infiltratie door criminele burgers is in Nederland, behoudens uitzonderingsgevallen waarvoor de minister van Justitie persoonlijk toestemming moet verlenen, niet mogelijk.

144 Wat overigens niet verhindert dat zij daarmee wel rekening houden en afschermingsmaatregelen nemen. Zie Spapens 2006.

genomen. Zo kan bijvoorbeeld, als blijkt dat het kenteken van een voertuig waarin een subject rijdt op naam staat van een leasebedrijf, bij de desbetreffende firma worden nagegaan aan wie de auto is geleased, of via welke rekening de kosten worden betaald. De meeste zware criminelen leasen echter bij vage bedrijven, die ofwel eigendom zijn van collega-wetsovertreders, ofwel van personen die zelf geen strafbare feiten plegen, maar vanwege hun sociale relaties met misdadigers wel tot het criminele milieu kunnen worden gerekend. Een gegevensvordering zal dus onmiddellijk leiden tot een berichtje aan het subject in kwestie.

5.4 Besluit

In dit hoofdstuk is kort geschetst hoe de opsporing in Nederland is georganiseerd en op welke wijze een opsporingsonderzoek over het algemeen wordt uitgevoerd. Nederland kent verschillende opsporingsdiensten. Hoewel cijfers ontbreken, mag worden aangenomen dat de politie het leeuwendeel van het jaarlijkse aantal opsporingsonderzoeken uitvoert. Met name de BOD'en hebben, voortvloeiende uit hun specifieke taakvelden, een andersoortige informatiebehoefte dan de politie. Een goed voorbeeld is de FIOD, die op grote schaal gebruikmaakt van gegevens van banken en financiële instellingen. Deze informatiebehoefte wijkt, zo zal in het volgende hoofdstuk worden geschetst, af van die welke in een gemiddeld onderzoek van de politie benodigd is.

Een tweede belangrijk punt dat in dit hoofdstuk aan de orde is gesteld, betreft het feit dat het verzamelen van politiegegevens, waarvan vorderingen in het kader van de Wbvg bovendien slechts een onderdeel zijn, maar een van de methoden vormt waarmee de opsporingsinstanties bewijsmateriaal verzamelen. Hoogstens in een kwart van de gevallen worden politiegegevens, waarvan bij derden opgevraagde gegevens nog maar een onderdeel zijn, gebruikt als onderdeel van het opsporingsonderzoek. Daarbij moet tevens in aanmerking worden genomen dat bij reactieve opsporingsonderzoeken primair van belang is gebeurtenissen te reconstrueren die zich reeds hebben afgespeeld. Ook dit heeft dus gevolgen voor de toepassing van de Wbvg: er zal eerder terug dan vooruit worden gekeken. Wanneer, in een proactief opsporingsonderzoek, informatie wordt verzameld over illegale activiteiten die nog gaande zijn, is de kans dat toekomstige gegevens moeten worden gevorderd groter.

Vanzelfsprekend moet bij deze bevindingen in aanmerking worden genomen dat elk opsporingsonderzoek uniek is, en dus om specifieke opsporingsmethoden kan vragen. Het feit dat bijvoorbeeld Wbvg-vorderingen in sommige typen zaken gemiddeld minder aan de orde zijn, betekent dus nog niet dat zij in

een individueel geval niet essentieel en van doorslaggevende waarde kunnen zijn.

6 Het beroep op de Wbvg: omvang, aard en procedures

6.1 Inleiding

In dit hoofdstuk wordt een begin gemaakt met het presenteren van de uitkomsten van het empirische onderzoek naar de toepassing van de Wbvg. Navolgend wordt in paragraaf 6.2 allereerst ingegaan op het beroep dat opsporingsinstanties doen op de diverse onderdelen van de Wbvg. Vervolgens wordt besproken welke vragen precies werden gesteld en om welke gegevenshouder het ging.

In paragraaf 6.3 staat de procedure die de gegevensvragers hanteren bij het doen van vorderingen centraal. Daarbij wordt onderscheid gemaakt tussen de vorderingen 126nc Sv, die door opsporingsambtenaren kunnen worden gedaan, de vorderingen die vallen onder de bevoegdheid van de officier van justitie, en de vorderingen waarbij deze laatstgenoemde een machtiging van de rechter-commissaris nodig heeft.

Paragraaf 6.4 besluit dit hoofdstuk wederom met een kort overzicht van de bevindingen.

6.2 Het beroep op art. van de Wbvg

Zoals in hoofdstuk 1 al aangegeven, was het niet eenvoudig om een cijfermatig beeld te schetsen van de vorderingen die in het kader van de Wbvg worden gedaan. Slechts bij de FIOD bleken de vorderingen op grond van art. 126nc Sv centraal te worden bijgehouden in een computersysteem. Van deze instantie werden 138 vorderingen verkregen, hetgeen alle vastgelegde verzoeken betrof met betrekking tot 2008.

Op het niveau van de parketten konden op twee locaties – Den Bosch en Groningen – gegevens worden verkregen waarmee een cijfermatig beeld kan worden geschetst. Daarbij moet worden aangetekend dat bij het parket Den Bosch, waar het ging om de eenvoudige verzoeken, moest worden volstaan met een steekproef van 100 uit in totaal 932 Wbvg-vorderingen. De vorderingen die werden gedaan in het kader van TGO's en onderzoeken naar zware en georganiseerde misdaad, 185 in totaal, zijn wel alle bestudeerd. Gegeven deze beperkingen konden in totaal 739 vorderingen worden ingezien en geanalyseerd die bruikbaar waren voor het onderhavige onderzoek. In de volgende tabel is een overzicht opgenomen.

Tabel 6.1 Aantal onderzochte vorderingen

	Aantal vorderingen
Den Bosch	285
Groningen	316
FIOD	138
Totaal	**739**

6.2.1 Geregistreerde vorderingen per wetsartikel

In deze paragraaf wordt allereerst beschreven op welke artikelen van de Wbvg de vorderingen bij de parketten van Den Bosch en Groningen betrekking hadden. De vorderingen die werden gedaan door de FIOD, waarbij het zonder uitzondering ging om art. 126nc Sv, zijn hier buiten beschouwing gelaten. Op de inhoud van deze vorderingen wordt afzonderlijk ingegaan in paragraaf 6.2.4.

Tabel 6.2 Aantal vorderingen per Wbvg-artikel (2008)

	Aantal vorderingen	
	Aantal	**Percentage**
126nc Sv en 126uc Sv (identificerende gegevens)	17	3%
126nd Sv en 126ud Sv (andere dan identificerende gegevens, historisch)	578	96%
126ne Sv en 126ue Sv (andere dan identificerende gegevens, toekomstig)	3	0,5%
126nf Sv en 126uf Sv (gevoelige gegevens)	3	0,5%
126nh Sv en 126uh Sv (ontsleutelen van versleutelde gegevens)	0	0%
125i Sv (doorzoeking ter vastlegging van gegevens)	0	0%
Totaal	**601**	**100**

De tabel laat zien dat de Wbvg in de praktijk zeer selectief wordt toegepast. Vrijwel alle vorderingen (96%) betroffen verzoeken op grond van art. 126nd Sv. Daarop volgen de 126nc-vorderingen waarbij sprake is geweest van betrokkenheid van het parket. Deze vorderingen tellen formeel gezien echter niet mee,

aangezien ze niet door een officier van justitie worden gedaan, maar door een 'gewone' opsporingsambtenaar. Ze werden slechts bij het parket geregistreerd omdat ze tegelijkertijd werden gedaan met een ander verzoek op grond van de Wbvg.

Deze uitkomsten illustreren dat in een gemiddeld opsporingsonderzoek de toepassing van andere dan identificerende en historische gegevens zelden nodig is. Dat wordt enerzijds verklaard door de aard van de meeste opsporingsonderzoeken. Het gaat, zoals uiteengezet in het vorige hoofdstuk, veelal om reactieve onderzoeken waarbij gebeurtenissen die zich hebben afgespeeld achteraf worden gereconstrueerd, en derhalve doorgaans alleen historische gegevens in het geding zijn. Een bevoegdheid als art. 126ne Sv, die ziet op toekomstige gegevens, is vooral van belang voor proactieve opsporingsonderzoeken, die getalsmatig echter minder vaak voorkomen.[145] De bevoegdheid wordt bijvoorbeeld gebruikt om informatie te verkrijgen over nieuwe transacties via bepaalde bankrekeningen, of om op de hoogte te worden gesteld, waar en wanneer een (gestolen) pinpas of creditcard wordt gebruikt.

Anderzijds zijn praktische omstandigheden aan de orde. De politie maakt in opsporingsonderzoeken bijvoorbeeld zelden gebruik van art. 125i Sv, zo blijkt uit afgenomen interviews, aangezien het eenvoudiger is de gegevensdrager in beslag te nemen en op het bureau door specialisten, die ter plekke over de benodigde apparatuur beschikken, verder te laten onderzoeken. Het is niet altijd mogelijk om degenen met de juiste expertise mee te nemen bij doorzoekingen, terwijl zij dan tevens niet beschikken over de juiste technische hulpmiddelen. Indien iemand zijn computer niet lang kan missen, wordt deze bijvoorbeeld 's ochtends in beslag genomen en, nadat een kopie van de harde schijf is gemaakt, 's middags weer teruggegeven. Slechts in onderzoeken door de FIOD blijkt art. 125i Sv soms een nuttig hulpmiddel, aangezien de dienst regelmatig ook bij bedrijven ter plekke onderzoek doet. Indien een firma gevestigd is in een bedrijfsverzamelgebouw bestaat de mogelijkheid dat gebruik wordt gemaakt van een computerserver, waarop de verschillende bedrijven elk ruimte huren. Het zou dan disproportioneel zijn de hele server in beslag te nemen, aangezien daarmee direct alle firma's in een dergelijk gebouw zouden worden gedupeerd.

---

[145] De mogelijkheid bestaat vanzelfsprekend, zoals hiervoor al werd aangeduid, dat een onderzoek dat als reactief is gestart, verandert in proactief, bijvoorbeeld als blijkt dat een verdachte betrokken is bij lopende illegale activiteiten.

Tabel 6.3 Aantal vorderingen per parket, per Wbvg-artikel (2008)

	Den Bosch		**Groningen**	
	Aantal	**Percentage**	**Aantal**	**Percentage**
126nc Sv en 126uc Sv	0	0%	17	5%
126nd Sv en 126ud Sv	281	99%	297	94%
126ne Sv en 126ue Sv	2	0,4%	1	0.3%
126nf Sv en 126uf Sv	2	0,4%	1	0.3%
Totaal	**285**	**100%**	**316**	**100%**

Wanneer de cijfers met betrekking tot de twee onderzochte parketten nader onder de loep worden genomen, blijkt dat het beeld in Den Bosch en Groningen niet verschilt. Bij beide parketten heeft het overgrote deel van de vorderingen betrekking op art. 126nd Sv.[146]

Hoewel hier slechts sprake is van een maar zeer beperkt representatieve steekproef, wordt het beeld uit de tabel bevestigd door de cijfers die van het parket Amsterdam werden verkregen en door gesprekken met officieren van justitie. In het tijdvak van september 2009 tot januari 2010 registreerde de BOB-administratie in Amsterdam (exclusief de zaken van de regionale recherche) geen enkele Wbvg-vordering anders dan op grond van art. 126nd. Ook de geïnterviewde officieren van justitie geven aan dat zij niet of slechts zeer sporadisch gebruikmaken van de andere wetsartikelen. Zij verwachten overigens wel dat het aantal vorderingen inzake art. 126nf Sv zal toenemen, vanwege het in hoofdstuk 3 besproken Trans Link-arrest. Ook dat kan in de toekomstige praktijk echter meevallen, aangezien die uitspraak is genuanceerd door nieuwe jurisprudentie.

Wanneer wordt nagegaan door wie de aanvraag is gedaan, blijkt dat, conform de vereisten van de Wbvg, de aanvrager in alle gevallen de officier van justitie is. Bij de drie vorderingen waarin dat noodzakelijk was, heeft de officier van justitie een machtiging verkregen van de rechter-commissaris. Deze vorderingen betroffen alle art. 126nf Sv (gevoelige gegevens). Er zijn geen vorderingen op basis van dit artikel gedaan *zonder* machtiging van de rechter-commissaris.

[146] De onderzoekers hebben beide parketten verzocht in het administratiesysteem na te gaan of er andere vorderingen waren gedaan dan op grond van art. 126nd Sv. De zes vorderingen die geen betrekking hadden op het voornoemde artikel zijn bij deze parketten dan ook de enige die in 2008 werden gedaan.

Tabel 6.4 Aantal vragen per vordering (excl. FIOD)

	Aantal vorderingen	
Aantal vragen per vordering	**Aantal**	**Percentage**
1	416	69%
2	96	16%
3	41	7%
4	25	4%
5	10	2%
6 of meer	13	2%
Totaal	**601**	**100%**

Tabel 6.4 laat zien dat een vordering aan een gegevenshouder niet beperkt hoeft te blijven tot een type gegevens. In 31% van de gevallen zijn dan ook meerdere vragen tegelijkertijd gesteld. Aan elke afzonderlijke gegevenshouder dient vanzelfsprekend wel een aparte vordering te worden gedaan. Er moet in de praktijk bij het stellen van meerdere vragen tegelijk vooral worden gedacht aan informatie over diverse rekeningnummers of cliënten van een en dezelfde bank of financiële instelling. Er is geen verschil gevonden tussen de drie onderzochte instanties ten aanzien van het aantal gegevens dat men per vordering opvraagt.

De tabel illustreert de weerbarstigheid van de praktijk bij het registreren van vorderingen. Bij het opstellen van de Wbvg heeft de wetgever hierom, begrijpelijkerwijs, verzocht om zicht te kunnen houden op de mate waarin de wet, met zijn gevoeligheden, wordt toegepast door de opsporingsinstanties. Nadere richtlijnen omtrent hoe te registreren zijn echter niet gegeven. Goed inzicht ontbreekt dan ook niet alleen bij gebrek aan een centrale registratie bij de opsporingsinstanties, maar ook omdat per vordering niet een, maar meerdere verzoeken tegelijkertijd kunnen worden gedaan.

Ook dan zijn de registratieproblemen nog niet voorbij: tijdens het dossieronderzoek werd duidelijk dat vorderingen door gegevenshouders ook met enige regelmaat – een voorzichtige schatting is dat het gaat om zo'n 5 procent van de gevallen – worden teruggestuurd. De belangrijkste redenen zijn dat ze niet juist zijn geadresseerd, of dat de officier van justitie wel heeft getekend, maar vergeten is zijn of haar naam leesbaar te vermelden. De adressering is bijvoorbeeld onjuist omdat een dochteronderneming verwijst naar het hoofdkantoor, of andersom. Een ander voorbeeld is de Rabobank die, omdat het om een

coöperatieve bank gaat, vereist dat de vordering specifiek wordt geadresseerd aan de vestiging waarop deze betrekking heeft.[147] Uit registratieoogpunt kan men zich echter afvragen of een vordering die opnieuw moet worden gedaan ook tweemaal moet worden geteld.

6.2.2 De aard van de gevraagde gegevens

Het volgende onderwerp van onderzoek betrof de vraag welke gegevens precies worden gevorderd. In de 601 bij de parketten Den Bosch en Groningen bestudeerde vorderingen ging het in totaal om 828 verschillende vragen, waarvan de aard sterk uiteenliep. Ten behoeve van de dossierstudie is dan ook een codeboek aangelegd van de gevraagde gegevens. Daarin zijn in totaal 232 codes geïdentificeerd, die variëren van concreet tot meer algemeen.

Voorbeelden van afgebakende vragen zijn Naam-adres-woonplaatsgegevens (NAW), zoals die welke behoren bij een rekeningnummer, een verzoek om een kopie van een legitimatiebewijs, een vraag vanaf welke datum bepaalde personen gemachtigd zijn tot een rekeningnummer, een verzoek om identificatie van een medepassagier bij een vliegreis, en het opvragen van de camerabeelden van specifieke pintransacties. Minder concrete omschrijvingen komen echter ook voor. Voorbeelden daarvan zijn vragen naar het arbeidsverleden van een verdachte, een verzoek om alle bij de Belastingdienst bekende en geregistreerde gegevens omtrent de fiscale en financiële situatie van een bepaalde persoon of met betrekking tot een bepaalde periode, een vraag om alle bekende gegevens omtrent de verkoop van mobiele telefoons en providers, en de afgegeven telefoonnummers en IMEI-nummers, een vordering om ‘uitkeringsgegevens’, een verzoek om persoonsgegevens en alle andere aanwezige gegevens of een ‘totaaloverzicht van het klantbeeld’.

Van de nauwkeurige omschrijvingen waar de opstellers van de Wbvg aan dachten, is derhalve lang niet altijd sprake. Daarbij moet uiteraard wel in het oog worden gehouden dat het stellen van welbepaalde vragen slechts dan mogelijk is wanneer de opsporingsinstanties enerzijds een nauwkeurig idee hebben van de benodigde gegevens, en anderzijds ook weet moeten hebben van de precieze informatie die bij de gegevenshouder beschikbaar is. Zoals in hoofdstuk 5 werd beschreven, ontbreekt vooral in *zoekzaken* zulke contextuele informatie nogal eens.

---

147 De vorderingen worden door de Rabobank overigens wel centraal afgehandeld.

Tabel 6.5 biedt een overzicht van het aantal maal dat gegevens zijn gevorderd, per categorie. Ten behoeve van de overzichtelijkheid zijn de 232 codes daarin tot dertien categorieën teruggebracht.

Tabel 6.5 Aard van de gevorderde gegevens, per categorie

	Vorderingen	
Categorie van gegevens	**N**	**%**
Financieel	353	43%
Camerabeelden	237	29%
Telefonie[148]	52	6%
Onroerend goed	29	4%
Digitaal	30	4%
Verkeer	25	3%
Arbeidssituatie	21	3%
Gevoelige gegevens	5	1%
Consument	12	1%
Onderneming	10	1%
Detentie	11	1%
Casino	8	1%
Overig	35	4%
Totaal	**828**	**100%**

De tabel laat zien dat financiële informatie, met 43 procent, verreweg het meest wordt gevorderd. Daarop volgen camerabeelden, met 29 procent. Samen bestrijken deze twee categorieën derhalve 72 procent van de gevorderde gegevens. De overige clusters van vragen komen beduidend minder vaak voor in de onderzochte dossiers. Bovendien lijkt ten aanzien van gegevens in de categorie 'telefonie' niet altijd helder of het wel gaat om een vordering op grond van de Wbvg. Voorbeelden die daar wel toe kunnen worden gerekend, zijn een vraag naar hoe een klant zijn beltegoed opwaardeert, of een vraag om een gemaakte bandopname van een telefoongesprek door een callcenter.

Deze gegevens zijn eveneens per onderzocht parket bekeken, zoals de navolgende tabel toont.

[148] Voorbeelden van vorderingen in deze categorie zijn vragen naar hoe een klant zijn beltegoed opwaardeert, een vraag om een gemaakte bandopname van een telefoongesprek door een callcenter, of mastverkeergegevens over een bepaalde periode.

Tabel 6.6 Categorieën van gevorderde gegevens per parket

	Den Bosch		**Groningen**	
	N	**%**	**N**	**%**
Financieel	140	37%	213	48%
Camerabeelden	135	35%	102	23%
Telefonie	19	5%	33	7%
Onroerend goed	18	5%	11	2%
Verkeer	14	4%	11	2%
Arbeidssituatie	15	4%	6	1%
Digitaal	1	0%	29	6%
Gevoelige gegevens	2	1%	3	1%
Consument	6	2%	6	1%
Onderneming	8	2%	2	0%
Detentie	2	1%	9	2%
Casino	0	0%	8	2%
Overig	21	5%	14	3%
Totaal	**381**	**100%**	**447**	**100%**

Tabel 6.6 laat zien dat de vorderingen die door de parketten Den Bosch en Groningen werden gedaan inhoudelijk niet wezenlijk van elkaar verschillen. Financiële gegevens en camerabeelden zijn in beide arrondissementen het belangrijkst. In Groningen werden verhoudingsgewijs meer financiële gegevens gevorderd, terwijl het in Den Bosch vaker om camerabeelden ging. Een opmerkelijk verschil tussen beide parketten is wel dat in Groningen vaker gegevens werden gevorderd in de categorie 'digitaal'.[149]

6.2.3 De geadresseerde gegevenshouders

De laatste vraag die in het cijfermatige deel van de evaluatie van de Wbvg centraal stond, is aan welke gegevenshouders de vorderingen worden geadresseerd. Ook hier was sprake van een veelheid van instanties, die nader zijn gecategori-

[149] Deze categorie omvat onder meer aanvragen omtrent emailadressen (zoals 'al het mailverkeer behorend bij een mailadres'), IP-adressen (bijvoorbeeld: 'het IP-adres van de pc waarmee bepaalde overboekingen hebben plaatsgevonden, alsmede de datum en het tijdstip van het meekrijgen van het IP-adres'), advertenties die op internet zijn geplaatst, en 'alle opgeslagen hyvesberichten, krabbels, chats van een hyves-contact'.

seerd. In tabel 6.7 wordt allereerst een algemeen overzicht geboden van de door de onderzochte instanties aangezochte gegevenshouders.

Tabel 6.7 Geadresseerde gegevenshouders per categorie, parketten

	Vorderingen	
Categorie van gegevenshouders	**N**	**%**
Financiële instelling	346	58%
Overheidsinstantie	69	12%
Detailhandel / Horeca	51	9%
Telecombedrijf	29	5%
Tankstation	29	5%
Zakelijke dienstverlening	32	5%
OV / Luchtvaart	22	4%
Camerabedrijf	8	1%
Overig	10	2%
Totaal	**596***	**100%**

* Bij 5 vorderingen was de gegevenshouder onbekend.

De tabel laat zien dat banken en andere financiële instellingen het leeuwendeel van de vorderingen in het kader van de Wbvg te verwerken krijgen. Andere relatief vaak voorkomende geadresseerden zijn overheidsinstanties (12%) en detailhandels- of horecaondernemingen (9%). Bij overheidsinstanties gaat het bijvoorbeeld om door de politie gevorderde gegevens van de belastingdienst, gemeenten of de UWV.

6.2.4 Identificerende gegevens

In deze subparagraaf wordt kort nader ingegaan op de vorderingen die in 2008 door de FIOD werden gedaan op grond van art. 126nc Sv. Zoals vermeld zijn 134 geregistreerde vorderingen nader geanalyseerd. Daarin werden 284 verschillende gegevens gevorderd. De volgende tabel laat zien om welke vragen het ging.

Tabel 6.8 Overzicht van vorderingen op basis van art. 126nc Sv (FIOD, 2008)

	Aantal vorderingen	
Categorie van gegevens	**Aantal**	**Percentage**
NAW-gegevens	89	31%
Geboortedatum en/of geslacht	34	12%
Administratieve kenmerken algemeen	23	8%
Bankpasnummer	4	1%
Bankrekeningnummer	39	14%
Andere administratieve kenmerken	5	2%
Rechtspersoon: rechtsvorm en vestigingsplaats	20	7%
Tenaamstelling rekeningnummer	6	2%
Gemachtigden rekeningnummer	10	4%
Zorgverzekeraar van een subject of informatie over verzekeringsproducten	10	4%
Telefoonnummer	7	2%
Informatie over huur kraam/box/kluis	12	4%
Foto en/of paspoort of rijbewijsgegevens	5	2%
E-mailadres/IP-adres gebruikt voor reservering	5	2%
Overige financiële gegevens	9	3%
Overige vragen	6	2%
Totaal	**284**	**100%**

De FIOD vorderde in 2008 op grond van art. 126nc Sv informatie over een breed scala aan onderwerpen. Het meest werden NAW-gegevens (31%) gevorderd, gevolgd door een verzoek om iemands bankrekeningnummer te achterhalen (14%). Een vraag om iemands geboortedatum en/of geslacht kwam met 12% eveneens relatief vaak voor. Het merendeel van de vragen had betrekking op natuurlijke personen (93%).

De FIOD stelde slechts in 7% van de vorderingen vragen betreffende rechtspersonen. Dit lage percentage valt echter te verklaren door het feit dat de dienst daartoe, als onderdeel van de Belastingdienst, doorgaans al directe toegang heeft, met inbegrip van gegevens van de Kamer van Koophandel. Politiekorpsen of andere BOD'en zullen dat type gegevens dus naar verwachting vaker via vorderingen in bezit moeten krijgen.

Een belangrijke vraag in het onderhavige onderzoek is of het onderscheid tussen gegevens die op basis van art. 126nc Sv kunnen worden gevorderd en informatie die op grond van andere wetsartikelen van de Wbvg moet worden verkregen, duidelijk is.

Zoals in hoofdstuk 3 werd beschreven, heeft de wetgever enerzijds een limitatieve opsomming gegeven van de gegevens die onder art. 126nc Sv vallen. Dat zijn: naam, adres, woonplaats, geboortedatum, geslacht en administratieve kenmerken. Als de identificerende gegevens betrekking hebben op een rechtspersoon, zijn daaronder begrepen de gegevens betreffende de rechtsvorm en de vestigingsplaats van de rechtspersoon. Anderzijds wordt ruimte gelaten voor interpretatie waar het gaat om administratieve kenmerken, die zijn gedefinieerd als 'de kenmerken waaronder een persoon bij de derde bekend is'. Hieronder vallen *bijvoorbeeld* (onze cursivering) een klantnummer, een nummer van een polis, of een lidmaatschapsnummer. Ook een nummer of een code met behulp waarvan een persoon toegang heeft tot een dienst kan ertoe worden gerekend.[150]

De hier uitgevoerde analyse wijst uit dat 82% van de onderzochte vorderingen zonder meer binnen de kaders valt die door de wetgever zijn aangegeven. Bij 18% van de vorderingen kan daarover echter discussie worden gevoerd. Zo werd in 4% van de vorderingen gevraagd bij welke zorgverzekeraar een subject was ondergebracht, dan wel of deze gebruikmaakte van een bepaald verzekeringsproduct (3%), hetgeen eigenlijk een vordering op grond van art. 126nd Sv zou moeten vergen.

Andere vragen hadden betrekking op een tijdvak waarin actief gebruik was gemaakt van een bankrekening of waarin een kluis of een opslagbox was gehuurd. In 2% van de gevallen werd informatie gevraagd over welk telefoonnummer iemand gebruikte, en in even zovele gevallen van welk e-mailadres of een IP-adres een klant gebruikmaakte. Wanneer de vorderingen nader worden bezien, blijkt dat deze vaak in combinatie met NAW-gegevens worden gevraagd. Bij een zorgverzekeraar werd bijvoorbeeld iemands naam, adres, woonplaats, postadres, telefoonnummer en GSM-nummer in een vordering opgevraagd. Bij een telefoonnummer dat in deze context wordt gevorderd, gaat het weliswaar eveneens om identificerende gegevens, maar formeel zou dat gegeven via art. 126nd Sv moeten worden gevorderd.

6.3 Procedures in relatie tot de Wbvg

In deze paragraaf komen de procedures aan de orde die worden gehanteerd bij de onderzochte politieregio's en bij de FIOD, respectievelijk de controle op de vorderingen die wordt uitgevoerd bij de parketten. De hier gepresenteerde bevindingen zijn enerzijds gebaseerd op interviews met medewerkers van het

[150] *Kamerstukken II* 2003/04, 29 441, nr. 6, p. 12.

openbaar ministerie, maar anderzijds ook op de verdiepende analyse van een dertigtal dossiers waarin vorderingen op grond van de Wbvg zijn gedaan.[151]

6.3.1 Vorderingen door de politie en de BOD'en

De onderzochte politiekorpsen blijken de procedure in het kader van art. 126nc Sv op verschillende wijze te hebben georganiseerd. In het korps Amsterdam-Amstelland bijvoorbeeld zijn alleen hulpofficieren van justitie geautoriseerd om deze vorderingen te doen. In andere korpsen worden echter ook wel andere procedures gevolgd. Aldaar mogen opsporingsambtenaren bijvoorbeeld in principe de vorderingen zelfstandig doen, tenzij het gaat om een verzoek dat gericht is aan een bank- of geldinstelling. In dat geval moet de vordering door een hulpofficier van justitie worden gedaan.[152] Bij de FIOD kan daarentegen elke opsporingsambtenaar vorderingen op grond van art. 126nc Sv zelfstandig doen, overigens wel nadat overleg met een hulpofficier heeft plaatsgevonden ter toetsing.

Vervolgens stelt de opsporingsambtenaar een zogeheten 'aanvraag proces-verbaal' op. In de politieregio Amsterdam-Amstelland wordt bijvoorbeeld gewerkt met standaardformulieren (in MSWord), per wetsartikel van de Wbvg, waarin de onderwerpen zijn aangeduid die in de aanvraag aan de orde moeten komen.[153] Het gaat daarbij om een korte beschrijving van het opsporingsonderzoek en de feiten die zich hebben voorgedaan, de reden waarom bepaalde gegevens worden gevorderd en de informatie die van de derde partij wordt gevraagd. Eventueel wordt vooraf contact opgenomen met de gegevenshouder om na te gaan of bepaalde informatie, via de 'ja/nee-vragen' voorhanden is.

Dit verbaal wordt naar de hulpofficier van justitie gestuurd die de vordering controleert en uitstuurt naar de gegevensverstrekker. Vanzelfsprekend ontvangt de gegevenshouder niet het aanvraag-PV, maar een aparte brief waarin alleen staat welke informatie wordt gevorderd. Na ontvangst van de gegevens stelt de opsporingsmedewerker een proces-verbaal van ontvangst op en verant-

---

151 Zie paragraaf 1.3.2. Dit betekent dat de inrichting van de procedures bij opsporingsdiensten of parketten waarvan geen vertegenwoordigers zijn geïnterviewd anders kan zijn.

152 In de Aanwijzing gegevensverstrekking financiële dienstverleners (2004A002) staat de procedure als volgt omschreven: 'In geval van een vordering verstrekking identificerende gegevens zoals neergelegd in art. 126nc/uc Sv, en in geval van de vorderingen op grond van de bijzondere wetten, toetst de hulpofficier van justitie de voorgenomen vordering op proportionaliteit en subsidiariteit. Hierna wordt de vordering schriftelijk gedaan door de hulpofficier van justitie via de infodesk.'

153 Zulke sjablonen zijn overigens ook opgenomen in het 'Handboek BOB'.

woordt hij of zij schriftelijk welke van de ontvangen gegevens relevant worden geacht in het kader van het opsporingsonderzoek.

Indien een beroep moet worden gedaan op een van de andere artikelen van de Wbvg is de werkwijze vergelijkbaar. Sommige geïnterviewden geven aan dat voordat het aanvraag-PV wordt opgesteld, de recherchemedewerker eerst een gesprek voert met de officier van justitie. Dat kan een zaaksofficier zijn, of een officier van de weekdienst. In dat gesprek komt aan de orde welke bevoegdheid zal worden ingezet, wie de vermoedelijke houder van de gegevens is en hoe de formulering van de vordering zal moeten zijn (inclusief het vaststellen van een zo afgebakend mogelijke tijdsperiode waarop de vordering betrekking heeft).

De volgende stap in de procedure is de verzending van het aanvraag-PV naar het openbaar ministerie. Deze stuurt, na controle en goedkeuring van de aanvraag, de feitelijke vordering uit naar de gegevenshouder (zie paragraaf 6.3.2).

De gegevenshouder levert de informatie vervolgens uit aan de recherchemedewerker, die van het ontvangen van de gegevens proces-verbaal opmaakt en een schriftelijke verantwoording toevoegt over het gebruik van de informatie in het opsporingsonderzoek. Een respondent van de politie Brabant-Noord legt de interne gang van zaken uit: ‘Er is maar een aantal politiemedewerkers bevoegd om gegevens te vorderen. Bij 126nd Sv is dat de hulpofficier van justitie, en een aantal medewerkers van de Infodesk.’

In geval van spoed is het mogelijk de gegevens uit te leveren zonder voorafgaande vordering. ‘Dan werkt [de gegevenshouder] gewoon goed mee door de gegevens uit te leveren en dan komt de vordering na afloop’, aldus een respondent van de politie Brabant-Noord. Dezelfde praktijk van mondelinge vorderingen in spoedgevallen wordt ook door de andere respondenten vermeld.

6.3.2 De werkwijze op de parketten

Bij de parketten verloopt de controle op de vordering in twee of, als de rechter-commissaris ook betrokken is, drie stappen.

Om te beginnen wordt het aanvraag-PV gecontroleerd door een parketsecretaris die zich bezighoudt met zaken die bijzondere opsporingsbevoegdheden betreffen. In de eerste plaats worden de juridische vereisten gecontroleerd: is er sprake van verdenking van een strafbaar feit waarvoor voorlopige hechtenis is toegestaan, waarop is de verdenking gestoeld, en is het juiste artikellid (de juiste grondslag) toegepast? In de tweede plaats wordt de aanvraag inhoudelijk beoordeeld: zijn de gegevens die gevraagd worden voldoende specifiek omschreven, is de tijdsperiode waarover de gegevens worden gevorderd, voldoende

nauwkeurig afgebakend, welke informatie wordt gevraagd, en is dit het juiste middel om succes te behalen? Ook wordt een kosten/baten-afweging gemaakt, omdat met het vorderen van gegevens kosten gemoeid zijn.[154]

Indien de parketsecretaris de aanvraag accordeert, maken de administratieve medewerkers van de zogeheten 'BOB-kamer' een brief op aan de gegevenshouder, waarin wordt gesteld welke informatie wordt gevraagd. Bij het parket Amsterdam-Amstelland wordt per afzonderlijk artikel van de Wbvg gewerkt met sjablonen waarin ook precies de voorwaarden zijn omschreven die per wetsartikel gelden.

De standaardbrief, met het aanvraag-PV, gaat vervolgens naar de officier van justitie die tekent. De feitelijke ondertekenaar van de vordering hoeft niet per se de zaaksofficier te zijn. Indien deze afwezig is, kan in principe elke willekeurige collega een handtekening zetten. Veel vorderingen zijn eenvoudig, waardoor de inhoudelijke *screening* door de parketsecretaris kan volstaan. Naarmate de aanvragen complexer worden, neemt uiteraard de zorgvuldigheid van de beoordeling door de zaaksofficier van justitie toe. Een respondent van het FP geeft bijvoorbeeld aan de vorderingen om die reden altijd zelf te controleren en ze bovendien ook zelf op te stellen.

De toetsing wordt door het openbaar ministerie serieus genomen, en de opsporingsdiensten 'passeren het openbaar ministerie niet', aldus een van de Groningse officieren van justitie. Vaak kan de toetsing evenwel min of meer parallel lopen met het indienen van het aanvraag-PV, omdat door het openbaar ministerie en de opsporingsdienst nauw wordt samengewerkt in een zaak. Volgens een van de parketsecretarissen '[leert de praktijk] dat we, de politie en ik, simultaan zitten te typen'. Het komt, zoals al is aangegeven, voor dat gegevens mondeling worden gevorderd; de Wbvg biedt daartoe ook de mogelijkheid. De vordering dient dan wel achteraf, binnen drie dagen, alsnog te volgen. Volgens de respondenten gebeurt dit ook.

Indien de rechter-commissaris moet worden ingeschakeld, is de procedure vergelijkbaar. De aanvraag gaat dan vanuit de BOB-kamer eerst naar de rechter-commissaris, waarbij het doorgaans ook degene betreft die op een bepaalde dag aanwezig en beschikbaar is, en dus niet noodzakelijkerwijs een RC die de zaak inhoudelijk al kent.

De BOB-kamer houdt bij welke vorderingen zijn gedaan. Die worden op papier bewaard, met de andere relevante machtigingen (zoals die van tele-

---

[154] Zie de Aanwijzing gegevensverstrekking financiële dienstverleners (2004A002), *Stcrt.* 2004, 95. De vergoedingsregeling is €10,- per identificerend gegeven en in de overige gevallen €70,- per uur voor de tijd die gemoeid is met de vordering tot uitlevering van bescheiden en verstrekking van gegevens.

foontaps of observaties) en stukken die in het kader van het opsporingsonderzoek zijn uitgegaan. De bestanden van de uitgestuurde vorderingen worden uiteraard ook in de computer opgeslagen. Alleen het parket Amsterdam-Amstelland gebruikt daarnaast bij de gebiedsteams, zoals al is beschreven, nog een eenvoudig centraal registratiesysteem. De BOB-kamer hanteert dit systeem voor de voortgangsbewaking, dat wil zeggen: om te volgen welke vorderingen in het kader van de Wbvg en de Wet BOB zijn uitgegaan, om te registreren of de antwoorden al zijn ontvangen, en om bij te houden wanneer verlengingen van bevelen moeten worden ingediend.[155]

6.4 Besluit

In dit hoofdstuk stond een cijfermatige analyse van het beroep dat wordt gedaan op de Wbvg centraal, en is tevens de werkwijze die de opsporingsdiensten en de parketten hanteren bij het opstellen en uitsturen van Wbvg-vorderingen beschreven.

De cijfermatige analyse kon slechts worden uitgevoerd bij twee parketten en bij de FIOD, en heeft dus maar een indicatief karakter. De bevindingen worden echter wel bevestigd in interviews met vertegenwoordigers van andere instanties. Om te beginnen blijkt dat van de Wbvg eerst en vooral art. 126nc Sv en 126nd Sv worden gebruikt. Verzoeken om toekomstige gegevens (art. 126ne Sv), om gevoelige gegevens (art. 126nf Sv), om het ontsleutelen van versleutelde gegevens (art. 126nh Sv) en om een digitale doorzoeking (art. 125i Sv) zijn in een gemiddeld opsporingsonderzoek zelden nodig.

Hoewel op grond van de Wbvg in principe een onbeperkte waaier aan gegevens kan worden gevorderd, blijkt de wet in de praktijk in overwegende mate te worden gebruikt om financiële gegevens en camerabeelden te vorderen. Bij elkaar beslaan deze 72 procent van de uitgebrachte vorderingen. Gezien dit cijfer is het niet verwonderlijk dat financiële instellingen het meest met Wbvg-vorderingen worden geconfronteerd. Overigens krijgen zij ook veelvuldig te maken met verzoeken om camerabeelden.

Bij de opsporingsdiensten en de parketten worden vaste procedures gevolgd voor het indienen van Wbvg-vorderingen. De vorderingen op grond van art. 126nc Sv kunnen bij sommige politieregio's of BOD'en door willekeurig

[155] Overigens vermeldde het parket Amsterdam dit systeem te hebben overgenomen van de parketten Den Haag en Rotterdam waar het ook in gebruik zou zijn (geweest?). Kennelijk is dat thans niet meer het geval aangezien op vragen van de onderzoekers aan de arrondissementele BOB-kamers ter zake werd aangegeven dat men met een dergelijk registratiesysteem volstrekt onbekend was

welke bevoegde opsporingsambtenaar worden gedaan, maar elders zijn daartoe alleen de hulpofficieren van justitie geautoriseerd. Uitzondering, althans voor wat betreft de politie, zijn vorderingen aan banken en geldinstellingen waarvan bij richtlijn is bepaald dat daarvoor altijd een hulpofficier van justitie moet worden ingeschakeld. Het, overigens niet in de wet geëxpliciteerde, oogmerk dat slechts enkele opsporingsambtenaren geautoriseerd zouden worden om Wbvg-vorderingen te doen, blijkt in de praktijk niet te zijn overgenomen.

7 De toepassing van de wet: perspectief van gegevensvragers

7.1 Inleiding

In dit hoofdstuk staat de toepassing en het functioneren van de Wbvg vanuit het perspectief van de opsporingsinstanties centraal. Navolgend komen allereerst de ervaringen van de politie aan de orde (paragraaf 7.2.1). Vervolgens wordt aandacht besteed aan het oordeel over het functioneren van de Wbvg door opsporingsmedewerkers van de FIOD (paragraaf 7.2.2). Paragraaf 7.3 is gewijd aan de ervaringen van het openbaar ministerie met de toepassing van deze wet. In de laatste paragraaf (7.4) worden de bevindingen kort samengevat.

7.2 De ervaringen van opsporingsambtenaren met de Wbvg

De informatie die navolgend gepresenteerd wordt, is gebaseerd op gesprekken met opsporingsambtenaren van de politie enerzijds, en van de FIOD anderzijds. Omwille van de verschillen in het type opsporingsonderzoek dat de FIOD doorgaans doet, wordt deze BOD afzonderlijk beschreven.

7.2.1 Politie

Bekendheid met de bevoegdheden van de Wbvg
Uit de interviews blijkt dat op rechercheafdelingen regelmatig gebruik wordt gemaakt van de bevoegdheden uit de Wbvg. Naarmate er sprake is van ernstiger strafbare feiten, gebeurt dat vaker. ‘In een geval van georganiseerde criminaliteit gebruik je de Wbvg vrijwel dagelijks, en in financiële onderzoeken ook’, aldus een respondent van de politieregio Brabant-Noord. Een respondent van de politieregio Midden- en West Brabant noemt de Wbvg ingeburgerd. ‘We hebben er veel mee van doen.’

In de politiepraktijk wordt vooral gebruikgemaakt van art. 126nc Sv en 126nd Sv. Het vorderen van toekomstige gegevens op basis van art. 126ne Sv gebeurt volgens een rechercheur van de politieregio Brabant-Zuidoost ‘wel eens, maar niet zo vaak. Soms passen we dit artikel toe in financiële onderzoeken [om mutaties in het banksaldo van een verdachte te kunnen nagaan] en ook in vermissingszaken.’ Een geïnterviewde uit de politieregio Brabant-Noord verklaart de beperkte toepassing van art. 126ne Sv uit de aard van het recherchewerk: ‘de meeste onderzoeken worden reactief opgezet, dus dan vorder je geen toekomstige gegevens’. Ook art. 126nf Sv wordt niet veel gebruikt. Een vertegenwoordi-

ger van de politieregio Brabant-Zuidoost verwacht dat dit in de toekomst zal veranderen vanwege de uitspraak in de zaak Trans Link.

De recherche onderscheidt enerzijds een aantal zogeheten vaste partners, zoals telecomproviders en grote banken, en anderzijds 'incidentele verstrekkers', die door de politie externe verstrekkers worden genoemd. De relatie met de gegevenshouders is over het algemeen goed. Een weigering om gevorderde gegevens uit te leveren heeft geen van de respondenten ooit meegemaakt. 'Mijn ervaring is dat we weinig tot nooit problemen hebben. Als er al instanties zijn die niet willen meewerken, dan komt dat vaak omdat er sprake is van een zekere betrokkenheid bij het strafbare feit', zo stelt een rechercheur uit de politieregio Brabant-Noord. Wel hebben sommige verstrekkers veel tijd nodig om te komen tot uitlevering, vaak ruim meer dan de termijn van veertien dagen die bedoeld is voor 126nd-vorderingen. 'Bij banken duurt het langer, maar dat heeft niet met de vorderingen te maken, meer met hun organisatiestructuur', aldus een medewerker van de Bovenregionale Recherche Zuid-Nederland. Een collega van de politieregio Brabant-Noord vult aan: 'Bij banken wil men vaker eerst garanties, zeker als het gaat om grote aantallen vorderingen. Dat vind ik dan wel te billijken, vanuit het soort relatie dat een bank heeft met zijn cliënt'. Een respondent van de politieregio Zeeland is van mening dat een Wbvg-vordering 'niet boven op de stapel [ligt] bij een gegevenshouder. Telecomproviders leveren snel, maar andere instellingen doen het langzamer.'

Vrijwilligheid

Vrijwillige verstrekking van gegevens is volgens de geïnterviewden met de komst van de Wbvg zo goed als van de baan. Een functionaris van de politieregio Brabant-Noord: 'Je ziet het nog maar zelden gebeuren dat professionele bezitters van gegevens zomaar meewerken [zonder een vordering]. Zij zijn bang voor claims van hun klanten, dus het is logisch dat bedrijven vragen om een goede regeling en zich willen verantwoorden.' Ook bij de recherche is het inmiddels een duidelijke zaak dat vrijwilligheid verleden tijd is. Een medewerker van Bovenregionale Recherche Zuid-Nederland blikt terug: 'de eerste twee à drie jaar na introductie van de wetgeving hadden we nog regelmatig discussies over of je gegevens nu wel of niet vrijwillig kon ontvangen. We zien het nu soms nog in overgedragen werk: dat er gegevens zijn opgevraagd, maar dat er geen vordering is. We bespreken dat dan met de zaaksofficier en dan is het aan hem om te beslissen of het acceptabel is. Maar ik weet ook dat het ontbreken van een vordering niet echt cruciaal is [in de zin dat er een procesrisico ontstaat als de gegevens gebruikt worden in de opsporing].'

Volgens een rechercheur uit de politieregio Zeeland is vrijwillige gegevensverstrekking nog niet helemaal verdwenen: 'er zijn er altijd die het alvast geven. Vaak zijn ze dan zelf ook belanghebbende partij: heb ik te maken met

een dubieuze klant? Wij sturen ook bij vrijwillige verstrekking alsnog een vordering.' Dezelfde aanpak wordt gehanteerd door de recherche Brabant Zuidoost: 'Wij vragen niet eens om vrijwillige verstrekking. Wij willen dat niet hebben. Wij willen uitsluitend geformaliseerd werken, zodat we geen discussie hebben [met de gegevenshouder].'

Verhouding tot andere bevoegdheden

Omdat de recherchemedewerkers ondertussen goed op de hoogte zijn van de bevoegdheden van de Wbvg wordt er ook veel mee gewerkt. Een functionaris uit de politieregio Zeeland legt uit dat er gewerkt wordt 'op basis van eerdere ervaringen. Je kijkt altijd of je zoiets eerder aan de hand hebt gehad en dan werk je op dezelfde manier. We gaan niet pionieren.' Opsporingsmedewerkers uit de politieregio Brabant Zuid-Oost vullen aan: 'er is nog een andere procedure om gegevens te vorderen, in een strafrechtelijk financieel onderzoek (SFO). Dan kom je door het ganse land en zonder de officier kun je dan de informatie gaan opvragen.' Hierbij wordt gedoeld op art. 126a Sv dat, zoals in hoofdstuk 4 aan de orde is gekomen, bedoeld is voor situaties waarin gegevens dienen te worden gevorderd om inzicht te krijgen in de vermogenspositie van de verdachte.[156] Een functionaris van de politieregio Midden- en West Brabant stelt dat soms bij het opvragen van camerabeelden gebruik wordt gemaakt van de mogelijkheden tot inbeslagneming, 'bijvoorbeeld bij beelden van het strafbare feit zelf, waar de verdachte op staat'.

Knelpunten in de praktijk

De geïnterviewde politiefunctionarissen noemen unaniem als een van de eerste nadelen van de Wbvg de administratieve belasting. 'Je moet vijf of zes PV's schrijven voordat je de informatie [die je gevorderd hebt bij een gegevenshouder] concreet op papier hebt. Wij zijn daar nu mee bekend, dus bij ons loopt dat nu wel goed. Maar bij de reguliere recherche is dat een heel ander verhaal', zo stelt een vertegenwoordiger van de politieregio Limburg-Zuid. Een functionaris van de politieregio Brabant-Noord vindt de procedures die gevolgd moeten worden een nadeel. 'Dat geldt niet alleen voor 126nd vorderingen, ook voor 126nc. Er is sprake van veel papierwerk, veel processen-verbaal, waar al gauw twee afdelingen bij betrokken zijn. Er komt een fysieke formulierenstroom op gang, en die veroorzaakt een administratieve ballast.' Dezelfde respondent stelt ook

[156] In 2009 diende minister van Justitie Hirsch Ballin een wetsvoorstel in ter verbetering van de toepassing van de maatregel ter ontneming van wederrechtelijk verkregen voordeel. Daarin is voorgenomen dat de officier van justitie bevoegd wordt, en in een aantal gevallen de rechter-commissaris. Zie *Kamerstukken II* 2009/10, 32 194, nr. 2.

dat naar zijn idee sprake is van een zware toetsing. ‘De controle vooraf [op het inzetten van de Wbvg-bevoegdheden] is bijna net zo zwaar als de controle achteraf: de toetsing door de rechter. Dat is in het geval van het toepassen van zware bevoegdheden wel legitiem, maar bij het opvragen van telefoongegevens en NAW-gegevens? Iedereen zet tegenwoordig alles op internet, maar als wij erom vragen, dan moet je een hele procedure volgen.’

De rechercheur van de Bovenregionale Recherche Zuid-Nederland ziet dat recherchemedewerkers die weinig met de Wbvg te maken hebben problemen ondervinden met de finesses van de wet. ‘Wij hebben korte lijnen naar justitie, dus wij kunnen snel werken, maar voor de gewone recherche is het moeilijker, omdat ze geen zaaksofficier hebben. Het zou voor hen gemakkelijk zijn als er een contactpersoon bij het openbaar ministerie is, zeker om vragen aan voor te leggen zoals het onderscheid tussen Artikel 126nc Sv en art. 126nd Sv. Ik zie nu dat collega’s weerhouden worden [om deze vragen te stellen], omdat ze geen aanspreekpunt hebben. Die drempel zou veel lager kunnen zijn.’

De uitspraak in de zaak Trans Link is ook aan de geïnterviewde politiefunctionarissen niet onopgemerkt voorbijgegaan en zij volgen de huidige discussie met veel belangstelling. Ze vrezen dat deze uitspraak het opvragen van camerabeelden in de praktijk ‘onwerkbaar’ maakt. Een medewerker van de politieregio Limburg-Zuid ‘houdt haar hart vast: als we naar de rechter-commissaris moeten voor camerabeelden. De regelgeving is er ter bescherming van de burger en dat vind ik een goede zaak. Maar het wordt op deze manier te gek voor ons, we schieten erin door.’

Een geïnterviewde uit de politieregio Zeeland constateert dat de praktijk over het algemeen niet verbeterd is. ‘We zijn er niet veel mee opgeschoten. Voor ons zijn de consequenties vooral van administratieve aard, we hebben inmiddels een woud aan formulieren. Ik weet niet meer welk formulier ik bij wie moet indienen.’ Deze onoverzichtelijkheid wordt bevestigd door de respondenten van de politieregio Brabant- Zuidoost: ‘Ik vind het goed dat je niet zomaar lukraak overal informatie kunt gaan bevragen en dat er een toetsing vooraf plaatsvindt. Die [toetsing] zou alleen een stuk eenvoudiger moeten kunnen zijn. Zeker in de gevallen dat het [de vordering] geen verstrekkende gevolgen heeft voor de betrokkene.’

De samenwerking met het openbaar ministerie in verband met de Wbvg-vorderingen verloopt volgens de politiefunctionarissen goed, maar zorgt in hun optiek ook voor vertraging. De inhoudelijke toets van de vordering is in het merendeel van de gevallen een formaliteit, omdat er tussen de opsporingsdienst en het openbaar ministerie nauw overleg plaatsvindt. De zaaksofficier van justitie is om die reden vaak al op de hoogte van het voornemen een vordering tot gegevensverstrekking te doen.

Een medewerker van de politieregio Midden- en West-Brabant constateert dat de procedure in de praktijk nog wat zorgvuldiger kan. De gegevens die zijn opgevraagd bij een gegevenshouder komen, op het moment dat ze zijn uitgeleverd, immers in het procesdossier terecht. Dat betreft alle gegevens die zijn opgevraagd, ook die waar in de opsporing uiteindelijk niet op doorgerechercheerd is. Een voorbeeld is een geval waarin over een aantal personen identiteitsgegevens bij een bank is opgevraagd, terwijl er daarvan uiteindelijk slechts een of twee als verdachte worden aangemerkt. Hij pleit dan ook voor de mogelijkheid om die informatie buiten het dossier te kunnen houden. 'Voor de bijvangst zou je een afschermingsregeling, zoals bij de afgeschermde aangever, moeten ontwerpen, of we zouden niet alles in het procesdossier moeten opnemen.'

7.2.2 FIOD

Bekendheid met de bevoegdheden van de Wbvg

Uit de interviews met vertegenwoordigers van de FIOD blijkt dat de bevoegdheden van de Wbvg eveneens goed bekend zijn bij de opsporingsmedewerkers en in de praktijk ook veel worden gebruikt. Daarbij betreft het vooral art. 126nc Sv en art. 126nd Sv. De geïnterviewden zijn weliswaar op de hoogte van art. 126ne Sv en 126nf Sv, maar zij passen deze zelden tot nooit toe.

Art. 126nc Sv en 126nd Sv worden, behalve voor het in kaart brengen van NAW-gegevens en administratieve gegevens van een verdachte of een groep verdachten, ook veel gebruikt voor het identificeren van de tenaamstelling van een bankrekening (art. 126nc Sv) en voor het opvragen van bankafschriften (art. 126nd Sv). De belangrijkste gegevensverstrekkers zijn banken, alsmede accountant- en administratiekantoren.

Relatie met gegevensverstrekkers

Opsporingsmedewerkers van de FIOD typeren de aard van de relatie met gegevensverstrekkers als verschillend. 'Banken zijn heel formeel en geven het liefst zo weinig mogelijk. Voor de opsporing is dat lastig. Ik weet ook niet of wij alles krijgen van een bank, zij maken een selectie. Bij andere verstrekkers gaat dat gemakkelijker', aldus een van de geïnterviewden. Geen van de respondenten heeft meegemaakt dat gegevensverstrekkers weigeren mee te werken. De termijn waarop de gegevens worden verstrekt, is per instelling verschillend, 'maar met een *reminder* heb je het vrij snel in huis'.

Verhouding tot andere bevoegdheden

Naast de bevoegdheden van de Wbvg kan een opsporingsmedewerker van de FIOD ook gegevens vorderen op grond van art. 81 Awr.[157] Het voordeel hiervan, ten opzichte van de bevoegdheden van de Wbvg, is dat ze ook van toepassing is op een verdachte. Bovendien kan de opsporingsambtenaar deze bevoegdheid zelfstandig aanwenden, dus zonder tussenkomst van het openbaar ministerie.

Een beperking van art. 81 Awr is evenwel dat het moet gaan om een fiscaal delict. In de praktijk doet de FIOD ook opsporingsonderzoek naar andere dan uitsluitend fiscale delicten: 'Het is in ongeveer de helft van de gevallen dat er ook een fiscaal delict in zit. Wij doen steeds minder fiscale onderzoeken en steeds meer commune strafbare feiten, zoals fraude, oplichting en merkvervalsing', aldus een van de respondenten. Een tweede beperking van art. 81 Awr is dat het een bevoegdheid tot inbeslagneming betreft, en in feite geen betrekking heeft op het vorderen van gegevens. In de praktijk wordt dan ook vooral een beroep gedaan op art. 81 Awr als een opsporingsmedewerker 'op locatie' is en hij stuit op gegevens die relevant zijn voor het opsporingsonderzoek. Er is dan geen gelegenheid om een Wbvg-vordering op te maken via de (hulp)officier, zodat alleen inbeslagneming tot de mogelijkheden behoort.

De strafvorderlijke tegenhanger van art. 81 Awr is art. 94 Sv, waarin de bevoegdheid tot inbeslagneming van voorwerpen is neergelegd. Ook deze bevoegdheid kan door functionarissen van de FIOD worden gehanteerd, maar daarbij is sprake van de beperking dat sprake moet zijn van een misdrijf waarbij voorlopige hechtenis is toegestaan.

In het verlengde hiervan biedt art. 96a Sv de mogelijkheid de uitlevering ter inbeslagneming te vorderen. De beperking van dit artikel (ten opzichte van de bevoegdheid van art. 81 Awr) is dat de vordering niet kan worden gericht aan de verdachte (art. 96a lid 2 Sv). Bovendien moet ook hier sprake zijn van verdenking van een misdrijf waarvoor voorlopige hechtenis is toegestaan. Daarbuiten kan het bevel tot uitlevering alleen door de rechter-commissaris worden afgegeven (art. 105 Sv).

In geval van verdenking van een economisch delict, biedt art. 19 WED opsporingsambtenaren van de FIOD de bevoegdheid gegevens en bescheiden in te zien en daarvan kopieën te maken. Voor de toepassing van deze bevoegdheid hoeft geen sprake te zijn van een concrete verdenking in de zin van art. 27 Sv. 'Concrete aanwijzingen' dat een WED-voorschrift is overtreden, zijn voldoende. Bovendien kan deze bevoegdheid ook worden ingezet tegen de verdachte. De

[157] Zie paragraaf 4.6.

beperking van de WED is echter dat het moet gaan om een economisch delict, dat is strafbaar gesteld in art. 1 en 1a van die wet. Specifieke WED-onderzoeken vormen echter maar een beperkt deel van de door de FIOD uitgevoerde strafrechtelijke onderzoeken en de bevoegdheid kan dus lang niet altijd worden toegepast. Eén van de geïnterviewden stelt voorts dat met de introductie van de Wbvg art. 19 WED zijn toepassing enigszins verloren heeft, ook al ligt de 'verdenkingslat' lager dan die bij art. 126nc Sv.[158]

De bevoegdheden op grond van de WED worden ook minder vaak gebruikt omdat deze bij de medewerkers niet zo bekend zijn als de Wbvg. Ten tijde van de introductie van de Wbvg is binnen de FIOD veel aandacht besteed aan interne training met betrekking tot de toepassing van de regelgeving in financiële onderzoeken. Geïnterviewde leidinggevende functionarissen van de dienst vermoeden dat medewerkers daarom wellicht ook eerder kiezen voor een vordering op basis van art. 126nc of 126nd Sv.[159] Zij stellen voorts dat art. 81 Awr en art. 19 WED in de praktijk binnen de FIOD worden beschouwd als 'zwaardere' opsporingsmiddelen dan de Wbvg.

De Wbvg heeft over het algemeen het belang van de andere bevoegdheden verminderd, hoewel niet bij alle geïnterviewden helder is waarom. 'Vroeger namen we nog wel in beslag, maar nu is alles onder artikel 126nd komen te vallen. Van artikel 94 Sv wordt gezegd dat het een zwaarder middel is, maar ik begrijp dat niet goed. Volgens mij is artikel 126nd zwaarder, want daar heb je een toets van de officier van justitie bij nodig', aldus een respondent. De geïnterviewde leidinggevenden bevestigen de gesignaleerde ontwikkeling: 'Voordat de Wbvg van kracht werd, werd opsporingsinformatie opgevraagd via artikel 81 Awr en artikel 19 WED. Deze bevoegdheden bestaan nog steeds, maar de Wbvg geldt als een lichtere maatregel, vandaar dat deze eerst moet worden toegepast. Van een verdachte worden overigens meestal geen gegevens gevorderd, maar worden deze verkregen door huiszoeking toe te passen.'

Vrijwillige gegevensverstrekking

Vrijwillige gegevensverstrekking is volgens de FIOD-medewerkers voor een goed deel verdwenen maar nog niet helemaal. 'Er zijn nog steeds omstandighe-

---

158 Voor toepassing van art. 19 WED volstaat een aanwijzing, terwijl voor toepassing van art. 126nc Sv een verdenking van een misdrijf nodig is.

159 Deze uitleg over de toepassing van art. 19 WED door FIOD-medewerkers is afkomstig van een juridisch beleidsmedewerker van de FIOD. De interviews met de opsporingsmedewerkers lijken te bevestigen dat art. 19 WED relatief onbekend is. De respondenten werd gevraagd naar andere wetgeving op basis waarvan gegevens kunnen worden gevorderd. Art. 81 Awr en art. 96a Sv werden spontaan genoemd, maar art. 19 WED geen enkele keer.

den waarin vrijwillig verstrekt wordt. Bijvoorbeeld in het geval dat je iemand [een getuige] aan het horen bent, dan wordt er wel eens door de betrokkene een uitdraai gemaakt van een document. Dat kan spontaan gebeuren, of naar aanleiding van een vraag van ons, en alle situaties daar tussenin. Wij zouden dat ook wel graag zo willen houden, want het is anders onwerkbaar', aldus een van hen. De leidinggevenden van de FIOD zijn het hier overigens volstrekt mee oneens: de opvatting van deze geïnterviewde is volgens hen strijdig met het beleid.

Knelpunten in de praktijk

Opsporingsmedewerkers stellen dat de Wbvg het werk niet moeilijker heeft gemaakt (ook niet gemakkelijker, overigens), maar constateren wel dat de wet tot 'een grotere papierwinkel' heeft geleid, 'met veel overhead en beleidsafdelingen'. De teneur in de interviews met medewerkers van de FIOD is dat de Wbvg inhoudelijk geen wezenlijke verandering in het werk heeft opgeleverd (er worden nog steeds gegevens gevorderd van derden). Wel is in hun optiek de administratieve belasting groter geworden, omdat voor het vorderen van gegevens op basis van de Wbvg processen-verbaal moeten worden geschreven ('het zijn zo zes pagina's extra in een dossier'). Eén van de geïnterviewden: 'ik zal wel gebruik moeten maken van de Wbvg, maar ik ben er niet heel enthousiast over. Het is wetgeving die ingewikkeld in elkaar zit (...) en in *ad hoc* situaties lastig toepasbaar is. Ik zie de verbetering niet: we krijgen nog steeds dezelfde gegevens als voorheen, alleen duurt het nu langer en kost het ons meer werk.' Een andere medewerker signaleert dat de Wbvg ertoe leidt dat minder snel kan worden gewerkt. 'Vroeger kon je overal je spullen halen, nu moet je eerst een aanvraag doen. (...) Onderzoeken gaan langer duren, de doorlooptijd is opgelopen.'

Een tweede probleem voor de opsporingsfunctionarissen van de FIOD is dat het onderscheid tussen art. 126nc Sv en art. 126nd Sv niet altijd duidelijk is. 'Een voorbeeld is de vraag of een rekeninghouder op een bepaald adres woont. Of informatie over een mederekeninghouder. Kan die informatie nog op basis van art. 126nc gevorderd worden, of moet daarvoor een 126nd vordering worden gedaan?', aldus de geïnterviewde leidinggevenden. In samenhang hiermee worstelen de opsporingsambtenaren ook met de afbakening van het begrip 'gegeven': heeft dat alleen betrekking op informatie die in een computer is opgeslagen, of (ook) op uitgeprinte documenten?

Een derde knelpunt in de praktijk (de FIOD-leidinggevenden spreken van 'een substantieel probleem') is dat de gegevenshouder mag bepalen hoe de gegevens worden uitgeleverd. Banken hebben de gegevens bijvoorbeeld digitaal voorhanden, maar kiezen er welbewust voor deze alleen op papier uit te leveren, ook al betekent dat voor henzelf (veel) meer werk. Bij bankafschriften kan het gaan om grote hoeveelheden afschriften, die bij de FIOD weer in de computer moeten worden ingevoerd. Dat levert ook de opsporingsdienst niet alleen veel

extra werk op, maar doet bovendien de kosten oplopen, omdat voor elk geprint afschrift een stuksprijs moet worden betaald.

Een vierde aandachtspunt is dat opsporingsmedewerkers niet altijd inzien waarom zij gegevensdragers niet simpelweg in beslag kunnen nemen. De respondenten ervaren beslaglegging niet als een zwaarder middel dan het vorderen van gegevens: 'inbeslagneming is juist gemakkelijker, want dat kan op basis van art. 81 Awr of art. 96a Sv. Daar heb ik dan geen officier van justitie bij nodig. Voor de betrokkene maakt het niet uit of je gegevens in beslag neemt of informatie vordert met een brief van de officier van justitie, hij moet toch dezelfde handeling verrichten. Je zou het vorderen van gegevens moeten inrichten op basis van de medewerking van de betrokkene: als hij gegevens vrijwillig verstrekt, dan kun je ze in beslag nemen. Werkt de betrokkene niet vrijwillig mee, dan kom je met een vordering.' Deze respondent wordt bijgevallen door een collega: 'als je het zelf kunt [vorderen zonder tussenkomst van de officier van justitie] dan is dat minder ingrijpend voor een betrokkene. Als je de spullen zo kunt krijgen, bijvoorbeeld een ordner met administratie die bij de betrokkene in de kast staat, dan neem je die in beslag. Maar als je moet zoeken in een digitale administratie, dan werk je met een Wbvg-vordering.'

Tot slot wordt ook bij de FIOD de uitspraak in de zaak Trans Link als problematisch voor het werk ervaren: 'het opsporen wordt onmogelijk gemaakt', aldus een van de functionarissen. De leidinggevenden: 'Dit is een onmogelijke uitspraak. Hoe moet je van te voren weten welke gegevens je gaat krijgen als je camerabeelden opvraagt? En wat is 'gevoelig': waarom is het feit dat je iemand met een hoofddoek op de beelden te zien kunt krijgen wel een gevoelig gegeven, terwijl er bij een blanke man met een bepaald soort tatoeage kennelijk geen sprake is van een probleem? Kern van de vraag is waar je naar op zoek bent. Dit punt dient dringend nader te worden geëxpliciteerd door de wetgever.'

7.2.3 Algemeen oordeel vanuit de optiek van de opsporingsdiensten

Uit de interviews met de medewerkers van opsporingdiensten blijkt dat zij zich bij de wetgeving hebben neergelegd. Men erkent de voordelen van de Wbvg, maar is niet gelukkig met de administratieve belasting die de wet met zich mee heeft gebracht.

Opsporingsmedewerkers zien duidelijk de meerwaarde van de bescherming van de burger tegen het 'zo maar' verstrekken van gegevens. De toegenomen zorgvuldigheid van de procedure rond strafvorderlijke gegevensvordering wordt dan ook positief gewaardeerd. De gegevensvordering verloopt nu meer gestructureerd, en volgens betere procedures. Het voordeel van het in processenverbaal vastleggen van de wijze van gegevensvordering en verstrekking, die aan

het dossier worden toegevoegd, is dat achteraf precies kan worden gereconstrueerd hoe de gegevensvordering verlopen is.

De keerzijde van deze zorgvuldigheid is de toegenomen formalisering en daarmee het papierwerk voor de opsporingsdiensten. Bovendien blijkt dat de functionarissen in de praktijk een gebrek aan nuance ervaren. Als een betrokkene vrijwillig meewerkt, kan de gegevensverstrekking dan niet met een minder zware (in de zin van toetsing vooraf én achteraf), bureaucratische en tijdrovende procedure worden gewaarborgd dan nu op grond van de Wbvg vereist wordt? Praktische barrières zijn verder de uitlevering van gegevens op papier en de hoge kosten die verbonden zijn aan de uitlevering.

Feitelijk lopen opsporingsonderzoeken niet 'stuk' op de door de opsporingsambtenaren ervaren nadelen van de Wbvg, maar de vertraging en de administratie worden wel als heel vervelend getypeerd. Ook is er behoefte aan meer kennis over de Wbvg, vooral voor wat betreft het onderscheid tussen art. 126nc Sv en 126nd Sv.

Ook pleiten de opsporingsdiensten voor meer armslag bij het toepassen van de Wbvg ten opzichte van andere bevoegdheden. Indien een gegevenshouder meewerkt, zou bijvoorbeeld vaker kunnen worden volstaan met inbeslagneming (met een schriftelijk bewijs voor de houder dat de gegevens gebruikt worden in een strafvorderlijk onderzoek). De Wbvg kan dan worden toegepast indien sprake is van een gegevenshouder die niet wil meewerken. Door deze mogelijkheid te bieden kan de tijdrovende procedure beperkt worden tot de 'moeilijke gevallen'. Of dit een werkbare suggestie is, is echter de vraag. Aangezien vrijwel alle gegevensverstrekkers vrijwillig meewerken, zou dit in de praktijk de Wbvg ernstig uithollen.

Een andere suggestie die door geïnterviewden werd gedaan, is de Wbvg niet van toepassing te laten zijn op gegevens die een verdachte uit vrije wil heeft achtergelaten. Te denken valt bijvoorbeeld om informatie die wordt ingevuld bij het aanvragen van een bonuskaart van een supermarkt, of aan gegevens die een burger vrijwillig achterlaat bij het registreren voor webfora. De vrijwillig verstrekte gegevens zouden op een eenvoudiger wijze gevorderd moeten kunnen worden dan de onvrijwillige. Ook hier is het de vraag of dit wenselijk is. De bedoeling van de Wbvg en de Wbp is nu juist om gegevens van derden te beschermen. Dat geldt ook voor gegevens die door een burger vrijwillig worden achtergelaten of opgegeven. Hij geeft deze immers niet af met de expliciete

goedkeuring dat deze ook voor andere doeleinden kunnen worden gebruikt, of vergeet de kleine lettertjes in de voorwaarden te lezen.[160]

7.3 De ervaringen van het openbaar ministerie met de Wbvg

7.3.1 Toepassing van de verschillende onderdelen van de wet

De volgende groep gegevensvragers die is bevraagd omtrent hun ervaringen met de toepassing van de Wbvg zijn de medewerkers van het openbaar ministerie, namelijk officieren van justitie en parketsecretarissen. Zij blijken allen ervaring te hebben met de Wbvg en noemen de regelgeving geheel ingeburgerd. De Wbvg wordt vooral ingezet in het beginstadium van een opsporingsonderzoek, als er nog niet veel bekend is over een verdachte. Het meest gebruikte onderdeel van de wet is art. 126nd Sv. Toepassing van art. 126ne Sv en art. 126nf Sv is veel minder gebruikelijk, en de overige artikelen worden volgens de respondenten vrijwel niet tot in het geheel niet gebruikt.

Het vorderen van toekomstige gegevens op grond van art. 126ne Sv gebeurt volgens de geïnterviewden vooral in drugssmokkelzaken. Het gaat dan bijvoorbeeld om toekomstige vluchtgegevens (wanneer vertrekt de verdachte, wanneer komt hij het land weer in) die worden opgevraagd bij een luchtvaartmaatschappij of bij een luchthaven. In een enkel geval wordt art. 126ne Sv ook gebruikt bij vermissingen of ontvoeringen, wanneer de opsporingsdiensten willen weten of er nog een teken van leven is van de vermiste (wordt bijvoorbeeld een bankpas gebruikt?). Een officier van justitie van het FP meldt dat art. 126ne Sv ook nuttig is in onderzoeken waarin de wens bestaat doorlopend op de hoogte te blijven van transacties die via bepaalde rekeningen worden gedaan. Een voordeel van dit wetsartikel is dat de gegevenshouder (in dat geval meestal een bank) de informatie direct moet leveren en het openbaar ministerie en de opsporingsdiensten dus niet wekenlang hoeven te wachten tot de gevorderde gegevens toekomen.

Art. 126nf Sv wordt volgens de respondenten zeer weinig gebruikt. Slecht enkelen hebben er ervaring mee, bijvoorbeeld in medische kwesties waarin een patiëntdossier is opgevraagd. De wetgever had de verwachting dat art. vooral zou worden gebruikt bij bijvoorbeeld levensdelicten of zedenzaken, maar dat blijkt in de praktijk niet het geval. In dergelijke ernstige zaken is de neiging

[160] Ofschoon ook bedrijven die informatie zelf ook voor andere (marketing)doeleinden gebruiken dan waarvoor de klant ze heeft verstrekt, of weer doorverkopen aan andere firma's.

bij de opsporingsdiensten veeleer om het middel van de telefoontap te gaan toepassen. ‘Je gaat dan de telefoon(s) van de verdachte afluisteren. Er wordt niet eens gedacht aan 126nf. (…) Dat kan ook komen door onbekendheid bij het openbaar ministerie, dat men niet goed op de hoogte is van de mogelijkheden van de Wbvg. Behalve wanneer het gaat om medische gegevens: dat is de duidelijkste categorie voor 126nf voor de officieren’, aldus een respondent.

Ook de geïnterviewde officieren van justitie verwachten echter dat het belang van art. 126nf Sv zal toenemen, naar aanleiding van de zaak Trans Link. Alle respondenten zijn op de hoogte van de uitspraak en van de consequenties ervan, en een aantal van hen heeft inmiddels ook, in verband met het opvragen van (mogelijk gevoelige) camerabeelden, gebruikgemaakt van art. 126nf Sv.

Art. 125i Sv, dat ziet op de doorzoeking ter vastlegging van gegevens, wordt slechts door een van de geïnterviewden, die werkzaam is bij het FP, gebruikt, maar dan wel in combinatie met art. 96c Sv. Zo’n ‘combivordering’ garandeert volgens deze respondent dat er flexibel kan worden opgetreden: ‘de digitale doorzoeking passen wij bijvoorbeeld toe wanneer een bedrijf in een bedrijfsverzamelgebouw zit, waar gebruik wordt gemaakt van een gezamenlijke server. Als we de hele server meenemen duperen we ook de andere bedrijven. We maken dan een *image* van de gegevens van het verdachte bedrijf en onderzoeken die later op het bureau verder.’

7.3.2 Verhouding tot andere BOB-bevoegdheden

De geïnterviewde vertegenwoordigers van het openbaar ministerie zien de meest gebruikte onderdelen van de Wbvg (in het bijzonder art. 126nd Sv) als een ‘eenvoudig middel’ dat snel resultaat oplevert. Bovendien biedt de Wbvg mogelijkheden om informatie over een (groep van) verdachte(n) te achterhalen, die niet (zo snel) door middel van andere BOB-middelen kan worden verkregen, terwijl inbreuk op de privacy van de betrokkenen vrij beperkt blijft. Toch geven zij wel voorbeelden van gevallen waarin de voorkeur uitgaat naar andere dwangmiddelen.

Eén van de geïnterviewden bij het parket Amsterdam geeft bijvoorbeeld aan dat in zijn praktijk camerabeelden die al door de beheerder zijn opgeslagen op een gegevensdrager (bijvoorbeeld op een CD-ROM), eerder in beslag worden genomen op basis van art. 96a Sv, dan dat de gegevens worden gevorderd op basis van art. 126nd Sv. Om pasfoto’s van personen te verkrijgen wordt bijvoorbeeld een beroep gedaan op art. 73, onder c van de Paspoortuitvoeringsrege-

ling.[161] In fiscale zaken wordt ook gebruikgemaakt van de algemene bevoegdheden tot gegevensvordering die zijn opgenomen in art. 55 en 81 van de Algemene wet inzake rijksbelastingen.

Tot slot wijst een van de respondenten op een lacune met betrekking tot het vorderen van gegevens van een aanbieder van een telecommunicatiedienst. Art. 126n Sv bevat de bevoegdheid om zulke gegevens van geïdentificeerde gebruikers (dus met een bekende naam of een bekend telefoonnummer) te vorderen. Art. 126ng Sv bepaalt echter dat verkeers- en gebruikersgegevens niet in het kader van de Wbvg kunnen worden gevorderd. Een voorbeeld is een geval van een inbraak in een bedrijfspand. De politie beschikt over camerabeelden van de bewakingscamera van het pand, waarop is geregistreerd dat een van de vermoedelijke daders staat te bellen met een mobiele telefoon, vlak vóór de inbraak werd gepleegd. De politie kent deze beller niet, en heeft evenmin de beschikking over diens telefoonnummer. Op grond van art. 126n Sv is het dan niet mogelijk om historische telefoongegevens (verkeersgegevens) te vorderen bij een aanbieder van een communicatiedienst, want van deze beller zijn naam noch telefoonnummer bekend. Met andere woorden: deze gebruiker is niet geïdentificeerd, zoals art. 126n Sv vereist. De Wbvg biedt voor deze situatie evenmin soelaas, want art. 126ng Sv verbiedt het vorderen van verkeers- en gebruiksgegevens op basis van de Wbvg (i.c. op basis van art. 126nc Sv of art. 126nd Sv). Er lijkt hier dus een leemte in de wet te zijn. Wil men in gevallen als dit de gegevens kunnen vorderen dan zou men gebruiker niet zo strikt als geïdentificeerde gebruiker moeten lezen of art. 126ng Sv aanpassen.[162]

7.3.3 Gebruik van gegevens in meerdere onderzoeken

Uit de interviews blijkt dat het voorkomt dat gegevens die in het kader van het ene onderzoek zijn gevorderd ook in andere onderzoeken worden gebruikt. De respondenten wijzen in dat verband op de regeling van art. 126dd Sv waarin is vervat dat 'de officier van justitie kan bepalen dat gegevens die zijn verkregen door observatie met behulp van een technisch hulpmiddel dat signalen registreert, het opnemen van vertrouwelijke communicatie, het opnemen van telecommunicatie of het vorderen van gegevens over een gebruiker en het telecommunicatieverkeer met betrekking tot die gebruiker, kunnen worden gebruikt

---

161 Paspoortuitvoeringsregeling, *Stcrt.* Supplement 2001, nr. 186.

162 Overigens wordt dit probleem in de praktijk opgelost door de mastgegevens op te vragen van het exacte tijdstip waarop het telefoongesprek werd gevoerd, om op die manier het telefoonnummer te achterhalen.

voor een ander strafrechtelijk onderzoek dan waartoe de bevoegdheid is uitgeoefend'.

De vraag is evenwel of deze regeling ook in het kader van de Wbvg van toepassing is, aangezien art. 126dd Sv expliciet lijkt te doelen op BOB-middelen die worden ingezet voor het opnemen van telecommunicatie. Bovendien is art. 126dd Sv (in samenhang met art. 126cc Sv) bedoeld voor *bulk*gegevens, het opnemen van vertrouwelijke communicatie met een technisch hulpmiddel, en dergelijke. Het is de vraag of op grond van de Wbvg gevorderde gegevens daaronder kunnen worden geschaard. Mogelijk doelen de respondenten dan ook niet (zozeer) op het Wetboek van Strafvordering, maar op bepalingen uit de Wet politiegegevens (WPG).[163] Daarin is, in paragraaf 3, het verstrekken van gegevens aan anderen dan de politie en de KMAR geregeld. Andere wetgeving die iets zegt over deze materie is de Wet justitiële en strafvorderlijke gegevens (tweede afdeling).[164]

Een Groningse officier van justitie legt uit dat voor het uitwisselen van gegevens tussen twee onderzoeken een zogeheten 'kluis-PV'[165] gebruikt wordt, 'met toestemming van de zaaksofficier. (…). Het [uitwisselen van gegevens] kan wel, je hoeft niet opnieuw dezelfde BOB-aanvraag te doen.' Een collega vult aan: 'Als het RC-bevoegdheden zijn [waarvan je de resultaten wilt toepassen in een ander onderzoek], dan moet je het [bij de rechter-commissaris] gaan vragen. Je moet je wel realiseren dat het privacygevoelige gegevens betreft, dus je moet er wel prudent mee omgaan.'

Eén van de geïnterviewde officieren van justitie meldt dat de procedure rond het bewaren en uitwisselen van gegevens bij de politie mogelijk met minder waarborgen omkleed is: 'Wat vaker gebeurt [vaker dan gegevensuitwisseling bij het openbaar ministerie] is dat onderzoeksresultaten bij de politie worden opgeslagen. Dat wordt dan wel gedeeld in andere onderzoeken.'

7.3.4 Notificatieplicht

De wet schrijft voor dat het openbaar ministerie degene op wie de vordering betrekking had, moet notificeren als er bevoegdheden op basis van de Wbvg zijn ingezet. Alleen het vorderen van identificerende gegevens op grond van art.

---

163 Wet politiegegevens, *Stb*. 2007, 300.
164 Wet justitiële en strafvorderlijke gegevens, *Stb.* 2000, 365.
165 In een kluis-PV is alle relevante informatie uit een opsporingsonderzoek opgenomen, zoals de naam van het onderzoek en de zaaksofficier, de regio waar het onderzoek wordt verricht en de toegepaste opsporingsmethoden en -bevoegdheden. Hoekendijk 2009, p. 41.

126nc Sv is van de notificatieplicht uitgezonderd. In de praktijk blijkt notificatie echter vrijwel niet plaats te vinden.[166] Een Amsterdamse officier van justitie: 'Dat gaat [bij de Wbvg] hetzelfde als bij andere bevoegdheden [in de BOB-paragraaf]: het wordt wel eens vergeten, het is een beetje een stiefkindje in de praktijk.' Sommige respondenten blijken niet goed op de hoogte te zijn van de notificatieplicht in relatie tot de Wbvg: 'Volgens mij is deze [wet] uitgezonderd van notificatie. Wij doen het in ieder geval niet. (…) Het is niet principieel, dat we dat niet doen, maar uit pragmatische overwegingen: we kunnen het niet bijhouden', aldus een officier van justitie uit Den Bosch.

Een Groningse officier van justitie is er niet van op de hoogte of notificatie plaatsvindt. 'We hebben een aparte BOB-administratie, ik neem aan dat zij geautoriseerd zijn om de notificatie te doen.' Ook een van de Amsterdamse officieren van justitie meldt dat notificatie door de administratie wordt afgehandeld en dat de officier van justitie daarbij niet betrokken is.[167] Een andere Groningse officier van justitie zegt echter: 'Op het parket in Den Haag deed ik dat zelf, daarvan weet ik zeker dat het gebeurde. Wat ik ervan weet, is dat de rechercheofficier dat doet. Het is geregeld, maar vraag me niet waar.' Eén van de geïnterviewde rechercheofficieren noemt de kwestie van de notificatieplicht een gewetensvraag. 'Wij doen dat wel, maar dan met een inhaalslag terug. Het is een groot landelijk probleem: we doen het als we er weer aan toe komen.'

7.3.5 Knelpunten in de praktijk

De Wbvg functioneert in de ogen van de vertegenwoordigers van het openbaar ministerie uitstekend. Er doen zich in de praktijk vrijwel geen knelpunten voor. Het belangrijkste nadeel, volgens de geïnterviewden, is dat de wet 'bewerkelijk' is. 'Vroeger kon een agent gewoon naar een pomphouder gaan en de beelden opvragen. Toen gebruikten we maar zelden een wettelijke vordering en nu moet het voor zo'n beetje alles.'

De geïnterviewden zijn ook geen van allen ooit geconfronteerd met het inroepen van weigeringsgronden door een gegevenshouder. Hooguit kan een

---

166 Deze constatering werd ook al gedaan in 2002, tijdens de eerste evaluatie van de Wet Bijzondere opsporingsbevoegdheden: slechts drie van de daarin geïnterviewde respondenten van het openbaar ministerie gaven te kennen genotificeerd te hebben. De onderzoekers noteren met gevoel voor understatement dat 'de notificatieplicht nog niet erg leeft'. Zie Bokhorst e.a. 2002, p. 115.

167 Op het moment dat het empirisch onderzoek ten behoeve van de onderhavige evaluatie plaatsvond, was men bij het parket Amsterdam bezig met het maken van een inhaalslag ten aanzien van het notificeren.

verstrekker de informatie niet uitleveren op de door de politie gewenste termijn, maar als er spoed geboden is, kan een vordering vaak alsnog met voorrang worden behandeld.

In het kielzog van functionarissen van de politie en de FIOD vinden ook alle respondenten van het openbaar ministerie de administratieve verplichtingen een nadeel. 'Bij banken vooral, dat je vraagt om het digitaal uit te leveren, als het gaat om een heleboel afschriften bijvoorbeeld, maar dat ze toch alles gaan uitprinten', aldus een van de parketsecretarissen. Ook gebeurt het dat een gegevensverstrekker de gevraagde gegevens in principe op vrijwillige basis zou kunnen verstrekken, bijvoorbeeld omdat hij of zij zelf slachtoffer is van een strafbaar feit (de pompstationhouder die overvallen is en camerabeelden ter beschikking stelt), maar dan toch om een vordering vraagt, aldus een van de Groningse officieren van justitie. 'Die beelden heb je nodig, maar dan wil de verstrekker toch een vordering uit angst voor claims van klanten. En dan sturen ze soms zelfs een rekening! Dat geldt niet alleen voor de banken, ook voor kleinere bedrijven.' Vooral voor de politie betekent de wet veel bureaucratie en administratieve rompslomp, die in sommige gevallen vertraging oplevert in opsporingsonderzoek: 'Het is allemaal administratie en dat is gevoeliger voor schrijffouten, maar onderzoeken lopen er niet op stuk. Het is arbeidsintensiever, maar niet moeilijker dan vóór de Wbvg', aldus een Groningse officier van justitie.

Geen van de geïnterviewden heeft tot op heden meegemaakt dat de verdediging (of de rechter) ter terechtzitting de rechtmatigheid van de gegevensvordering heeft bestreden. Volgens hen komt dat omdat de inbreuk die met de Wbvg op de privacy van de verdachte wordt gemaakt (vooral bij vorderingen op basis van art. 126nd Sv), slechts gering is. De rechter zou dan theoretisch gezien kunnen constateren dat er geen (juiste) vordering is gebruikt, maar zal tevens oordelen dat de verdachte daardoor niet (ernstig) in zijn verdediging is geschaad. De verdediging op haar beurt zal zich veeleer richten op de vraag hoe het openbaar ministerie tot verdenking is gekomen, en op de vermeende onrechtmatigheid van andere, ingrijpender, BOB-middelen. 'Het is vaak een kleiner onderdeel van een hele bewijsconstructie en daarmee maar van zijdelings belang', zo verklaart een van de Bossche officieren van justitie. Een collega: 'De Wbvg is vooral bedoeld ter bescherming van de gegevensverstrekker, niet ter bescherming van de verdachte. Dus de rechter zal niet veel consequenties verbinden aan een overtreding van art. 126nd Sv.'

Eén van de respondenten van het FP vindt het grootste probleem dat in de Wbvg niet duidelijk wordt omschreven wat 'een gegeven' is. 'Wanneer het om papier gaat kan een opsporingsambtenaar dat papier in beslag nemen op basis van art. 96a Sv. Maar als het om gegevens gaat, dan moet de officier van justitie vorderen op grond van art. 126nd Sv. Is een kopie van een factuur een ge-

geven of niet? En als je informatie op papier aangeleverd wilt krijgen, vraag je dan om een gegeven of een stuk?'

Een ander inhoudelijk probleem dat zich manifesteert is de uitzonderingspositie die in de Wbvg is gemaakt voor verschoningsgerechtigden. Van geheimhouders, zoals advocaten, kunnen geen gegevens worden gevorderd. Het gevolg is dat kwaadwillende (rechts)personen een verschoningsgerechtigde kunnen inschakelen als tussenpersoon, om aldus hun activiteiten af te schermen. Eén van de geïnterviewde officieren van justitie ziet dat nu al als een groot probleem. In een van diens onderzoeken, een zaak van oplichting, bleek het onmogelijk om het bewijs rond te krijgen omdat de verdachte bij alle zakelijke transacties een advocatenkantoor had betrokken, waardoor geen enkele informatie kon worden verkregen.

De kans is groot dat dit probleem in de toekomst zal groeien, aangezien sommige dienstverleners, die kennelijk weinig bezwaar hebben tegen het type klanten dat zij daarmee aantrekken, nu al min of meer openlijk adverteren met het feit dat degenen die gebruikmaken van hun dienstverlening, bijvoorbeeld als belastingadviseur, zich daarmee tevens buiten zicht plaatsen van de opsporingsinstanties. Bovendien kunnen bonafide geheimhouders die juist willen meewerken aan gegevensvorderingen als er sprake is van strafbare feiten, dat in de huidige context evenmin doen.

7.3.6 'Trans Link' en de gevolgen

In paragraaf 3.6 werd al gewezen op de gevolgen van de uitspraak in de zaak Trans Link voor de toepassing van de Wbvg, met name op het vlak van camerabeelden. In deze paragraaf wordt om te beginnen kort ingegaan op de (verwachte) gevolgen van de uitspraak voor de opsporingspraktijk. Vervolgens komen de reacties van Landelijke vergadering van rechercheofficieren van justitie (LROvJ) en van de grondlegger van de Wbvg, professor Mevis, aan de orde. Tot slot wordt ook kort stilgestaan bij de reactie van de regering op vragen die het Tweede Kamerlid Fred Teeven in juli 2010 over deze kwestie heeft gesteld.

De (verwachte) consequenties voor de opsporingspraktijk

De uitspraak door de HR in de zaak Trans Link wordt door alle betrokkenen met zorg bezien. In hoofdstuk 6 werd immers duidelijk dat camerabeelden, na financiële gegevens, het meest worden gevorderd. Als die voortaan in alle gevallen op basis van art. 126nf Sv zouden moeten worden opgevraagd, zijn de consequenties voor de opsporingsdiensten en het openbaar ministerie ingrijpend.

Ten eerste zijn aan de toepassing van art. 126nf Sv zwaardere voorwaarden verbonden dan aan art. 126nd Sv. Er moet immers niet alleen sprake

zijn van een 'voorlopige hechtenis feit' (art. 67, lid 1 Sv), maar ook van een misdrijf dat gezien zijn aard of de samenhang met andere door de verdachte begane misdrijven 'een ernstige inbreuk op de rechtsorde' oplevert. Vooral deze eis zou ertoe leiden dat camerabeelden in veel opsporingsonderzoeken niet meer zouden mogen worden opgevraagd.

In de tweede plaats vergt de toepassing van art. 126nf Sv een machtiging van de rechter-commissaris, en brengt deze dus een zwaardere procedure met zich mee. Hier lijkt in de praktijk echter wel een mouw aan te worden gepast. 'Wij hebben al afspraken gemaakt met de rechters-commissarissen. Zij tekenen [de vorderingen] gewoon, tot nu toe zijn er geen problemen', aldus een Amsterdamse officier van justitie.

Het standpunt van de LROvJ

De LROvJ heeft naar aanleiding van het Trans Link-arrest een voorlopig standpunt ingenomen, en daarin ook de visie van het College van Procureurs-Generaal in acht genomen.[168] De LROvJ geeft aan dat in zijn optiek in een aantal gevallen de toepassing van art. 126nf Sv niet nodig is.

In de eerste plaats betreft dat gevallen waarin de beelden vrijwillig worden afgegeven. 'Vrijwillig moet in dit verband worden verstaan als: spontaan afgegeven. De politie zal dus niet actief vragen om de gegevens.'

Vervolgens blijft het ook toegestaan dat opsporingsambtenaren zelf informatie uit de reisdocumentenadministratie opvragen (waaronder paspoortfoto's). Daarbij wordt wel de beperking aangebracht dat de gegevens noodzakelijk moeten zijn voor de opsporing van strafbare feiten in het kader van het onderzoek waarbij zij betrokken zijn, of voor zover die gegevens noodzakelijk zijn voor de uitoefening van de hun opgedragen werkzaamheden (conform art. 73 Paspoortuitvoeringsregeling). Dit standpunt is ook in lijn met de in paragraaf 3.6 besproken uitspraak van het Gerechtshof te Arnhem van 24 september 2009.

Ten derde is art. 126nf Sv niet van toepassing op camerabeelden die door politie en/of justitie zelf worden beheerd, zoals beelden van camera's die in een veiligheidsrisicogebied hangen. Er wordt dan immers niet gevorderd van een derde.

In de vierde plaats vallen beelden van strafbare feiten evenmin onder het bereik van art. 126nf Sv. Daarbij gaat het om situaties waarin algemeen bekend is dat er videobewaking is (bijvoorbeeld bij een bank of een benzinestation). Er mag worden aangenomen dat de wetgever niet de bedoeling heeft ge-

---

168 Standpunt Landelijke Vergadering Rechercheofficieren inzake de toepassing van art. 126nf Sv met inachtneming van het standpunt van het College d.d. 27 april 2010.

had de persoonsgegevens van een verdachte, die voor het oog van de camera strafbare feiten pleegt, te beschermen.

Belangrijk is ook dat beelden die afkomstig zijn van een camera die is opgesteld in een publieke ruimte eveneens niet hoeven te worden opgevraagd middels art. 126nf Sv, mits in de publieke ruimte kenbaar is gemaakt dat er beeldopnamen worden gemaakt.[169]

Het College [van Procureurs-Generaal] heeft bovendien het standpunt van de LROvJ onderschreven dat niet van alle camerabeelden op voorhand kan worden gezegd dat dit gevoelige gegevens zijn die vallen onder het regime van art. 126nf Sv, doch dat deze in de regel gevorderd kunnen worden onder art. 126nd Sv. Wanneer bedrijven beveiligingscamera's gebruiken om hun bedrijf te beveiligen, kunnen zij dit doen op grond van art. 8 Wbp. De beelden van personen worden dan niet beschouwd als gevoelige gegevens. Dit heeft onder meer te maken met het ontbreken van een directe koppeling tussen het beeldmateriaal en de namen van degenen die zijn opgenomen. Daarnaast is het doel beveiliging en niet identificatie of het verlenen van toegang. De verwerking vindt hiermee plaats tegen een geheel andere achtergrond dan wanneer het gaat om foto's in bijvoorbeeld een personeelsadministratie. Er wordt dus niet vanuit gegaan dat uit camerabeelden zonder meer gevoelige gegevens zoals ras kunnen worden afgeleid, mede omdat vooraf onbekend is van welke personen beelden worden gemaakt.

De informatie die wordt verkregen met het opvragen van camerabeelden is om die redenen dus niet te vergelijken met die van pasfoto's op identificerende pasjes. Dit betekent dat bijvoorbeeld voor het opvragen van rijbewijsfoto's wél een machtiging van de rechter-commissaris nodig is. De LROvJ stelt overigens nog wel dat 'in geval van dringende noodzaak de officier van justitie mondeling de gegevens [kan] vorderen van degene van wie redelijkerwijs kan worden vermoed daar toegang tot te hebben'. Mondelinge machtiging door de rechter-commissaris is sinds kort eveneens mogelijk.[170]

Het standpunt van professor Mevis in diens annotatie bij 'Trans Link'[171]

De grondlegger van de Wbvg, professor Mevis, heeft zich in een annotatie uitgesproken over het arrest Trans Link. Hij legt het accent bij de voorzienbaarheid van de gevoeligheid van gegevens, op het moment dat het openbaar ministerie deze vordert. Als de officier van justitie op dat moment reeds weet dat de gege-

---

169 Zie paragraaf 3.6 met betrekking tot de uitspraak van de Rb. Zutphen d.d. 15 april 2010, *LJN* BM1196.

170 Zie *Stb*. 2009, 525.

171 Annotatie bij HR 23 maart 2010, *NJ* 2010, 355.

vens rechtstreeks gevoelige informatie zullen bevatten, dan is art. 126nf Sv de enig mogelijke weg om de gegevens te vorderen, dus uitsluitend met een machtiging van de rechter-commissaris.

Een andere categorie gegevens is volgens Mevis die welke als 'bijvangst' kan worden gekwalificeerd: het openbaar ministerie vordert in een opsporingsonderzoek allerhande informatie en treft daarbij per ongeluk ook gevoelige gegevens aan. Als er dan is gevorderd op basis van art. 126nd Sv, is dat niet onrechtmatig gebeurd.

Uit het standpunt van Mevis valt overigens wel op te maken dat er een vorm van zorgplicht bestaat voor het openbaar ministerie. Dat moet van tevoren nagaan (en misschien ook wel verantwoorden of expliciteren) dat het voorziet dat er geen gevoelige gegevens gevorderd worden. Laat het deze exercitie na, dan neemt het openbaar ministerie het immers op de koop toe dat er tóch gevoelige gegevens aangetroffen worden en dat de voorzienbaarheid daarvan het openbaar ministerie achteraf verweten kan worden.

Deze zorgplicht vloeit voort uit de (tamelijk ingewikkelde) overweging van Mevis onder punt 3 van zijn annotatie: het doet er niet toe wat de bedoeling is van het openbaar ministerie bij het vorderen van (potentieel gevoelige) gegevens, en ook niet of het van plan is die gegevens daadwerkelijk in het opsporingsonderzoek te gebruiken. Het blote feit dat die gegevens ter kennis komen van justitie rechtvaardigt dat ze (extra) beschermd worden. Deze opvatting van de HR wordt onderbouwd door de wetsgeschiedenis van de Wbp, ook al is er een enkel Kamerstuk uit de wetsgeschiedenis van de Wbvg waarin mogelijk een afwijkende opvatting is te vinden. Overigens wordt van de opsporende instantie niet het onmogelijke gevergd: dát er zich gevoelige kenmerken in de gevorderde gegevens kunnen bevinden, moet 'voldoende te voorspellen zijn'. De aanduiding van de HR dat de gevoeligheid uit de gegevens 'kan worden afgeleid' is te vaag, aldus Mevis.

Volgens Mevis hanteert de HR in dezen een betrekkelijk streng standpunt. Los daarvan gaat het in dit geval om duidelijke, heldere foto's waarop iemand goed herkenbaar moet zijn (het gaat om foto's ter identificering, onder andere om fraude met de chipkaarten tegen te gaan). Dan gaat het al snel om gevoelige gegevens, die moeten worden gevorderd op basis van art. 126nf Sv, aldus Mevis. Daarbij lijkt het ons ook relevant dat de gegevens, in dit geval de pasfoto's, door de betrokkene zelf aan de betreffende instantie zijn verstrekt. Juist spontane verstrekking van gegevens, waarbij de burger erop vertrouwt dat er zorgvuldig mee wordt omgesprongen, zou extra bescherming dienen te krijgen

Ander beeldmateriaal, bijvoorbeeld van bewakingscamera's, ook uitsluitend te vorderen op basis van art. 126nf Sv, zou volgens Mevis zowel onpraktisch zijn, als 'raar' (wij begrijpen: niet consistent met de wetssystematiek),

want dergelijke bewakingscamera's zijn juist bedoeld om gegevens te verzamelen voor de opsporing van strafbare feiten die geen ernstige inbreuken op de rechtsorde opleveren. Dit 'ernstvereiste' is in art. 126nf Sv opgenomen als een extra waarborg voor het vorderen van gevoelige gegevens in het kader van de opsporing van strafbare feiten. Als ook voor het vorderen van 'simpele' beelden van bewakingcamera's een machtiging van de RC vereist is, dan kan dit vorderen in de praktijk niet meer plaatsvinden (omdat camerabeelden de drempel van het ernstvereiste niet passeren) en zal de Wbvg worden omzeild door inbeslagneming van de beelden of door een beroep te doen op vrijwillige verstrekking door de gegevenshouder. Dat is in de ogen van Mevis een onwenselijke uitkomst.

De HR geeft in zijn uitspraak geen antwoord op de vraag hoe in de toekomst camerabeelden gevorderd zullen moeten worden, maar laat wel doorschemeren dat zijn beslissing niet tot foto's beperkt is. Het valt dus niet uit te sluiten dat ook beelden van bewakingscamera's uitsluitend op grond van art. 126nf Sv te vorderen zijn. Mevis probeert een aanknopingspunt te vinden in het Vrijstellingsbesluit Wbp, dat bepaalt dat beelden van beveiligingscamera's niet onder art. 16 Wbp worden geschaard (beelden die gevoelige gegevens 'betreffen'). Maar ook hij erkent dat het giswerk is: er is eenvoudigweg geen duidelijke regeling die uitmaakt wanneer beeldmateriaal gevoelige gegevens bevat en wanneer niet. Bovendien hoeft het niet zo te zijn dat de wijze waarop een en ander in de Wbp is geregeld, op dezelfde wijze in strafvordering moet terugkeren. Misschien moet er voor strafvorderlijk gebruik wel een strengere toets worden toegepast.

Volgens Mevis kan de ontstane problematiek op twee manieren worden opgelost. Ten eerste kan worden bepaald dat camerabeelden geen gevoelige gegevens zijn, behalve wanneer het openbaar ministerie erop uit is het 'ras' van de verdachte te achterhalen op basis van deze beelden. De tweede optie is het laten vervallen van het 'ernstvereiste' in art. 126nf Sv, zodat dit artikellid in een ruimere verzameling van gevallen kan worden gebruikt. Volgens Mevis is de tweede optie de veiligste en de te prefereren weg, omdat hij het zorgvuldigst is. Het openbaar ministerie weet dan zeker dat er gebruik is gemaakt van de juiste grondslag voor de vordering. Mochten er gevoelige gegevens als bijvangst bij de beelden worden aangetroffen, dan zijn die in ieder geval rechtmatig gevorderd.

Wij kunnen ons bij het standpunt van Mevis aansluiten. Uit het empirische deel van dit onderzoek blijkt dat in de opsporingspraktijk veel camerabeelden worden gevorderd, juist in gevallen van relatief eenvoudige strafbare feiten. Deze feiten zullen niet voldoen aan het ernstvereiste dat als voorwaarde voor toepassing van art. 126nf Sv is geformuleerd. De vraag is of dat wenselijk is. Om de systematiek van de Wbvg niet te doorbreken en om geen rechtsonzekerheid te doen ontstaan, is het laten vervallen van het ernstvereiste een beter idee

dan te bepalen dat camerabeelden niet gevoelig zijn. De consequentie van een dergelijke verandering van de Wbvg is vanzelfsprekend wel dat de RC meer werk krijgt, en de (administratieve) procedure wordt uitgebreid.

Het antwoord van de minister van Justitie op Kamervragen inzake Trans Link

Naar aanleiding van de uitspraak in de zaak Trans Link heeft het Tweede Kamerlid Fred Teeven (VVD) vragen gesteld aan de minister van Justitie over de gevolgen van de uitspraak voor de politie- en justitiepraktijk.[172] De minister sluit daarbij aan, maar dat mag geen verrassing heten, bij de overwegingen die hiervoor al de revue zijn gepasseerd.

De minister van Justitie benoemt als gevolgen voor de praktijk dat in ieder geval vorderingen ten behoeve van gegevensverwerking met betrekking tot *pasfoto's, in combinatie met andere persoonsgegevens*, voortaan alleen na rechterlijke machtiging kunnen worden gedaan. Volgens de minister behoren beelden van particuliere bewakingscamera's echter tot een andere categorie dan een bestand met pasfoto's en daaraan gekoppelde andere persoonsgegevens. 'In geval van pasfoto's op toegangspasjes is er een koppeling met andere persoonsgegevens, gekoppeld aan het verlenen van toegang of andere rechten. In geval van bewakingscamera's is vooraf onbekend of en van welke personen beelden worden gemaakt en wat daarop wel of niet zichtbaar zal zijn. Ook zijn daarbij geen andere persoonsgegevens bekend. Dergelijke camerabeelden worden om die reden bij de toepassing van de Wbp niet als bijzondere persoonsgegevens gezien', aldus de minister. Aan dergelijke 'bijzondere persoonsgegevens' (in de zin van art. 16 Wbp) komt een andere bescherming toe dan aan gegevens die deze status niet hebben. In de praktijk van het opsporingsonderzoek is het de officier van justitie die beoordeelt of er sprake is van bijzondere persoonsgegevens en of deze gevorderd moeten worden. Als dat het geval is, dan dient het openbaar ministerie daartoe een verzoek in te dienen bij de rechter-commissaris.

Uit de antwoorden die de minister geeft, blijkt dat hij de lijn van de HR volgt ten aanzien van de bijzondere bescherming voor beeldmateriaal die kan worden gekoppeld aan persoonsgegevens. De minister sluit echter de beelden van bewakingcamera's uit van de categorie 'bijzondere persoonsgegevens', zij het dat hij het eindoordeel aan de officier van justitie over laat.

---

172 Aanhangsel Handelingen, vergaderjaar 2009-2010, nr. 2724.

7.3.7 Algemeen oordeel over de Wbvg: verbetering?

Tot slot van deze paragraaf volgt het algemene oordeel van de respondenten die namens het openbaar ministerie aan het onderhavige onderzoek hebben meegewerkt. Deze wijkt maar weinig af van het oordeel van de opsporingsmedewerkers van de politie en de FIOD.

Ook de officieren van justitie waarderen de verbeterde zorgvuldigheid die de Wbvg met zich mee heeft gebracht. 'Het vorderen van gegevens is een bewuste beslissing van het openbaar ministerie geworden, dat is een verbetering', zo geeft een van de parketsecretarissen aan. Een Bossche officier van justitie vindt de stroomlijning van de procedure van gegevensvordering een voordeel: 'Voorheen moest je zoeken naar welke instantie de betreffende gegevens zou hebben. Voor de gegevensverstrekkers is het ook prettig dat ze gedekt zijn.' Zij krijgt bijval van een collega: 'in het verleden wilde een bank soms niet meewerken zonder dat een onafhankelijke rechter werd ingeschakeld. Dan namen we een rechter-commissaris mee en dan wilden ze wel meewerken. De samenwerking [met gegevensverstrekkers] was grillig en willekeurig in het verleden, dat is nu verbeterd.'

Als belangrijkste nadeel van de Wbvg noemen de geïnterviewden de toegenomen administratieve belasting. 'Het is wel heel veel meer papierwerk geworden, dat is minder praktisch. Je snelheid en je slagkracht in een onderzoek zijn daardoor wat afgenomen', aldus een parketsecretaris. Een Amsterdamse officier van Justitie verlangt terug naar de tijd vóór de Wbvg: 'het is veel te veel papierwerk nu, vooral voor de politie. Dingen die vroeger gemakkelijk gingen, daar is nu veel werk aan. De gegevensvordering is nu duidelijker, dat is waar, maar die papierwinkel is een nadeel.' Een Groningse officier van justitie merkt 'niet veel verschil ten opzichte van de tijd vóór de Wbvg. Het is wel veel meer werk dan voorheen, maar dat zit hem ook in andere zaken. Er is steeds meer formalisering en zelfs een zekere achterdocht [van de zittende magistratuur] naar politie en justitie, en die vind ik onterecht.'

De ontwikkelingen naar aanleiding van de discussie over het opvragen van camerabeelden en foto's worden met belangstelling, maar ook zorg gevolgd: 'Ik ben benieuwd hoe het nu gaat met de Trans Link-uitspraak. Die haalt namelijk heel veel snelheid uit je onderzoek.'

Een bijzonder aandachtspunt is dat de Wbvg niet regelt hoe gegevenshouders informatie moeten aanleveren. De gedachte daarachter is waarschijnlijk dat deze dit als vanzelf op de meest efficiënte manier doet, maar daarvan is in de praktijk, en dan met name bij banken en geldinstellingen, niet altijd sprake.

7.4 Besluit

Uit de interviews met de opsporingsdiensten en het openbaar ministerie blijkt dat de Wbvg niet meer uit de opsporingspraktijk is weg te denken. Er wordt veelvuldig gebruikgemaakt van de wet, om allerlei uiteenlopende informatie te verzamelen. Het van kracht worden van de Wbvg heeft inhoudelijk geen grote veranderingen voor de praktijk met zich meegebracht, aangezien dezelfde informatie voorheen ook al werd verzameld. Procedureel heeft de wet wel voor een verandering gezorgd, aangezien het opvragen van gegevens bij derden meer is geformaliseerd.

De procedures die voortvloeien uit de Wbvg zijn duidelijk en werkbaar. Tussen de opsporingsdiensten en het openbaar ministerie bestaan korte lijnen, zeker in de opsporingsonderzoeken die worden geleid door een zaaksofficier van justitie. Ook de relatie met de gegevenshouders is goed: in vrijwel alle gevallen werken ze mee aan het uitleveren van de gevorderde gegevens. Hooguit is er soms sprake van een oplopende wachttijd, zeker bij gegevenshouders die met veel vorderingen te maken krijgen, maar opsporingsonderzoeken lopen niet stuk op de vertraging.

Vrijwillige gegevensverstrekking lijkt met de introductie van de Wbvg niet helemaal verdwenen te zijn, maar toch voor een groot deel ingeperkt. De wet is inmiddels breed bekend, dus in theorie zou er geen opsporingsambtenaar meer moeten zijn die niet weet dat vrijwillige gegevensverstrekking tot het verleden behoort. Opsporingsdiensten willen bovendien geen procesrisico lopen en zullen ervoor zorgen dat ze kunnen verantwoorden hoe opsporingsinformatie verzameld is en dat daarbij de juiste procedures zijn doorlopen.

Ook de gegevenshouders zijn over het algemeen goed op de hoogte van hun rechten en plichten rondom het uitleveren van gegevens, en zij zijn niet (meer) bereid vrijwillig informatie te verstrekken. Los hiervan komt het in de praktijk nog voor dat materiaal vrijwillig aan de opsporingsdiensten wordt geleverd, bijvoorbeeld door getuigen of door de aangever van een strafbaar feit. Deze incidentele gevallen waren door de wetgever al voorzien bij het ontwerp van de Wbvg. Derden zijn immers in beginsel vrij op eigen initiatief een bijdrage te leveren aan de opsporing van strafbare feiten door van bepaalde feiten of omstandigheden melding te doen aan de politie of anderszins informatie aan de politie te verstrekken.

Uit de interviews met de medewerkers van de politie en de FIOD blijkt dat vrijwillige verstrekking vooral voorkomt bij aangiften, als de aangever spontaan materiaal overhandigt dat de opsporing ten gunste kan zijn. Ook komt het voor dat een getuige een verklaring aflegt omtrent wat hij over het strafbare feit

heeft waargenomen. Daarbij kan hij (spontaan) stukken overhandigen. Op deze gevallen van aangevers en getuigen heeft de Wbvg geen betrekking, hoewel het incidenteel voorkomt dat een aangever of een getuige toch vraagt om een vordering, om zichzelf tegen mogelijke claims van klanten te kunnen indekken.

Waar het gaat om de afstemming met andere wettelijke bevoegdheden die het mogelijk maken gegevens van derden te vorderen, blijkt in de praktijk dat de Wbvg een zekere voorrang geniet (in ieder geval bij de FIOD-medewerkers). De Wbvg wordt als een relatief 'licht' opsporingsmiddel beschouwd, dat niet meer dan een geringe inbreuk maakt op de privacy van betrokkenen. Dit geldt in het bijzonder voor art. 126nc Sv en 126nd Sv, die in de praktijk het meest van alle Wbvg-bevoegdheden worden toegepast. In specifieke gevallen wordt (ook) gebruikgemaakt van andere bevoegdheden, zoals het opvragen van pasfoto's op grond van de Paspoortuitvoeringsregeling, de inbeslagneming in fiscale onderzoeken op grond van art. 81 Awr en de strafvorderlijke inbeslagneming op grond van art. 96a Sv.

De opsporingsdiensten en het openbaar ministerie waarderen de toegenomen zorgvuldigheid van de procedure van het vorderen van gegevens bij derden door de komst van de Wbvg. De medewerkingsplicht heeft een einde gemaakt aan soms langdurige discussies met privacyexperts van een gegevenshouder en de juridische waarborgen van de procedure zijn niet alleen voor de gegevenshouders, maar ook voor de opsporingsdiensten een wenselijk kader. Het belangrijkste nadeel van de Wbvg is evenwel de evidente toename van administratieve handelingen. Voordat gevorderde gegevens aan het procesdossier kunnen worden toegevoegd moet een heel aantal processen-verbaal geproduceerd worden, die de gegevensvordering inbedden. De uitspraak in de zaak Trans Link, zij het dat die inmiddels iets genuanceerd wordt door recentere rechtspraak, de annotatie van Mevis en de antwoorden die de minister van Justitie op Kamervragen heeft geformuleerd, worden dan ook met een zekere moedeloosheid ontvangen door de opsporingsdiensten en het openbaar ministerie, omdat men nog meer 'papierwerk' verwacht en een extra 'schijf' in de afwikkeling van vorderingen in de vorm van de rechter-commissaris. Vanuit de praktijk komt (dan ook) een nadrukkelijke wens de gang van zaken rond het vorderen van gegevens te vereenvoudigen, bijvoorbeeld door een verschil te maken naar de soort gegevens die worden gevorderd en door een onderscheid aan te brengen al naar gelang de bereidheid tot medewerking van de gegevenshouders. Dat die wens bestaat, is vanuit de optiek van de opsporingsdiensten wellicht begrijpelijk, maar of ze ingelast kan worden, is de vraag, gegeven de nadrukkelijke bescherming van het privacybelang van de burger, welk belang door de zaak Trans Link nog eens benadrukt is.

8 De toepassing van de wet: het perspectief van de gegevenshouders

8.1 Inleiding

In de Wbvg zijn waarborgen opgenomen die dienen ter bescherming van de gegevensverstrekker. De wet schrijft daartoe ten eerste voor dat van derden niet kan worden verlangd dat zij informatie vastleggen die niet al in het kader van de gewone bedrijfsvoering wordt geregistreerd. Ten tweede moeten de vorderingen precies zijn geformuleerd (het bepaaldheidsvereiste). Tot slot mogen gegevenshouders zo min mogelijk worden belast met de afhandeling van vorderingen. De vraag die in dit hoofdstuk centraal staat, is in hoeverre aan deze waarborgen in de praktijk ook wordt voldaan.

In hoofdstuk 6 bleek al dat financiële instellingen bij een relatief hoog percentage van de Wbvg-vorderingen de aangezochte gegevenshouders zijn. Om die reden is in dit hoofdstuk dan ook een onderscheid gemaakt tussen financiële instellingen enerzijds en de overige gegevenshouders anderzijds.[173] De beide categorieën komen aan de orde in respectievelijk paragraaf 8.2 en 8.3. In paragraaf 8.4 worden de bevindingen uit dit hoofdstuk kort op een rij gezet.

8.2 Financiële instellingen

8.2.1 Aantal vorderingen en werkbelasting

Financiële instellingen krijgen dagelijks tientallen vorderingen van de opsporingsdiensten en het openbaar ministerie om gegevens te verstrekken. De aantallen variëren bij de geïnterviewde bedrijven van tien tot veertig vorderingen per dag. Uit cijfers van ABN Amro blijkt dat zij, in 2008, 3800 vorderingen op grond van de Wbvg ontvingen, waarvan 1500 stuks op basis van art. 126nc Sv en 2300 op basis van art. 126nd Sv. De Nederlandse Vereniging van Banken telde in 2008 in totaal 6000 vorderingen op basis van art. 126nc Sv, 7000 op grond van art. 126nd Sv en 44 op basis van art. 126ne Sv.

De geïnterviewde vertegenwoordigers van banken melden dat het aantal verzoeken op basis van de Wbvg in de afgelopen jaren is toegenomen. Volgens de Nederlandse Vereniging van Banken is het aantal vorderingen tussen 2007 en 2009 met 50 procent gestegen. Niet alleen de absolute aantallen nemen toe, ook

---

[173] Onder financiële instellingen zijn hier verstaan: banken, Equens en de Nederlandse Vereniging van Banken.

de samenstelling van de vorderingen verandert: steeds vaker worden van een verdachte niet alleen de bankafschriften met betrekking tot een bepaalde tijdsperiode gevorderd, maar ook diens hypotheekdossier, zijn IP-adres en camerabeelden van pintransacties. Voorts vragen opsporingsdiensten in toenemende mate in een vordering gegevens over een groep personen. 'Er is niet alleen een toename aan bevelen maar ook een toename aan subbevelen in een bevel', aldus een van de respondenten. De geïnterviewde vertegenwoordigers van financiële instellingen geven aan dat deze diversiteit aan informatie niet altijd kan worden geleverd, wat dan tot de nodige discussie met de opsporingsinstanties leidt.

De financiële instellingen geven aan dat de vorderingen op basis van art. 126nc Sv het minste tijd in beslag nemen. Deze identificerende gegevens zijn vaak op eenvoudige wijze uit de administratie te genereren. De vorderingen die worden gedaan op basis van art. 126nd Sv (historische gegevens) leveren daarentegen veel meer werk op voor de banken.

Een verzoek op grond van art. 126nd Sv wordt veelal voorafgegaan door een telefonische voorvraag van de zijde van de opsporingsinstantie. Dit betreft de zogeheten ja/nee-vraag die wordt gebruikt om te achterhalen of de betreffende instantie over de gewenste gegevens beschikt. Voor deze voorvraag is, zoals in hoofdstuk 3 werd uiteengezet, geen schriftelijke vordering vereist. Als blijkt dat de gegevenshouder over de gevraagde informatie beschikt, wordt een vordering op papier opgesteld (ondertekend door de officier van justitie) en per fax of e-mail verzonden naar de instelling.

Gedurende de afhandeling van de vordering is in veel gevallen (telefonisch of per e-mail) contact tussen de bank en de opsporingsinstantie, om te garanderen dat de juiste gegevens worden uitgeleverd. De bankinstellingen vermelden dat er soms veel tijd gemoeid is met het verduidelijken van de oorspronkelijke vordering. Ook komt het voor dat er door de opsporingsdienst fouten worden gemaakt in de vordering, en deze moet worden teruggestuurd met het verzoek om aanpassing. De door de opsporingsdiensten gevraagde informatie wordt bovendien niet door alle banken centraal bijgehouden, waardoor het voldoen aan de vorderingen tijdrovend is.

8.2.2 Procedure

De meeste (groot)banken beschikken over een speciale afdeling die de vorderingen beoordeelt en afhandelt. Niet zelden zijn hier medewerkers werkzaam met een verleden bij de politie of bij andere opsporingsinstanties.

De financiële instellingen werken uitsluitend op basis van schriftelijke vorderingen, die duidelijk en ondubbelzinnig moeten zijn opgesteld. Bij het merendeel van de vorderingen is dat ook het geval. Indien er wel vraagtekens zijn,

interpreteren de financiële instellingen niet zelf wat de bedoeling van de vordering is, maar sturen zij het bevel terug met de vraag om verduidelijking. Deze opstelling wordt door opsporingsinstanties vanzelfsprekend niet altijd geapprecieerd. Enkele respondenten melden – overigens in uitzonderlijke gevallen en in het bijzonder indien er sprake is van een onervaren opsporingsambtenaar – te zijn geconfronteerd met bluf of zelfs met intimidatie om ervoor te zorgen dat de gewenste gegevens worden geleverd. 'Dan zeggen ze: we komen het wel halen, of: u krijgt last met de officier van justitie', aldus een van de respondenten.

De zogeheten ja/nee-vragen zijn een bekend verschijnsel voor financiële instellingen en die leveren in de praktijk geen problemen op. Voor de banken biedt een dergelijke voorvraag ook gelegenheid om alvast te anticiperen op de feitelijke vordering.

8.2.3 Vrijwilligheid

Eén van de centrale elementen in de Wbvg is de doelstelling om aan de figuur van vrijwillige gegevensverstrekking een eind te maken. Inderdaad stelt geen enkele geïnterviewde financiële instelling nog op basis van vrijwilligheid gegevens uit te leveren. De procedures zijn geformaliseerd en er wordt gewerkt met contactpersonen. De Nederlandse Vereniging van Banken heeft een lijst met contactpersonen opgesteld voor de politie die zij in het geval van informatievragen dienen te benaderen.[174]

Daarmee is overigens niet volledig uitgesloten dat nog op vrijwillige grond gegevens worden verstrekt. Een voorbeeld is een situatie waarin een politiefunctionaris een lokaal filiaal van een kleine bank binnenloopt, daar informeert naar beschikbare gegevens in het kader van een gepleegd strafbaar feit en die gegevens zonder onderliggende vordering uitgeleverd krijgt, in plaats van door de bankmedewerker te worden doorverwezen naar een contactpersoon.

Vrijwillige verstrekking komt ook voor wanneer de financiële instelling zelf slachtoffer is geworden van een strafbaar feit. In dat geval doet het bedrijf immers uit eigen initiatief aangifte en staat het vrij ook andere gegevens, zoals camerabeelden, aan de opsporingsdienst te verstrekken. Hierbij moet overigens worden opgemerkt dat een situatie waarin de gegevenshouder op eigen initiatief informatie aanreikt, buiten de kaders van de Wbvg valt (zie hoofdstuk 3).

---

[174] Deze lijst kan elke politiefunctionaris via het intranet (Politie Kennis Net) raadplegen.

8.2.4 Waarborgen ter bescherming van de gegevensverstrekkers

Bedrijven, instellingen of individuen die te maken krijgen met een vordering om informatie door een opsporingsinstantie dienen daarmee zo min mogelijk te worden belast, zo luidt een uitgangspunt van de Wbvg. Ook daarvoor zijn waarborgen in de wet opgenomen. Zo mag van derden niet worden verlangd dat zij informatie vastleggen die niet in het kader van de gewone bedrijfsvoering wordt geregistreerd. Een vordering dient voorts 'gericht en bepaald' te zijn. Te algemeen geformuleerde of op de verkeerde grondslag gebaseerde vorderingen hoeven door een instelling niet in behandeling te worden genomen.

In de praktijk voldoen vorderingen niet altijd aan het bepaaldheidsvereiste, aldus de respondenten van de financiële instellingen. Geïnterviewden van een van de banken verwoorden dat als volgt: 'Onze indruk is soms dat [de opsporingsdiensten] zelf niet weten wat ze opvragen. Ze vragen maar alles op in de hoop dat er iets bij zit dat ze kunnen gebruiken.' Een vertegenwoordiger van een andere bank heeft vergelijkbare ervaringen: 'Het eerste waar ze mee beginnen in de opsporing, is het vorderen van gegevens en dat doen ze dan zo breed mogelijk: trek het bankdossier maar leeg.' Een derde sluit aan: 'Vaak wordt er gezegd: ik wil alle gegevens van die klant. Ze [de opsporingsinstanties] moeten zo eenduidig mogelijk zijn, maar dat zijn ze niet altijd. Wij bellen dan met de opsporingsinstantie en dan volgt er een discussie omdat wij het niet concreet genoeg vinden.' Tot slot wordt volgens de Nederlandse Vereniging van Banken: 'niet eerst gekeken of er een andere manier is, er wordt heel gemakkelijk een vordering neergelegd. Het is gemakkelijk voor de politie, er wordt niet echt een afweging gemaakt of het nuttig of noodzakelijk is. (...) Politie en justitie zetten zo breed mogelijk in: doet u maar het dossier, dan kijken wij wel wat bruikbaar is.' In een heel enkel geval leidt een kritische vraag van een financiële instelling bij een in hun ogen (te) ruim geformuleerde vordering van de opsporingsdiensten tot discussies, waarbij eventueel ook druk kan worden uitgeoefend op de gegevenshouder.

Op grond van de interviews kan moeilijk worden geschat of het in de voornoemde gevallen gaat om incidenten of om regelmatige voorvallen. Het lijkt er echter op dat het eerste het geval is. Ten behoeve van de onderhavige evaluaties is ook een aantal dossiers inhoudelijk nader geanalyseerd. Daaruit blijkt, zo werd al in hoofdstuk 5 beschreven, dat er in eenvoudige opsporingsonderzoeken meestal geen sprake is van ruim geformuleerde vorderingen: er wordt dan zeer gericht gevraagd naar specifieke rekeningnummers of transacties, over een afgebakende periode.

Breed geformuleerde vorderingen kunnen daarentegen wel aan de orde zijn in opsporingsonderzoeken waarin nog maar beperkt informatie voorhanden is over betrokkenen of over gebeurtenissen die zich hebben afgespeeld, of waarin het illegale activiteiten betreft die nog gaande zijn. In die gevallen zullen opsporingsinstanties inderdaad nog geen goed beeld hebben van de gegevens die mogelijk voor de bewijsvoering van belang kunnen zijn, en of die aanknopingspunten kunnen bieden voor nader onderzoek. Ook kunnen in lopende onderzoeken, bijvoorbeeld via een telefoontap, vage aanwijzingen binnenkomen over financiële transacties die zeer lastig te preciseren zijn.

In zulke gevallen ligt het dilemma voor dat een zoekvraag pas in te perken valt wanneer duidelijk is wat er precies aan informatie voorhanden is. Men kan uiteraard ook stellen dat de opsporingsinstantie de zoekvraag, en de aanleiding daarvan, dan maar gedetailleerder moet toelichten om deze nader af te kunnen bakenen. Dat is echter weer niet wenselijk omdat de aard van het opsporingsonderzoek vertrouwelijk dient te blijven.

8.2.5 Beklagregeling

Art. 552a lid 1 Sv biedt gegevensverstrekkers de mogelijkheid zich schriftelijk bij de rechtbank te beklagen over een vordering van gegevens. Uit de interviews blijkt dat geen van de financiële instellingen van deze regeling gebruik heeft gemaakt. Eén van de respondenten noemt de beklagregeling ‘een dode letter’, omdat er in de praktijk een verplichting tot meewerken is. Hij verwacht voor de oplossing van knelpunten meer van de afspraken die op landelijk niveau worden gemaakt door de Nederlandse Vereniging van Banken. Andere geïnterviewden zeggen geen gebruik te maken van de regeling omdat ze de relatie met de opsporingsdiensten en met het openbaar ministerie goed willen houden: ‘Als we ontevreden zijn over de gang van zaken, dan bellen we met het openbaar ministerie of de politie en praten we het uit. Maar we hebben nog nooit een officiële klacht bij de rechtbank ingediend.’

8.2.6 Knelpunten

De vertegenwoordigers van financiële instellingen dragen hoofdzakelijk drie, deels samenhangende, knelpunten aan in relatie tot de Wbvg. Het betreft de tijdrovendheid van het afhandelen van gegevensvorderingen, de declaratie van de kosten die daarmee gepaard gaan en het stijgende aantal vorderingen.

De tijd die gemoeid is met de afhandeling van vorderingen neemt volgens de financiële instellingen toe omdat het aantal vorderingen een stijgende lijn vertoont, ze steeds uitgebreider worden en er fouten in gemaakt worden die

extra overleg en aanpassingen vergen. Bovendien kunnen de meeste instellingen volgens eigen zeggen niet 'met een druk op de knop' aan de vorderingen voldoen, terwijl zij de indruk hebben dat bij de opsporingsinstanties dat beeld wel bestaat. Opsporingsdiensten willen de gegevens vaak op zeer korte termijn ontvangen, maar daaraan kunnen de financiële instellingen doorgaans niet voldoen. Voorts willen de banken de gegevens niet digitaal uitleveren. Zij stellen dat veiligheidsoverwegingen daarbij het punt vormen. Deze opstelling betekent dat alle gegevens worden geprint en op papier uitgeleverd, wat niet alleen tijdrovend(er) is, maar ook tot praktische knelpunten leidt als het moeten achterhalen van het postadres van de betreffende opsporingsdienst.

Het tweede probleem, de kosten die gepaard gaan met de uitlevering van gegevens, houdt verband met het feit dat de vergoedingen die in het landelijke convenant[175] zijn opgenomen, volgens de vertegenwoordigers van de banken en geldinstellingen de werkelijk gemaakte kosten onvoldoende dekken. Bovendien is het in de praktijk soms onduidelijk aan wie de rekening verstuurd kan of moet worden, omdat politie en justitie naar elkaar verwijzen. Op dit moment is er zelfs een aantal banken dat niet meewerkt aan het uitleveren van gegevens, tot het moment dat nog openstaande rekeningen door politie en justitie betaald zijn.

Tot slot is sprake van een toename van de hoeveelheid vorderingen en alle geïnterviewde vertegenwoordigers van financiële instellingen verwachten dat dit aantal in de toekomst verder zal stijgen, zoals ook in de afgelopen jaren het geval is geweest. Vooral de vestigingen van banken in de vier grote steden zouden nu al 'continu' bezig zijn met het afhandelen van Wbvg-vorderingen. Een aantal banken heeft inmiddels een werkachterstand opgebouwd, wat consequenties heeft voor het tijdig uitleveren van gegevens. In de beleving van de financiële instellingen was het moeten betalen voor uitgeleverde gegevens juist bedoeld om het aantal vorderingen in te perken, maar die drempel heeft in de praktijk evenwel weinig effect. De vraag is overigens of deze perceptie correct is, aangezien ook voor het van kracht worden van de Wbvg al een vergoedingsregeling bestond, specifiek voor banken en geldinstellingen. Opvallend genoeg ontbreekt zo'n regeling geheel ten aanzien van de telecomproviders, die in nog sterkere mate te maken hebben met verzoeken van opsporingsinstanties.

---

[175] Bedoeld wordt de Aanwijzing gegevensverstrekking financiële dienstverleners (2004A002), *Stcrt.* 2004, 95. De vergoedingsregeling is €10,- per identificerend gegeven en in de overige gevallen €70,- per uur voor de tijd die gemoeid is met de vordering tot uitlevering van bescheiden en verstrekking van gegevens.

8.3 Niet-financiële instellingen

8.3.1 Aantal vorderingen en werkbelasting

Naast de financiële instellingen zijn in dit hoofdstuk de andere gegevenshouders onderscheiden. De overige geïnterviewde bedrijven en instellingen ontvangen aanmerkelijk minder vorderingen tot het verstrekken van gegevens. De aantallen variëren van een keer in de twee maanden (bij benzinestations) tot 170 vorderingen per jaar (bij Holland Casino) en 40 per maand bij de Nederlandse Spoorwegen. Omdat de aantallen vorderingen kleiner zijn dan bij de financiële instellingen, is de belasting voor de gegevensverstrekker navenant geringer. Bij de benzinestations gaat het bovendien vrijwel uitsluitend om camerabeelden, die tegenwoordig digitaal worden opgenomen en opgeslagen. Voor de pompstationhouder is het veiligstellen van de beelden een kleine moeite. Voor een gegevensverstrekker als Holland Casino is de belasting groter, omdat het in de vorderingen aan dit bedrijf niet alleen gaat om het uitleveren van camerabeelden (hoewel dat het grootste deel van de verzoeken betreft), maar ook om bezoekersgegevens en om afschriften van overgeboekte speelwinsten of bedragen waarvoor speelfiches zijn gekocht.

8.3.2 Procedure

Evenals de financiële instellingen hanteren ook de meeste niet-financiële instellingen een duidelijk protocol voor het uitleveren van gegevens. Holland Casino hanteert bijvoorbeeld een formele procedure: ‘Wij beoordelen of de vraag rechtmatig is en dan gaan wij over tot verstrekking in persoon of per e-mail. We gebruiken geen USB-sticks en geen cd’s om de gegevens uit te leveren, behalve voor camerabeelden. Wij werken alleen met papieren vorderingen en we gebruiken een protocol voor onze medewerkers.’ Een ander groot bedrijf geeft eveneens aan de procedure zeer serieus te nemen: ‘We hebben een interne procedure, waarbij we eerst controleren of het goede artikelnummer is gebruikt. Als dat niet zo is, dan sturen we de vordering terug en vragen we om een rectificatie. Ik wil als bedrijf niet in het verdachtenbankje terechtkomen omdat we op onjuiste gronden gegevens hebben uitgeleverd. Bij twijfel leveren we niet uit.’

Aangezien de verscheidenheid in de informatievragen bij de hier beschreven categorie van gegevenshouders groter is, en het ook om kleinschalige bedrijven gaat, zoals franchisehouders van benzinestations, is vanzelfsprekend echter niet altijd sprake van strak bepaalde procedures.

In de praktijk wordt ook hier door de opsporingsdiensten eerst een ja/nee-vraag gesteld voordat een papieren vordering wordt gedaan. De opsporingsdienst belt eerst met de gegevenshouder met de vraag of bepaalde informatie voorhanden is. Als het camerabeelden betreft, wordt in het telefoongesprek vaak al verzocht de beelden veilig te stellen, om te voorkomen dat ze verloren gaan. Een aantal instellingen belt na de telefonische ja/nee-vraag 'contra' naar de politie, om zeker te weten dat de vraag daadwerkelijk van een opsporingsdienst afkomstig is.

Vervolgens wordt het formele bevel per e-mail of fax naar de gegevenshouder gezonden, die de vordering controleert op fouten.[176] Het komt ook hier voor dat de verkeerde bevoegdheid wordt gebruikt, waarna de gegevensverstrekker de vordering retourneert en verzoekt om een correct bevel. 'Wat wij eerst doen, is kijken of ze [de opsporingsdienst] het goede artikel hebben en dat gaat nog wel eens fout. Het verschilt per opsporingsinstantie wat voor reactie je krijgt als je ziet dat ze een fout hebben gemaakt: sommigen worden boos op ons. Uiteindelijk komt dat wel goed, maar het leidt wel eens tot discussies', aldus een van de respondenten.

Veelal volgt na ontvangst van de juiste vordering een aanvullend telefoongesprek ter verheldering, waarna de vordering in behandeling wordt genomen. In uitzonderingsgevallen wordt zonder papieren vordering gewerkt. Het moet dan gaan om ernstige strafbare feiten, met een spoedeisend belang, zoals een vermissing of een ontvoering. Bij dergelijke zaken kan de officier van justitie (of een rechercheur van politie) mondeling de vordering doen, waarna later alsnog het papieren bevel volgt.

De meeste geïnterviewde instellingen leveren de gegevens wel digitaal uit, per e-mail of op een USB-stick. Zij volgen daarbij dus een ander beleid dan de financiële instellingen.

8.3.3 Vrijwilligheid

Zeker door de grotere bedrijven en instellingen die zijn geïnterviewd, wordt gesteld dat gegevensverstrekking op basis van vrijwilligheid niet meer voorkomt. Een respondent laat weten uitsluitend op basis van papieren vorderingen mee te werken aan gegevensuitlevering: 'Wij doen dat [gegevens verstrekken] niet zo-

[176] De gegevensverstrekker mag de vordering niet inhoudelijk toetsen, dat wil zeggen nagaan of er sprake is van een strafbaar feit. De gegevensverstrekker is evenwel bevoegd om op basis van de Wbp te controleren of de vordering aan de formele vereisten voldoet: de vorm van de vorderingen en de vraag welke gegevens gevorderd worden.

maar vrijwillig. We moeten een vordering hebben, die we na moeten komen [bedoeld wordt de medewerkingsplicht], want anders hebben we een probleem. Wij zouden anders ook niet meewerken. We hebben deze werkwijze zo kenbaar gemaakt [aan de opsporingsdiensten] en krijgen hierover ook geen discussies met de politie.'

Wederom is het beeld bij de kleinschaliger bedrijven wat minder eenduidig. Eén van de geïnterviewde exploitanten van benzinestations, bijvoorbeeld, geeft aan wel altijd schriftelijke vorderingen te ontvangen. 'Meestal bellen ze [de politie] van tevoren om te vragen of wij de gegevens [meestal camerabeelden] hebben. Als wij inderdaad beelden hebben, vraagt de politie ons die alvast veilig te stellen. Vervolgens komen ze langs met een brief en een USB-stick. Op die brief staat een handtekening van de officier van justitie (...). We houden eerst een vooroverleg om uit te zoeken wat ze nodig hebben en dan komt het verzoek', aldus een van de geïnterviewde pompstationhouders.

Een ander laat echter weten dat er nog altijd geen schriftelijke verzoeken worden gedaan. 'De politie komt aan de balie [in de winkel bij het benzinestation] en ze legitimeren zich. Ze vragen dan of wij beelden hebben. Als wij die hebben, dan laten ze een USB-stick achter. Dan maak ik een bestand van de beelden en die zet ik dan op de stick. Die halen ze dan later weer op. Ik heb niet meegemaakt dat er een vordering op papier komt.'[177] Het is in dit geval dus de vraag of de opsporingsambtenaren in alle gevallen een juist onderscheid weten te maken tussen hun bevoegdheid om voorwerpen in beslag te nemen en de bevoegdheden op grond van de Wbvg.

Ook een respondent die wel namens een grote koepel van bedrijven spreekt, sluit informatieverstrekking op basis van vrijwilligheid echter niet helemaal uit. 'De vrijwilligheid is niet weggenomen. Soms bellen ze [de opsporingsdiensten] ons op om direct iets te weten te komen en dan moeten wij wel tegen veel druk bestand zijn. Maar wij werken wel mee in een noodsituatie. We doen dan wel altijd een controle op de ambtenaar die ons belt, en als we die niet kunnen vinden, krijgen ze geen informatie.' Uit het citaat blijkt overigens niet ondubbelzinnig of sprake is van een mondelinge of een vrijwillige vordering. Mondelinge vorderingen in spoedeisende situaties zijn immers op grond van de Wbvg mogelijk, maar moeten wel worden gevolgd door een vordering op papier.

---

[177] Nota bene: het is mogelijk dat de respondent, beheerder van een pompstation, vertelt over wat er zich voordeed toen hij *slachtoffer* was van een misdrijf. Uiteraard hoeven politiefunctionarissen dan geen schriftelijke vordering te doen. Ook is het mogelijk dat de beheerder de schriftelijke vordering niet onder ogen heeft gekregen, omdat deze is verstuurd naar het moederbedrijf of het hoofdkantoor.

8.3.4 Waarborgen ter bescherming van de gegevensverstrekkers

Ook de niet-financiële instellingen hebben te maken met vorderingen die niet precies omschreven zijn. Eén van de respondenten formuleert dit als volgt: 'Ik heb soms het idee, zeker met camerabeelden, dat het een schot hagel is. Er is een aanwijzing dat een verdachte mogelijk op een bepaald traject heeft gereisd en de politie zegt: geef ons alles [alle beelden van de betreffende dag] maar. Dan denk ik: ho even. (...) Wij werpen dan tegen dat we dat niet kunnen doen, als het zo ongericht is. Wij proberen dat in te perken. Negen van de tien keer lukt het wel om daar in onderling overleg uit te komen.'

Een andere geïnterviewde geeft aan dat al op voorhand terughoudendheid wordt betracht bij het verstrekken van gegevens aan de opsporingsdiensten: 'Wij willen geen verlengde zijn van de opsporing. We willen de privacy van anderen niet schaden en we willen niet heel ruim de medewerking verlenen [aan de opsporing van strafbare feiten].'

Een derde respondent geeft eveneens aan wel te maken te hebben met te ruim geformuleerde vorderingen: 'Ze [de opsporingsdiensten] willen dan een bezoekerslijst van twee weken van een heel grote vestiging. Wij hebben per dag per vestiging soms wel drieduizend bezoekers, dus op zo'n lijst staan heel veel namen. Ook komt het voor dat men geen gegevens heeft die erop wijzen dat de [de verdachte(n)] klant bij ons is, maar dan komt er een *fishing expedition*, of ze denken dat wij een verlengstuk van de herkenningdienst van de politie zijn. Onze reactie is dan dat wij de vordering formeel afwijzen omdat ze niet proportioneel is. Of we vinden dat het eigenlijk gaat om gevoelige gegevens, waarvoor art. 126nd niet kan worden gebruikt. (...) De politie reageert op onze weigering soms met begrip, soms niet en soms met een dreigement van een huiszoekingsbevel of een bevel tot inbeslagneming. (...) Meestal komen we daar wel uit, omdat we affiniteit hebben met het werk van de politie: veel van onze medewerkers zijn zelf ook van de politie afkomstig.'

Omgekeerd geven sommige bedrijven aan dat zij met hun kennis en kunde juist een grotere bijdrage zouden kunnen leveren aan het opsporingsonderzoek. Zij zouden met andere woorden, een zelfstandige(r) rol willen hebben in het uitleveren van gegevens die hen nuttig lijken te zijn. 'Buiten de opsporingsinstanties zijn er [ook andere] instellingen die kennis van zaken hebben die zinnig is voor de opsporing.'

8.3.5 Beklagregeling

De beklagregeling is bij de niet-financiële instellingen bekend, maar wordt niet of nauwelijks gebruikt. Knelpunten in de afhandeling van vorderingen worden rechtstreeks met het openbaar ministerie of de politie afgehandeld. Holland Casino geeft aan een keer gebruik te hebben gemaakt van de beklagregeling, in een zaak waarin de gegevenshouder vond dat een vordering niet rechtmatig was. 'We moesten bezoekgegevens afgeven aan een korps waarvan wij vonden dat het niet mocht. Toen kwam er een dreigement van de politie dat ze ons zouden aanhouden als we niet zouden meewerken. We hebben de zaak toen laten voorkomen en gelijk gekregen, maar de politie hoefde de gegevens niet terug te geven, omdat wij ze toch al hadden geleverd.' Of dit ook betekende of de informatie niet mocht worden gebruikt in de strafzaak kon niet worden achterhaald. De mogelijkheid bestaat uiteraard ook dat de zaak nooit voor het gerecht is gebracht.

8.3.6 Knelpunten

Bij het noemen van knelpunten kan in zijn algemeenheid een onderscheid worden gemaakt tussen de grotere bedrijven en instellingen, die met regelmaat geconfronteerd worden met gegevensvorderingen en die bovendien ook ingewikkeld kunnen zijn, en de gegevenshouders die meer incidenteel te maken hebben met verzoeken, van veelal eenvoudiger aard. Exploitanten van benzinestations zijn bijvoorbeeld zeer positief. 'We kennen elkaar en elkaars problematieken. De politie doet er enorm veel aan om een goede samenwerking te hebben met de ondernemers om alle trajecten soepel te laten verlopen.'

Evenals bij de financiële instellingen is de tijdrovendheid van het afhandelen van de vorderingen en het uitleveren van gegevens een knelpunt bij de grotere bedrijven en instellingen. Ook hier zien de meeste respondenten een toename van het aantal, dan wel de complexiteit van de vorderingen in het verschiet. 'Het kost tijd, en dat is het probleem. Er komt een e-mail [met de vordering] bij ons binnen die best veel informatie bevat. Soms ook gevoelige gegevens over de betreffende strafzaak. Dat moet je er eerst uithalen en dan kun je de vordering pas doorsturen aan de betreffende afdeling. Vervolgens moet je het proces [van afhandeling en uitlevering] bijhouden en dat kost ook tijd. (...) Per aanvraag kost het gemiddeld een half uur, beeldaanvragen kosten helemaal veel tijd', aldus een geïnterviewde. Ook een ander bedrijf stelt dat het voorkomt dat de politie hen bij het afhandelen van een vordering te veel informatie verstrekt over de onderliggende strafzaak.

Een andere respondent wijst ook op de extra inspanning die het voldoen aan een vordering om gegevens vereist. ‘We doen 120 vorderingen per jaar. Dat is niet meer dan een halve FTE op jaarbasis, maar het verstoort wel degelijk de processen van het reguliere werk. Het kost ons zeker inspanning om de informatie te vinden en dat is niet altijd een druk op de knop.’

Als tweede knelpunt worden de kosten genoemd die gepaard gaan met het voldoen aan de vorderingen. Volgens de Nederlandse Spoorwegen zou de uitlevering van gegevens op grond van de Wbvg 250.000 à 300.000 euro op jaarbasis kosten. Er is 1 FTE op jaarbasis mee gemoeid. ‘Wij zouden dat wel willen doorbelasten en bij sommige arrondissementen kun je een factuur terugsturen, maar dat is geen standaard beleid.’ Ook gaan er kosten gepaard met het op voorhand veiligstellen van gegevens (in het bijzonder camerabeelden). Als er dan uiteindelijk geen vordering volgt, kunnen die niet in rekening worden gebracht. Voor andere dan financiële instellingen is geen vergoedingsovereenkomst afgesloten.

8.4 Besluit

Uit de interviews bleek dat gegevensverstrekkers uiteenlopende ervaringen hebben met, en verschillende oordelen hebben over de consequenties van de Wbvg in de praktijk. Aangezien het vooral gaat om financiële instellingen enerzijds en overige gegevensverstrekkers anderzijds is in dit hoofdstuk de beschrijving langs die lijnen in tweeën gedeeld.

In algemene zin kan geconcludeerd worden dat gegevensverstrekkers (zowel de financiële als de niet-financiële instellingen) tevreden zijn over de komst van de Wbvg. De regelgeving heeft (ook bij de instellingen zelf) duidelijkheid gebracht wat de procedure van het uitleveren van gegevens betreft en er is een einde gekomen aan de soms langdurige discussies met opsporingsinstanties die bestonden in de tijd van de vrijwillige uitlevering. Het merendeel van de uitleveringssituaties verloopt goed, zonder noemenswaardige problemen of miscommunicatie met de opsporingsdiensten.

Drie structurele knelpunten die zich in de praktijk voordoen, zijn de grote groei in het aantal vorderingen, dat bovendien toe lijkt te nemen, het kennisgebrek bij de opsporingsdiensten, en de vergoeding van de gemaakte kosten. Het kennisgebrek is een gevolg van het feit dat veel opsporingsambtenaren bevoegd zijn gegevens te vorderen op basis van art. 126nc Sv, maar dat zij niet allemaal even kundig zijn. Dit kennisgebrek zou vooral voorkomen in financiële strafzaken, waarvoor speciale expertise gewenst is. Vóór de introductie van de Wbvg werden dergelijke vorderingen beheerd door een financieel rechercheur, met aanzienlijk minder foute vorderingen tot gevolg. Het zijn dan ook in het

bijzonder de financiële instellingen die pleiten voor een centralisatie in de vorderingen, om de communicatie meer gestroomlijnd en overzichtelijk te doen verlopen en de expertise (opnieuw) te beperken tot een aantal ervaren opsporingsambtenaren. Ook het aanstellen van een Wbvg-contactpersoon per arrondissementsparket zou kunnen helpen een aantal (praktische) knelpunten zoals vergoeding van kosten, op te lossen.

9 Algemeen besluit

9.1 Inleiding

In dit rapport stond het functioneren van de Wet bevoegdheden vorderen gegevens (Wbvg) centraal. Het wetsvoorstel riep onder juristen nogal wat discussie op toen het in 2003 en 2004 werd besproken. De huidige Amsterdamse wethouder Lodewijk Asscher, toen nog onderzoeker informatierecht aan de Universiteit van Amsterdam, sprak bijvoorbeeld van een 'muisstille revolutie in het strafrecht'.[178] Het wetsvoorstel maakte het in beginsel immers mogelijk om alle informatie te vorderen die er over iemand voorhanden was, met de verplichting aan de gegevenshouders om ook gevolg te geven aan de uitgebrachte vorderingen. Toen de Wbvg in 2005 werd aangenomen, deed de minister van Justitie dan ook de toezegging aan de Eerste Kamer dat de wet zou worden geëvalueerd. Dit rapport vormt daarvan de weerslag.

In dit hoofdstuk is de beantwoording van de vier in hoofdstuk 1 geformuleerde centrale onderzoeksvragen aan de orde (paragraaf 9.2). Verder zullen in paragraaf 9.3 puntsgewijs enkele afsluitende observaties worden gedaan met betrekking tot geconstateerde knelpunten.

9.2 Beantwoording van de onderzoeksvragen

1 In welke mate en ten behoeve waarvan wordt een beroep op de Wbvg gedaan?

De eerste onderzoeksvraag had primair betrekking op de aard en de inhoud van de gegevensvorderingen die op grond van de Wbvg worden gedaan. Een landelijk beeld daarvan kon helaas niet worden geschetst, bij gebrek aan systematische registratiegegevens. In het onderhavige onderzoek kon van een opsporingsinstantie (FIOD) en van twee parketten (Den Bosch en Groningen) door middel van handmatig tellen en classificeren een redelijk, maar niet in alle opzichten volledig beeld worden geconstrueerd van de vorderingen die door de opsporingsambtenaren, respectievelijk de officieren van justitie, al dan niet met machtiging van de rechter-commissaris, worden gedaan.

Het ontbreekt bovendien aan richtlijnen omtrent hoe vorderingen moeten worden vastgelegd. Eén vordering kan bijvoorbeeld over meerdere personen

---

178 *Kamerstukken II* 2003/04, 29 441, nr. 5, p. 3.

tegelijk gaan, of meer dan een informatieverzoek bevatten. Ook wordt, voorzichtig geschat op grond van de dossieranalyse, zo'n 5 procent van de vorderingen retour gestuurd door de aangezochte gegevenshouder, vanwege onduidelijkheden, een onjuiste adressering, of omdat de vordering, althans in de optiek van de bevraagde partij, anderszins niet aan de richtlijnen voldoet.

Hoewel dus in allerlei opzichten beperkt, levert een cijfermatige analyse van de vorderingen toch belangwekkende conclusies op. In de eerste plaats blijkt de Wbvg selectief te worden gebruikt. Slechts art. 126nc Sv en 126nd Sv worden in de praktijk veelvuldig toegepast. De onderzochte parketten doen echter slechts zelden een beroep op de overige onderdelen van de Wbvg, dat wil zeggen art. 126ne Sv, 126nf Sv, 126nh Sv en 125i Sv. 96 procent van de vorderingen had betrekking op art. 126nd Sv.

In de tweede plaats bestrijkt de Wbvg, zoals bij de invoering ook werd verwacht, inhoudelijk inderdaad een breed informatiepalet. In totaal stelden de onderzochte parketten in de bestudeerde dossiers 828 vragen, die over 232 verschillende onderwerpen gingen. Naar zijn aard is het spectrum van de gestelde vragen echter weer beperkter: het bleek in 72 procent van de gevallen te gaan om financiële gegevens of om camerabeelden. Het is dan ook niet verwonderlijk dat financiële instellingen de belangrijkste categorie van bedrijven zijn die met gegevensvorderingen op grond van de Wbvg worden geconfronteerd. Daarbij gaat het overigens niet alleen om klantgegevens, maar ook om camerabeelden, bijvoorbeeld van geldopnames bij pinautomaten.

Ten derde kan, zowel op grond van de dossierstudie als op basis van interviews met gegevensvragers, worden geconcludeerd dat de Wbvg niet wordt gebruikt om gegevens van burgers te vorderen. De wet sluit dat niet expliciet uit, hetgeen door sommige academici bij de introductie van de wet als onwenselijk werd gezien. In de praktijk heeft dit veronderstelde probleem zich dus echter (nog) niet gemanifesteerd.

De verklaring voor deze drie bevindingen ligt eerst en vooral in het feit dat de politie in de praktijk een beroep kan doen op allerlei opsporingsmethoden om informatie en bewijsmateriaal te vergaren: het vorderen van gegevens van derden is er daarvan slechts een. Bovendien, zo blijkt uit een studie van De Poot e.a. (2004), wordt die optie maar in een minderheid van de opsporingsonderzoeken toegepast. In plaats daarvan kan veelal worden volstaan met gegevens die de politie eigenstandig kan verzamelen.

2 Wordt de wet toegepast zoals bedoeld en omschreven door de wetgever?

De volgende centrale vraag in het onderhavige onderzoek was of de Wbvg wordt toegepast zoals bedoeld en omschreven door de wetgever. Deze hoofd-

vraag is uiteengelegd in diverse deelvragen, die navolgend de revue zullen passeren.

Een eerste belangrijke kwestie is of de Wbvg inderdaad een einde heeft gemaakt aan de praktijk van vrijwillige gegevensverstrekking. Uit het onderzoek blijkt dat enerzijds de recherche-afdelingen die vaak gegevens vorderen op basis van de Wbvg en de vertegenwoordigers van het openbaar ministerie thans goed op de hoogte zijn van de wet en de daarin gestelde verplichtingen. Ook de 'grote' gegevenshouders, vooral de financiële instellingen, leveren alleen nog gegevens uit wanneer deze worden gevorderd.

Anderzijds stellen sommige geïnterviewde gegevenshouders dat de politie soms nog steeds gegevens opvraagt zonder dat sprake is van een schriftelijke vordering. Of daarbij inderdaad niet conform de Wbvg is gewerkt, laat zich echter niet goed reconstrueren. De Wbvg is bijvoorbeeld niet van toepassing wanneer de gegevenshouder op eigen initiatief informatie levert, en evenmin in gevallen waarvoor de Wbp niet geldt. In een geval noemde een respondent echter dat camerabeelden door opsporingsambtenaren werden opgehaald zonder papieren vordering, een situatie waarop de wet wel ziet. Al bij de behandeling van de Wbvg in de Eerste Kamer kwam aan de orde dat het niet eenvoudig is om het correcte onderscheid te maken tussen gevallen waarop de Wbvg wel en niet van toepassing is.[179] Het ligt voor de hand dat zulke finesses voor de gemiddelde opsporingsambtenaar evenmin altijd helder zullen zijn.

De tweede vraag in het kader van de toepassing van de wet is of het onderscheid in verschillende categorieën van gegevens, met uiteenlopende randvoorwaarden voor vordering, in de praktijk hanteerbaar en toepasbaar is. De interviews laten zien dat er weinig problemen zijn met het maken van een onderscheid tussen art. 126nc Sv en 126nd enerzijds en art. 126ne Sv, 126nf Sv, 126nh Sv en 125i Sv anderzijds. Wel slagen opsporingsambtenaren (in tegenstelling tot de officieren van justitie en de parketsecretarissen) er niet altijd in een correct onderscheid te maken tussen art. 126nc Sv en art. 126nd Sv. Een factor die daarbij meespeelt, is dat de wetgever een zekere ruimte voor interpretatie heeft overgelaten. De opsomming die in art. 126nc lid 2 is opgenomen is enerzijds limitatief. Identificerende gegevens zijn beperkt tot, als het om personen gaat, naam, adres, woonplaats, geboortedatum en geslacht, en als het rechtspersonen betreft, de gegevens betreffende de rechtsvorm en de vestigingsplaats. Anderzijds heeft de wetgever de administratieve kenmerken waarmee een persoon bij een bedrijf of instelling bekend is niet strikt afgebakend. Daaronder kunnen *bijvoorbeeld* een nummer van een polis, of een lidmaatschapsnummer

179 *Kamerstukken I* 2004/05, 29 441, C, p. 5-6.

vallen.[180] Kennelijk ontstaat in de praktijk met enige regelmaat discussie over de invulling van art. 126nc Sv op dit punt. Geïnterviewde gegevenshouders laten weten dat zij nogal eens vorderingen retour sturen omdat deze naar hun idee onterecht op art. 126nc Sv zijn gebaseerd.

Ten derde diende te worden nagegaan of de bevoegdheden waarin de Wbvg voorziet toereikend zijn vanuit het perspectief van de opsporingsverantwoordelijken. Over het algemeen kan worden vastgesteld dat dit inderdaad het geval is. Er werd altijd al informatie van derden gebruikt in opsporingsonderzoeken. De Wbvg heeft aan die praktijk niets veranderd, maar de gegevensvordering wel transparanter gemaakt en meer gestructureerd. De keerzijde is dat de administratieve belasting voor opsporingsinstanties is toegenomen. Thans moeten zij immers de feiten en omstandigheden in het kader waarvan gegevens van derden benodigd zijn op papier zetten, de vordering moet worden beoordeeld, en vastgelegd in het dossier.

Uit het onderzoek komen twee aandachtspunten naar voren die de werking van de Wbvg negatief beïnvloeden: de uitspraak in de zaak Trans Link, en de uitzonderingspositie die wordt ingenomen door geheimhouders.

Het probleem dat ongewild gevoelige gegevens worden verkregen op het moment dat informatie wordt gevorderd, speelde ook in de discussie in de Tweede Kamer over het wetsvoorstel al een rol. De minister van Justitie nam daarbij het standpunt in dat alleen indien de officier van justitie specifiek navraag deed naar zeer privacygevoelige aspecten art. 126nf Sv van toepassing zou moeten zijn.[181] In de gevallen waarin gevoelige gegevens ongewild als 'bijvangst' werden verkregen, hoefde art. 126nf Sv niet te worden ingeroepen. De Hoge Raad besloot in de zaak Trans Link de redenering van de minister echter niet te volgen. Op 23 maart 2010 oordeelde deze in een zaak waarin door de officier van justitie van Trans Link Systems B.V. gegevens waren gevorderd, waaronder foto's van personen. Met verwijzing naar de Wet bescherming persoonsgegevens besliste de HR dat gegevens waaruit informatie over het ras van een persoon kan worden afgeleid, zoals foto's van personen, als gevoelige informatie wordt gezien waarvoor art. 126nf Sv geldt. Het feit dat met de vordering niet beoogd werd de desbetreffende informatie aan de foto's te ontlenen doet daar niet aan af. Deze uitspraak roept de belangrijke vraag op of deze opvatting ook zonder meer geldt ten aanzien van camerabeelden. Inmiddels is deze uitspraak in recente (weliswaar lagere) jurisprudentie overigens wel genuanceerd.

---

180 Zie ook: *Kamerstukken II* 2003/04, 29 441, nr. 6, p. 12.
181 *Kamerstukken II* 2003/04, 29 441, nr. 6, p. 7.

Een ander inhoudelijk probleem dat naar verwachting in de toekomst zal groeien, is het feit dat verschoningsgerechtigden zijn uitgezonderd in de Wbvg. Zij kunnen dus door malafide personen gemakkelijk worden ingeschakeld om, bijvoorbeeld, zakelijke transacties af te schermen. Bovendien kunnen geheimhouders die wel willen meewerken aan gegevensvorderingen dat in de huidige situatie evenmin doen.

Een praktisch vraagstuk dat zich vooral voordoet rondom financiële gegevens zijn de relatief lange doorlooptijden die gepaard gaan met vorderingen aan banken en geldinstellingen. Opsporingsinstanties als de FIOD, die op grote schaal van zulke gegevens gebruikmaken, spreken van doorlooptijden tot enkele maanden. In spoedeisende gevallen en in geval gegevens worden gevorderd op grond van art. 126ne Sv blijkt van dat probleem overigens geen sprake. Dit roept bij de gegevensvragers de suggestie op dat er kennelijk geen technische redenen zijn voor de wachttijden. De gegevenshouders wijzen op hun beurt op het grote aantal vorderingen waarmee zij worden geconfronteerd.

De volgende belangrijke vraag in verband met de toepassing van de Wbvg betrof de relatie met andere wettelijke mogelijkheden om gegevens te vorderen. In de meeste gevallen blijkt geen sprake van onduidelijkheid ten aanzien van het toepassingsbereik van de uiteenlopende wettelijke regelingen. Rechtswetenschappers vreesden bijvoorbeeld dat er een onwenselijke overlap zou kunnen ontstaan tussen art. 126na Sv en art. 126nc Sv wanneer het gaat om het vorderen van gegevens bij *telecomproviders*. In de praktijk lijkt dit probleem gering: uit een analyse van een dertigtal vorderingen op grond van art. 126na Sv, die in het licht van de onderhavige evaluatie werd uitgevoerd, bleek dat slechts in een geval een vraag om identificerende gegevens onterecht via dat wetsartikel was gevorderd.

Een ander potentieel probleem dat is geopperd door rechtswetenschappers, is het grijze gebied dat kan ontstaan tussen inbeslagneming en vordering van gegevens. Het staat de gegevenshouder nu vrij om de gevorderde informatie aan te leveren op de manier zoals hij dat zelf wenselijk vindt. Dit kan betekenen dat de opsporingsinstantie informatie digitaal krijgt aangeleverd, maar evengoed kan de derde partij de gegevens op papier verstrekken, of zelfs originele stukken ter beschikking stellen. Met het 'gegeven' kan de opsporingsinstantie dus tegelijkertijd een 'voorwerp' verkrijgen. Als dit voorwerp via de Wbvg wordt gevorderd, ontbreken echter waarborgen waarin bij een inbeslagneming wel is voorzien. In beslag genomen voorwerpen kunnen bijvoorbeeld, al dan niet op last van de rechter, worden teruggegeven terwijl de Wbvg niet in die mogelijkheid voorziet.

Tegelijkertijd is niet duidelijk of de opsporingsinstanties originele stukken die (ongewild) via een Wbvg-vordering zijn verkregen vervolgens bijvoorbeeld ook mag testen op vingerafdrukken. Dit vraagstuk doet zich in de praktijk

inderdaad voor, waarbij de opsporingsinstanties van mening zijn dat zij originele stukken die op basis van een Wbvg-vordering zijn verkregen onder zich hebben, en dus desgewenst bijvoorbeeld ook aan een forensisch onderzoek kunnen onderwerpen.

Tot slot heeft de wetgever aangeduid dat bij de opsporingsinstanties het aantal opsporingsambtenaren dat zou worden gerechtigd vorderingen op grond van art. 126nc Sv te doen, diende te worden beperkt. Uit de discussie over het wetsvoorstel kan worden afgeleid dat daarbij werd gedacht aan een beperking tot medewerkers van de *infodesks,* opdat tevens een vorm van centraal overzicht, aanspreekpunten en kwaliteitscontrole zou worden gerealiseerd. De wetgever stelde echter geen harde richtlijnen op. Het gevolg is dat er in de praktijk grote verschillen bestaan. De bevoegdheid is in een deel van de politieregio's ingeperkt tot de hulpofficieren van justitie, maar elders kan elke opsporingsambtenaar vorderingen op grond van art. 126nc Sv doen, met uitzondering van vorderingen bij banken of geldinstellingen waarvoor een aparte richtlijn geldt. Bij geen van de onderzochte politieregio's of opsporingsinstanties is de bevoegdheid echter toebedeeld aan (alleen) de *infodesks*.

De belangen van de gegevensvragers en gegevenshouders lopen hier vanzelfsprekend niet parallel. Voor de gegevenshouder is het zonder meer een voordeel om met zo min mogelijk verschillende opsporingsambtenaren en rechercheafdelingen te maken te hebben. Voor de opsporingsdiensten is een beperking van bevoegdheden tot een vast aantal ambtenaren natuurlijk nadelig, omdat het extra administratieve stappen creëert en vertraging van het opsporingsonderzoek tot gevolg kan hebben. Bovendien zijn de *infodesks* niet op 24/7-basis operationeel, waardoor voor spoedeisende gevallen toch weer uitzonderingen zouden moeten worden gecreëerd.

3 Worden de waarborgen die zijn opgenomen in de Wbvg nageleefd?

De derde centrale onderzoeksvraag had betrekking op de waarborgen die in de Wbvg zijn opgenomen. Een eerste waarborg in de wet is dat de vorderingen zo gericht mogelijk worden afgebakend en dat geen sprake mag zijn van zogeheten *fishing expeditions*, oftewel 'ongerichte gegevensverzameling om, met behulp van bijvoorbeeld *data-mining* technieken, te kunnen komen tot een verdenking'. In de tweede plaats kent de Wbvg een strikte bevoegdheidsverdeling. Tot slot zijn ook waarborgen opgenomen ten aanzien van de (rechts)persoon waarop de informatie betrekking heeft, in de vorm van een notificatieplicht, en voor de gegevensverstrekkers, in de vorm van een beklagregeling.

In hoofdstuk 5 werd geschetst dat er in de praktijk grote verschillen bestaan tussen opsporingsonderzoeken en de beschikbare informatie waarop kan worden gerechercheerd. Wanneer direct duidelijk is wie de verdachte is, bij-

voorbeeld omdat een slachtoffer een gedetailleerde aangifte heeft gedaan, is het doorgaans geen probleem om ook op afgebakende wijze gegevens te vorderen. In zulke gevallen is het noch in het belang van het onderzoek, noch in het belang van de opsporingsfunctionaris, om grote hoeveelheden gegevens op te vragen die vervolgens allemaal moeten worden beschouwd en geanalyseerd.

Indien daarentegen vaag is wat zich heeft afgespeeld, of wanneer het misdrijf precies heeft plaatsgevonden, wordt afbakening moeilijker. In zo'n geval is het eerder denkbaar dat bijvoorbeeld camerabeelden over een langere tijdsperiode moeten worden opgevraagd en bekeken. Ook in de beginfase van proactieve opsporingsonderzoeken, waarin de opsporingsinstanties nog zoekende zijn naar de precieze illegale activiteiten van een subject, kan een breder geformuleerde vordering ('het hele klantdossier') noodzakelijk worden geacht. Bij sommige opsporingsinstanties, zoals de FIOD, vloeit het echter uit de aard van de opsporingsonderzoeken voort dat grote hoeveelheden gegevens van derden, vooral van banken en geldinstellingen, benodigd zijn.

Wanneer omvangrijke vorderingen worden gedaan, neemt vanzelfsprekend de kwetsbaarheid voor bezwaren dat er 'ongericht' gegevens worden gevraagd navenant toe. Zeker wanneer sprake is van zogeheten zoekzaken is echter ook vaak sprake van een 'kip-ei'-problematiek: je kunt pas bepalen of informatie relevant is wanneer je die eerst hebt gezien. Dat is echter wat anders dan een *fishing expedition* zoals hierboven gedefinieerd. Daarvan lijkt geen sprake, niet in de laatste plaats omdat geen Wbvg-gegevens kunnen worden gevorderd wanneer niet eerst sprake is van een verdenking van een strafbaar feit van een bepaalde zwaarte.

De tweede vraag die werd gesteld waar het de waarborgen in de Wbvg betreft, namelijk of het getrapte stelsel van bevoegdheden in de praktijk wordt toegepast, kan zonder meer bevestigend worden beantwoord. Bij alle onderzochte gegevensvragers is sprake van vaste procedures en wordt nauw samengewerkt tussen de parketten en de politie, respectievelijk de BOD'en.

In de derde plaats was de vraag of de notificatie- en de beklagregeling feitelijk functioneren zoals beoogd door de wetgever. Ten aanzien van de notificatieregeling kan worden geconstateerd dat deze niet of nauwelijks wordt nageleefd. In een aantal interviews met officieren van justitie werd bovendien duidelijk dat zij niet eens weet hadden van het feit dat ook bij onderdelen van de Wbvg een notificatieplicht geldt. De problematiek is daarmee vergelijkbaar met die welke eerder bij de eindevaluatie van de Wet BOB werd geconstateerd.[182]

---

[182] Zie Beijer e.a. 2004, p. 145-147. Overigens was men ten tijde van het onderhavige onderzoek bij het parket Amsterdam bezig met een inhaalslag ten aanzien van de notificatie in BOB-zaken.

Omtrent de beklagregeling kan worden vastgesteld dat deze in de praktijk eveneens niet of nauwelijks wordt gebruikt. Gegevenshouders zijn zich over het algemeen bewust van de wederkerige relatie die zij onderhouden met politie en justitie. De zakelijke en persoonlijke relaties tussen de gegevenshouders en politie en justitie is doorgaans dan ook goed. Dat laatste vloeit ook voort uit het feit dat op de veiligheidsafdelingen van gegevenshouders (de afdelingen die zich bezighouden met het afhandelen van de vorderingen en het uitleveren van de gegevens) vaak ex-politiemedewerkers werkzaam zijn, die affiniteit hebben met het opsporingswerk. Als een gegevenshouder toch een probleem heeft met een vordering wordt daarover direct in overleg getreden met het openbaar ministerie, hetgeen vrijwel altijd tot een oplossing leidt. Slechts een van de geïnterviewde gegevenshouders heeft ooit, in een uitzonderingssituatie, gebruikgemaakt van de beklagregeling.

Tot slot hebben rechtswetenschappers, na publicatie van de wet, gewezen op enkele potentiële knelpunten die zouden kunnen ontstaan. Ter afsluiting gaan we hier kort in op de vraag of deze zich in de praktijk ook manifesteren. Om te beginnen werd de vrees geuit dat art. 126ne Sv aan gegevenshouders een algemene meldplicht zou opleggen. Nu bleek al uit de dossierstudie die ten behoeve van het onderhavige onderzoek werd uitgevoerd, dat dit artikel zeer weinig wordt toegepast. In de praktijk zijn er niet veel soorten misdrijven die zich lenen voor het vorderen van toekomstige gegevens. In de weinige aangetroffen voorbeelden was bovendien sprake van een zeer specifieke, in tijd en naar personen afgebakende, meldplicht voor de betrokken gegevenshouder. Van een algemene meldplicht op basis van art. 126ne Sv kan dan ook niet worden gesproken.

Een ander potentieel probleem dat werd geopperd, was dat de mogelijkheid van het stellen van ja/nee-vragen in het kader van art. 126nc Sv in feite een spreekplicht inhield. Het vertrekpunt van deze gedachte lijkt echter primair te zijn geweest dat de gegevenshouders weinig animo zouden vertonen om mee te werken aan vragen van opsporingsdiensten. In werkelijkheid blijkt eerder sprake van het tegendeel. Voorts neemt het stellen van ja/nee-vragen veelal de vorm aan van een vooroverleg en biedt het de mogelijkheid na te gaan hoe de vordering het efficiëntst kan worden opgesteld. Het behoedt dus enerzijds de opsporingsdiensten voor het insturen van onzinnige of te ruim geformuleerde vorderingen. Anderzijds bespaart het de gegevenshouders onnodig werk. Zij overleggen graag zelf ook met de opsporingdienst voordat de definitieve vordering hen bereikt.

4 Hoe functioneert de Wbvg vanuit het perspectief van de gegevenshouders?

Voor een bedrijf of instelling betekent een vordering onvermijdelijk een zekere extra belasting: er wordt immers om een dienst gevraagd die normaliter niet tot de bedrijfsvoering behoort. De wetgever heeft dan ook gesteld dat bedrijven, instellingen of individuen die te maken krijgen met een vordering om informatie door een opsporingsinstantie daarmee zo min mogelijk dienen te worden belast. Zo kan van derden niet worden verlangd dat zij informatie vastleggen die niet reeds in het kader van de gewone bedrijfsvoering wordt geregistreerd. Bovendien brengt het moeten verstrekken van gegevens kosten met zich mee, en moeten mogelijk ook infrastructurele maatregelen worden getroffen. Het was dan ook een belangrijke onderzoeksvraag hoe gegevenshouders, in het licht van het voorgaande, het functioneren van de Wbvg beoordelen.

Zoals hiervoor al werd beschreven, worden financiële instellingen verreweg het meest met vorderingen op grond van de Wbvg geconfronteerd. Daarnaast zijn er ook andere grotere bedrijven, zoals Holland Casino en de Nederlandse Spoorwegen, die veelvuldig vorderingen krijgen. Bij deze firma's zijn dan ook organisatorische maatregelen getroffen om daaraan te kunnen voldoen, in de vorm van de aanstelling van medewerkers die zich specifiek met de afhandeling van de vorderingen bemoeien.

Uit de interviews met gegevenshouders blijkt niet dat opsporingsinstanties gegevens vorderen die het bedrijf of de instelling niet al vanwege de dagelijkse bedrijfsvoering vastlegt. Wel kan de klacht worden beluisterd dat de gevraagde informatie niet altijd voorhanden is in de vorm zoals de opsporingsinstanties die wensen te ontvangen. Het bijeenbrengen van de gevraagde gegevens kan daarom de nodige inspanning vergen, buiten de reguliere bedrijfsactiviteiten om. Het verstrekken van de gevorderde gegevens kan daardoor de nodige tijd vergen.

Kritiek op de Wbvg kan vooral worden beluisterd bij de bedrijven en instellingen die veelvuldig gegevens dienen aan te leveren. Zij beklagen zich over een toenemend aantal vorderingen en over de stijgende complexiteit en uitgebreidheid van de verzoeken. Gegevenshouders die meer incidenteel worden benaderd, maken niet of nauwelijks gewag van problemen.

Het moeten voldoen aan een gegevensvordering brengt soms onkosten met zich mee, bijvoorbeeld in de vorm van de uren die worden gemaakt door de medewerkers. In de Wbvg is dan ook voorzien in een vergoedingsregeling. Ook hier geldt dat de bedrijven en instellingen die op grote schaal worden benaderd eerder bezwaren hebben dan de incidentele gegevensverstrekkers. In het bijzonder financiële instellingen, die min of meer als een 'vaste partner' worden beschouwd door de opsporingsdiensten, zijn ontevreden. Dat is opmerkelijk, aan-

gezien al voor de komst van de Wbvg door de Nederlandse Vereniging van Banken en het openbaar ministerie landelijke afspraken zijn gemaakt over het vergoeden van kosten die gepaard gaan met gegevensverstrekking. Deze afspraken voldoen echter niet, aldus de geïnterviewde financiële instellingen. De standaardvergoeding wordt als onvoldoende dekkend beschouwd. Voorts verloopt ook de praktische afhandeling van ingestuurde facturen soms moeizaam, bijvoorbeeld wanneer onenigheid tussen de politie en het openbaar ministerie ontstaat over de betalingsplicht. De Nederlandse Vereniging van Banken voert (nog steeds) overleg met het openbaar ministerie om te komen tot verbetering van de onkostenvergoeding.

Aan deze discussie moet echter worden toegevoegd dat opsporingsinstanties de handelwijze van financiële instellingen bij gegevensvorderingen over het algemeen met verbazing, en met een behoorlijke mate van achterdocht, bezien. Zo wordt niet begrepen dat financiële instellingen weigeren gevraagde gegevens digitaal aan te leveren, maar dat, als enige gegevenshouder, per se op papier willen doen. Het zou immers voor beide partijen veel goedkoper en efficiënter zijn om digitale bestanden te leveren, respectievelijk geleverd te krijgen. Opsporingsinstanties ervaren deze handelwijze dan ook als welbewuste obstructie. Zij zien het vooral als een poging van de banken en geldinstellingen om een extra drempel op te werpen en daarmee het beroep op hun gegevens enigszins te beperken. Daarnaast biedt het de mogelijkheid om per papieren afschrift een standaardbedrag in rekening te kunnen brengen.

De politie en de BOD'en plaatsen vergelijkbare vraagtekens bij de tijd die de banken en geldinstellingen nemen voor het aanleveren van gevorderde informatie. In het geval van ingewikkelde en uitgebreide vragen is het vanzelfsprekend dat gegevens niet *à la minute* kunnen worden geleverd. Opsporingsinstanties kunnen echter minder begrip opbrengen voor het feit dat het ook weken kost om dezelfde eenvoudige transactiegegevens aangeleverd te krijgen die elke klant thuis via het internet met een druk op de knop op het beeldscherm kan oproepen.

Tot slot werd bij de introductie van de Wbvg door rechtswetenschappers betoogd dat de geheimhoudingsplicht voor gegevenshouders op gespannen voet zou staan met een integere klantrelatie. In de praktijk blijkt daarvan echter geen sprake. Waarschijnlijk hangt deze uitkomst samen met het feit dat Wbvg-vorderingen vooral worden gebaseerd op art. 126nc Sv en art. 126nd Sv. Aangezien het daarbij om historische gegevens gaat, wordt van een gegevenshouder niet verlangd een klantrelatie in stand te houden omwille van het kunnen uitleveren van gegevens aan politie en justitie. Uit de interviews blijkt bovendien dat de opsporingsdiensten in de regel terughoudend zijn met het verstrekken van details over het opsporingsonderzoek dat de achtergrond van de vordering vormt.

9.3 Afsluitende observaties

Als sluitstuk van dit hoofdstuk nemen wij graag de vrijheid om enkele afsluitende observaties op een rij te zetten, die voortvloeien uit de uitgevoerde evaluatie. Daarbij gaat het enerzijds om aspecten die strekken tot verbetering of verduidelijking van de Wbvg. Anderzijds zijn ook zaken vastgesteld die anders lopen dan bij de invoering van de wet was voorzien, maar waarbij het aangewezen is geen nadere actie te ondernemen.

Ten eerste laat het onderhavige onderzoek zien dat de afhandeling van vorderingen in het kader van de Wbvg thans bij de opsporingsdiensten en de parketten, uitzonderingen daargelaten, veelal niet centraal wordt bewaakt. Het is de vraag of een (eenvoudig) registratiesysteem zoals in gebruik is bij het parket Amsterdam, geen zinvolle aanvulling zou kunnen vormen. Een dergelijk systeem kan ook bij de opsporingsdiensten worden ingevoerd bij de *infodesks*, waarbij het kan volstaan dat een geautoriseerde opsporingsambtenaar van elke uitgebrachte vordering ook een digitale kopie verstuurt, die in het bestand kan worden verwerkt.

In de tweede plaats bleek dat opsporingsambtenaren vooral moeite hebben met het maken van een goed onderscheid tussen informatie die op grond van art. 126nc Sv mag worden gevorderd en vragen waarop art. 126nd Sv van toepassing is. Het is hier enerzijds zinvol de reikwijdte van art. 126nc Sv nader te preciseren. De opsomming is nu deels limitatief, maar biedt deels ook, waar het gaat om administratieve kenmerken, ruimte voor interpretatie. Anderzijds dienen opsporingsambtenaren die geautoriseerd zijn vorderingen af te geven beter te worden opgeleid in de categorieën van gegevens waarvoor zij art. 126nc Sv mogen toepassen.

Ten derde is duidelijk geworden dat het ontbreken van explicatie in de wet hoe moet worden omgegaan met het feit dat gevoelige gegevens kunnen worden verkregen terwijl de gegevensvrager daar niet op uit was, een gemis vormt. De consequentie hiervan is dat de rechter aan dit punt nadere invulling heeft gegeven, met, gezien het Trans Link-arrest, gevolgen voor de opsporingspraktijk. Hoewel het desbetreffende arrest door lagere rechters in meer recente uitspraken is genuanceerd valt het toch te overwegen om het ‘ernstvereiste’ in art. 126nf Sv, conform een advies van professor Mevis, te laten vervallen, opdat dit artikellid in een ruimere verzameling van gevallen kan worden gebruikt.

Een vierde aandachtspunt is het misbruik dat malafide (rechts)personen kunnen maken van geheimhouders, al dan niet met hun welwillende medewerking, omdat die thans geheel zijn gevrijwaard van vorderingen in het kader van

de Wbvg. Het is dan ook gewenst om na te gaan welke oplossingen ten aanzien van dit probleem denkbaar zijn.

Ten vijfde blijkt in de praktijk het onderscheid tussen een 'gegeven' en een 'voorwerp' niet geheel duidelijk. De Wbvg ziet immers niet alleen op digitale informatie, maar ook op gegevens die op papier kunnen worden aangeleverd. Het kan zelfs gaan om de originele stukken van de gegevenshouder. Er bestaat dus overlap tussen voorwerpen die op grond van de bevoegdheden tot inbeslagneming worden verkregen en gegevens die worden gevorderd op grond van de Wbvg. In het geval van inbeslagneming zijn echter waarborgen van toepassing die niet gelden wanneer de gegevens zijn gevorderd. De wetgever zou op dit punt meer helderheid kunnen verschaffen, bijvoorbeeld door de gegevensvrager te laten expliciteren hoe hij de gevraagde informatie wenst te ontvangen.

In de zesde plaats blijkt de notificatieregeling die is opgenomen in de Wbvg slecht te functioneren. Deels lijkt dit een probleem dat voortvloeit uit onbekendheid met die regeling. Voor een ander deel blijkt de regeling voor opsporingsinstanties echter moeilijk interpreteerbaar en hanteerbaar. Aangezien dezelfde problematiek ook in het algemeen geldt met betrekking tot de Wet BOB (waarop hetzelfde wetsartikel ten aanzien van notificatie van toepassing is) zou in breder verband kunnen worden nagegaan welke oplossingen hiervoor mogelijk zijn.

Tot slot kan over het algemeen worden vastgesteld dat bedrijven en instellingen ruimhartig medewerking verlenen aan vorderingen die in het kader van de Wbvg worden gedaan. Knelpunten worden door gegevensvragers met name ervaren bij banken en geldinstellingen, die overigens bij een zeer substantieel deel van de vorderingen de aangezochte partij zijn. Dat zal in de toekomst niet veranderen aangezien onderzoek naar geldstromen alleen maar belangrijker wordt. Het is in dat licht ongewenst dat financiële instellingen voor vertragingen zorgen door gegevens louter op papier aan te leveren, en daarvoor een tijdsperiode te nemen waarvan men zich kan afvragen of die werkelijk noodzakelijk is. Van banken en geldinstellingen mag, gezien hun positie in de samenleving, worden verwacht dat zij zich in het bijzonder medeverantwoordelijk achten voor het bijdragen aan de opsporing van misdrijven. Ook zouden (juist) zij zich bereid moeten tonen om de kosten, die op de omzetten van de desbetreffende firma's als bagatel kunnen worden beoordeeld, te dragen. Financiële instellingen worden bovendien toch al bevoordeeld ten opzichte van andere gegevensverstrekkers, die in het geheel geen vergoeding ontvangen. De wetgever zou de mogelijkheden om striktere eisen te stellen aan de wijze waarop en het tijdsbestek waarin financiële gegevens worden aangeleverd, nader kunnen onderzoeken.

Summary

Until several years ago, the police and the special investigation services experienced a number of problems as regards the competence of their criminal investigation departments to request information from third parties. The government installed the Mevis Committee, named after its chairman, to study whether the Code of Criminal Procedure (*Wetboek van Strafvordering, Sv*) still offered a satisfactory legal framework for obtaining third party information in criminal investigations, particularly in view of new developments in information and communication technology. The Committee concluded that adaptation of the Code of Criminal Procedure was indeed advisable, and drafted a bill accordingly. Parliament ultimately passed the proposal into new legislation: the [Investigative] Powers to Request Information Act (*Wet bevoegdheden vorderen gegevens, Wbvg*), effective from 1 January 2006. The Act's main purpose is to provide a clear legal framework for the investigation services and the third parties from whom they request information, as well as to give the latter better legal guarantees. The powers defined by the *Wbvg* are part of the Code of Criminal Procedure.

The Minister of Justice agreed with Parliament that the *Wbvg* would be evaluated four years after it had become effective. The Department of Criminal Law at Tilburg University and IVA, the institute for policy research affiliated with Tilburg University, conducted the evaluation study. The project started in November 2009 and concluded in September 2010.

Evaluation of the *Wbvg* focused on three main topics. First, the study was to explore the number and nature of the requests for information based on the *Wbvg*. Secondly, it was to address how the investigative authorities apply the Act in practice and to what extent the legal guarantees included in the *Wbvg* function as intended. Thirdly, it was to explore how both those requesting data and those receiving these requests assessed the Act. These topics were cast into four main research questions:

1. To what extent and for what purposes do parties make use of the *Wbvg* in practice?
2. Is the Act functioning as the legislative authorities intended?
3. Do investigative authorities follow the rules included in the *Wbvg* that guarantee the interests of the information holders and of the individuals and legal entities about whom information is requested?
4. How do the parties who receive requests for information assess the workings of the *Wbvg*?

Methodology

The evaluation of the *Wbvg* was based on empirical data sources. The first source consisted of quantitative data on information requests submitted to third parties registered by the investigative authorities. The second source consisted of the files of closed investigations that had involved requests based on the *Wbvg*. Thirdly, researchers conducted interviews with representatives of various investigation services and private companies that receive information requests regularly, such as banks and transport authorities. The first two sources, however, proved to be of only limited value.

To begin with, a complete overview of the number of requests based on the *Wbvg* would require having a national database that records such requests. Unfortunately, no such database exists. Nor are requests for information registered consistently at local level by the public prosecution service districts, the police regions or the four special investigative departments.[183] In order to present quantitative information, then, we needed to access individual requests based on the *Wbvg* and register those in a specific temporary database. The intention was to gather information from three local public prosecution service districts (Amsterdam, Den Bosch, Groningen), the Functional Prosecution Service at the national level,[184] three police regions (Amsterdam-Amstelland, Brabant-Noord, Groningen) and one special investigation service (FIOD). Due to practical problems at the other locations, however, it was only possible to obtain information from the districts of Den Bosch and Groningen, and from the FIOD.

Secondly, in-depth study of the files of closed criminal investigations made only a limited contribution to answering the research questions stated above. The researchers reached this conclusion after studying approximately thirty investigation cases. Consequently, evaluation of the *Wbvg* came to depend more than intended on interviews with the representatives of parties holding or requesting information.

---

183 The Dutch public prosecution service comprises 19 local districts. The police are organized into 25 police regions. The four special investigation departments are attached to the Ministry of Finance (Fiscal Intelligence and Investigation Service, FIOD), the Ministry of Social Affairs and Employment (Social Intelligence and Investigation Service, SIOD), the Ministry of Agriculture, Nature and Food Quality (General Inspection Service, AID) and the Ministry of Housing, Spatial Planning and the Environment (Intelligence and Investigation Service, IOD). As of 14 October 2010, the new government reorganized the latter two, which are now part of the Ministry of Economic Affairs, Agriculture and Innovation and the Ministry of Infrastructure and the Environment respectively.

184 The Functional Prosecution Service acts on behalf of the special investigation services.

Content of the *Wbvg*

The *Wbvg* offers competent police detectives, detectives working for the special investigation departments, and public prosecutors (either independently or with the consent of the investigative magistrate) six specific powers to request information from third parties. First, a competent detective may request information for identification purposes (Art. 126nc *WvSv*). Secondly, the public prosecutor has the power to request other types of information, both historical information registered by third parties (Art. 126nd *WvSv*) and information which they may register in the future as part of their regular business processes (Art. 126ne *WvSv*). Thirdly, the public prosecutor may request a holder of information to assist in decrypting information that has been encrypted before storage (Art. 126nh *WvSv*). Fifth, he or she may order a search of electronically stored data (Art. 125i *WvSv*). If, however, the public prosecution service requests information regarded as extremely sensitive to privacy, for example concerning a persons' religious or ethnic background, a higher level of suspicion is needed and the public prosecutor also needs the consent of the investigative magistrate (Art. 126nf *WvSv*).

It is clear from the above that the more sensitive the information being requested and the more effort it takes a data holder to comply with a requisition demand, the more restricted the *Wbvg*. The Wbvg makes it possible to request information about suspects in criminal investigations, but also about other individuals if doing so contributes to the purpose of the investigation. Art. 552 *WvSv* allows holders of information to file a complaint against a requisition, albeit only in retrospect. The following sections address the empirical outcomes of the present research.

Practical use of the Wbvg

This section begins by considering the extent to which investigation services submit requests based on the *Wbvg*, the background of such requests, and the operating procedures put into place.

The first important conclusion is that only two of the specific powers included in the *Wbvg* are widely used, namely requests for information for identification purposes (Art. 126nc *WvSv*) and requests for historical information registered by third parties (Art. 126nd *WvSv*). Criminal investigations, however, seldom require application of the other powers defined in the Act.

The second major observation is that, although requests may and do cover a broad spectrum in terms of content, only two types of enquiries predominate, namely requests for financial information and requests for CCTV images. The two categories account for 72% of all requests based on the *Wbvg*. Not surprisingly, banks and financial institutions receive the majority of the requests,

not only for financial information but also for CCTV footage of ATM transactions, for example. In addition, other government bodies, such as the Tax and Customs Administration and local councils handle a relatively large number of requests.

Criminal investigation services and the public prosecution service use a standard protocol for requests based on the *Wbvg*. Contrary to the expectations of legislators, however, the authority to file a request for information for identification purposes (Art. 126nc *WvSv*) is not restricted to just a few detectives. In some cases, all the police officers designated as auxiliary to the public prosecution service may file such requests, while in other police regions and special investigation departments, all competent investigators have the authority to do so. Financial information is exempt from this rule, however, owing to a special arrangement made with banks and financial institutions; only a police officer designated as auxiliary to the public prosecution service may request such information.

How the investigation services assess the *Wbvg*

Representatives of investigation services use the *Wbvg* regularly to request information, and view the legislation as part of their daily routine. In their view, the Act did not lead to changes as far as the content of the information is concerned. It did, however, result in increasingly formal procedures.

The investigative authorities assess their relationships with holders of information as good and say that the latter comply with almost all requests. The representatives interviewed also appreciate the fact that investigation services have handled information requests more carefully since the *Wbvg* came into effect. The compulsory nature of valid requests for information has put an end to discussions with the privacy experts of third parties. The guarantees against claims from individuals and legal entities who feel that their interests may be harmed by disclosure are seen as useful, not only for the holders of information, but for the investigation services as well.

The legislator's primary aim with the *Wbvg* was to put an end to the practice of information being handed over to investigation services voluntarily with liability resting with the holders of information. Interviews with representatives of investigation services reveal that the Act has generally accomplished this goal. Investigators and public prosecutors are familiar with the regulations set out in the *Wbvg* and comply with these when requesting information. In turn, holders of information, particularly those frequently contacted, are also well aware of their rights, and now refuse to hand over information without being requested to do so officially. Representatives of companies that receive occasional requests may still hand over information voluntarily, however. At times individual police officers may also still seize information when a request would

be the appropriate tool. Finally, there are rare instances not covered by the legal framework where the only option is to ask a third party to hand over information voluntarily.

Practical bottlenecks identified by the investigative authorities

The investigative authorities requesting information from third parties identify two practical bottlenecks and four problems with regard to legislative aspects of the *Wbvg*. We discuss these practical difficulties below.

The first practical problem mentioned is the growing administrative burden placed on investigative authorities after the *Wbvg* came into effect. Submitting a request for information usually requires the authorities to draw up a verbatim report explaining the nature of the case and the reason for requesting specific information. Except in cases where an investigator requires information for identification purposes only, he or she must have the consent of the public prosecutor first, and the latter may need to consult the investigative magistrate if the information is sensitive in nature. The public prosecutor needs to draw up the formal request, and send it to the holder of the information. Finally, when the investigator receives a reply, he or she has to write another verbatim report confirming receipt. Furthermore, investigation services are, in specific cases, also required to notify the persons or legal entities to whom the information refers. Representatives of investigative bodies are particularly critical of the paperwork involved in the procedure.

The second practical bottleneck concerns compliance with information requests by banks and financial institutions. Representatives of the FIOD are particularly critical of this, because their investigations often depend on large volumes of financial information. For a start, they state that banks and financial institutions are usually slow to hand over information. Furthermore, the holders of financial information insist on delivering data only on paper. This results in higher costs, not only because the investigation service has to pay for every transcript separately but also because detectives first need to digitize the data to be able to analyse it.

Legislative bottlenecks identified by the investigative authorities

The evaluation identified four problems with regard to the legislative aspects of the *Wbvg*. The first problem is the result of the ruling of the Dutch Supreme Court in the Translink case. The second problem is how to distinguish adequately between Articles 126nc *WvSv* and 126nd *WvSv*. Thirdly, the definition of information overlaps with the definition of objects carrying information, and the overlap causes difficulties. Finally, the *Wbvg* exempts certain holders of information, such as lawyers, from the obligation to disclose information, and criminals can use this exemption to their advantage.

The Translink case concerned a public prosecutors' request for copies of photographs of holders of electronic travel cards used in public transport. The Supreme Court considered this information sensitive because a photograph can reveal ethnic background, and because an image may be linked directly to other information, such as the subject's name. Consequently, in such cases it is the investigative magistrate, rather than the public prosecutor, who is competent. Furthermore, a higher level of suspicion is needed for requests for sensitive information. Although we may question the ruling as such, it being impossible to say beyond a doubt whether a personal characteristic visible on a picture is sensitive, for instance, this particular case law had far-reaching implications at first. That was because the public prosecution service concluded that the ruling also extended to CCTV images recorded by cameras installed in public places. Such material is also widely used in cases of relatively minor offences, but now that would no longer be possible. This particular problem has yet to be resolved, although lower courts have since ruled that CCTV images do not compare to photographs and other personal information registered when someone subscribes to a specific service, for example. The Minister of Justice concluded that images recorded in public places are generally not sensitive information and instructed the public prosecution service accordingly, although individual public prosecutors may decide otherwise in specific cases.

The second legislative problem is how an investigator is to distinguish adequately between information for identification purposes, which he may request on his own authority, and other historical information for which he needs the public prosecutors' consent. The problem arises because the *Wbvg* is open to interpretation with respect to the scope of Art. 126nc *WvSv*. An investigator may request 'administrative characteristics' recorded about a person by a private company or a public body. The *Wbvg* only gives examples of administrative characteristics, such as the number of an insurance policy. In practice, investigators define such characteristics more broadly than the legislator appears to have intended.

Thirdly, investigative authorities in some cases have trouble distinguishing between information and the objects carrying information. If a holder of information hands over original documents, for example, these are also objects that investigation services might subject to forensic tests, for instance. The question is whether the *Wbvg* allows them to do this when the object is obtained by means of a request for information. Another problem is that legal guarantees are more extensive in the event of seizure. In such cases, a person may ask the court to order the investigation services to return the object to him, for example; that is not possible if they obtained the information by means of the *Wbvg*.

Finally, one of the public prosecutors interviewed brought up the problem that criminals might misuse the fact that certain parties are exempt from the

obligation to deliver information upon request. In one particular fraud case, the main suspect had involved a law firm in all of his business transactions; as a result, the investigative authorities could not obtain any information about these transactions. Although this is currently not a major problem, it may develop into one in the future, as there are already law firms advertising this particular 'advantage' of hiring their services.

How holders of information assess the *Wbvg*

Based upon the number of requests, we may divide holders of information into banks and financial institutions on the one hand and other third parties on the other. The first category receive by far the most requests based on the *Wbvg*.

The evaluation concludes that banks and financial institutions are generally satisfied with the changes brought about by the *Wbvg*. For the holders of information, the new legislation created greater transparency of procedures and put an end to the sometimes lengthy discussions with investigation services about handing over information voluntarily. They had experienced no serious problems handling requests based on the *Wbvg*, although there are two points that require attention.

To begin with, banks and financial institutions in particular complain about the growing number of requests submitted to them and their increasing complexity. In their view, investigative authorities unjustifiably think that delivering almost all the information in their possession only requires them to 'push a button'. Secondly, although banks and financial institutions receive financial compensation for handling information requests, they do not feel that it makes up for the costs involved. Other companies – only banks and financial institutions are compensated – also complain that handling requests for information is often time consuming and costly. All third parties sometimes question the broadness of the information requests submitted by the investigation services.

Another observation is that Art. 552 *WvSv,* which offers parties the opportunity to complain about specific requests, is seldom used in practice. This is not because this particular safeguard is inadequate, but because such parties and the investigative authorities usually solve their disputes bilaterally. They regard filing an official complaint as a last resort.

Finally, the *Wbvg* also requires the individual or legal entity about whom the authorities have requested information to be notified, albeit only on specific occasions and when this no longer interferes with the investigation. This rule does not function adequately, however, because many public prosecutors are unaware of it and because investigation services generally regard it as difficult to interpret and use in practice.

Concluding observations

The *Wbvg* evaluation study resulted in a number of concluding observations. We present the most important of these below.

Generally, our study revealed that most holders of information generously comply with requests submitted to them by investigation services. Only banks and financial institutions raise the threshold somewhat by taking their time to deliver information, and by submitting it only on paper. It may be advisable to impose stricter requirements on those parties, given the growing importance of financial investigation.

The problem of overlap in the definition of information on the one hand and of objects carrying information on the other can be solved by allowing investigation services to decide how they wish to receive information. This may prevent the parties receiving requests from delivering original documents when a copy would suffice, and it may also put an end to holders of information delivering information in formats of their own choice.

The legislator could furthermore provide a more detailed definition of Art. 126nc *WvSv*. It would also be advisable to restrict the competence to submit requests for information for identification purposes to police officers designated as auxiliary to the public prosecution, and offer them additional training in adequately assessing the nature of specific requests.

This evaluation study showed that the scope left by the legislator with regard to the definition of sensitive information, particularly when investigative bodies receive such information without specifically asking for it, has led to practical problems, culminating in the ruling of the Dutch Supreme Court in the Translink case. Although lower courts have already qualified case law to a certain extent, a more definitive solution has been suggested by Professor Mevis: lower the level of suspicion needed for requesting CCTV images recorded in public spaces.

Finally, the authorities should address the possibility that criminals misuse parties who are exempt from the obligation to comply with information requests. There are several ways to solve this problem, but these should first be subject to a detailed legal review.

Bijlage 1 Schematisch overzicht bevoegdheden Wbvg

De bevoegdheden in de Wbvg laten zich als volgt schematisch samenvatten.

Vorderen van:	**Aard gegevens:**	**Benodigde verdenking:**	**In welk geval:**	**Bevoegd tot vorderen:**	**Van welke derde:**
Identificerende gegevens. Art. 126nc Sv en 126uc Sv.	Naam, adres, woonplaats, geboortedatum, geslacht en administratieve kenmerken. Administratieve kenmerken zijn o.a. klantnummer, polisnummer, bankrekeningnummer.	- elk misdrijf of - het in georganiseerd verband beramen of plegen van misdrijven als omschreven in art. 67 lid 1 Sv die gezien hun aard of de samenhang met andere misdrijven die in dat georganiseerde verband worden beraamd of gepleegd een ernstige inbreuk op de rechtsorde opleveren. NB: via art. 126nd lid 6 Sv is de ovj bevoegd om in geval van een overtreding identificerende gegevens te vorderen. Een machtiging van de rechtercommissaris is dan vereist.	In het belang van het onderzoek.	Opsporingsambtenaar.	Degene die daarvoor redelijkerwijs in aanmerking komt en die anders dan ten behoeve van persoonlijk gebruik gegevens verwerkt. Het betreft het verwerken van gegevens vanwege een functie of beroepsuitoefening. Er dienen aanwijzingen te zijn (hoe licht ook) die erop wijzen dat er een kans bestaat dat deze gegevens heeft van de persoon die onderwerp is

Vorderen van:	Aard gegevens:	Benodigde verdenking:	In welk geval:	Bevoegd tot vorderen:	Van welke derde:
					van onderzoek.
Ook andere dan identificerende gegevens (historisch). Art. 126nd Sv en 126ud Sv.	Alle gegevens met uitzondering van gevoelige gegevens. Betreft o.a. gegevens over diensten die verleend zijn (duur, data, plaats, aard dienstverlening) en rekening- en betalingsgegevens.	- een misdrijf als omschreven in art. 67 lid 1 Sv, of - het in georganiseerd verband beramen of plegen van misdrijven als omschreven in art. 67 lid 1 Sv die gezien hun aard of de samenhang met andere misdrijven die in dat georganiseerde verband worden beraamd of gepleegd een ernstige inbreuk op de rechtsorde opleveren.	In het belang van het onderzoek.	Officier van justitie.	Degene van wie redelijkerwijs kan worden vermoed dat hij toegang tot bepaalde opgeslagen of vastgelegde gegevens heeft. De derde die slechts ten behoeve van persoonlijk gebruik gegevens verwerkt valt hier ook onder.

Vorderen van:	**Aard gegevens:**	**Benodigde verdenking:**	**In welk geval:**	**Bevoegd tot vorderen:**	**Van welke derde:**
	Kan ook identificerende gegevens betreffen.	De ovj kan in geval van een lichter strafbaar feit ook andere dan identificerende gegevens vorderen. Een machtiging van de rechter-commissaris is dan vereist (art. 126nd lid 6 Sv).			Concrete feiten of omstandigheden moeten een redelijk vermoeden rechtvaardigen dat bepaalde gegevens bij de derde beschikbaar zijn. Geen redelijk vermoeden maar wel aanwijzingen? Dan kan duidelijkheid verkregen worden door art. 126nc Sv te gebruiken.
Ook andere dan identificerende gegevens (toekomstig).	Alle gegevens met uitzondering van gevoelige gegevens. Deze gegevens zijn op het moment van de vordering nog niet	- een misdrijf als omschreven in art. 67 lid 1 Sv, of - het in georganiseerd verband beramen of plegen van misdrijven als omschreven in art. 67 lid 1 Sv die gezien hun aard of de samenhang met andere misdrijven die in dat georganiseer-	In het belang van het onderzoek. Een vordering om toekomstige	Officier van justitie. Een vordering om toekomstige gegevens *direct* te verstrekken: officier van justitie na machti-	Degene van wie redelijkerwijs kan worden vermoed dat hij toegang tot bepaalde opgeslagen of vastgelegde gegevens zal krijgen en die anders dan ten behoeve van persoonlijk gebruik gegevens verwerkt.

Vorderen van:	**Aard gegevens:**	**Benodigde verdenking:**	**In welk geval:**	**Bevoegd tot vorderen:**	**Van welke derde:**
Art. 126ne Sv en art. 126ue Sv.	verwerkt door de derde. Betreft o.a. gegevens over diensten die verleend zijn (duur, data, plaats, aard dienstverlening) en rekening- en betalingsgegevens.	de verband worden beraamd of gepleegd een ernstige inbreuk op de rechtsorde opleveren.	gegevens *direct* te verstrekken kan slechts indien het belang van het onderzoek dit *dringend* vordert.	ging Rechter-Commissaris.	Concrete feiten of omstandigheden moeten een redelijk vermoeden rechtvaardigen dat bepaalde gegevens bij de derde beschikbaar zijn. Het betreft het verwerken van gegevens vanwege een functie of beroepsuitoefening.
Gevoelige gegevens. Art. 126nf Sv en art. 126uf Sv.	Gegevens als bedoeld in art. 16 van de Wbp. Betreft o.a. persoonsgegevens over godsdienst of levensovertuiging ras, politieke gezindheid, gezondheid, seksuele	- een misdrijf als omschreven in art. 67 lid 1 Sv dat gezien zijn aard of samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert of - het in georganiseerd verband beramen of plegen van misdrij-	Indien het onderzoek dit *dringend* vordert.	Officier van justitie na machtiging Rechter-Commissaris.	Degene van wie redelijkerwijs kan worden vermoed dat hij toegang tot bepaalde opgeslagen of vastgelegde gegevens heeft. De derde die slechts ten behoeve van persoonlijk gebruik gegevens ver-

Vorderen van:	**Aard gegevens:**	**Benodigde verdenking:**	**In welk geval:**	**Bevoegd tot vorderen:**	**Van welke derde:**
	leven of lidmaatschap vakvereniging.	ven als omschreven in art. 67 lid 1 Sv die gezien hun aard of de samenhang met andere misdrijven die in dat georganiseerde verband worden beraamd of gepleegd een ernstige inbreuk op de rechtsorde opleveren.			werkt valt hier ook onder.
Ontsleutelen van versleutelde gegevens. Art. 126nh Sv en art. 126uh Sv.	Alle gegevens (identificerende gegevens, andere dan identificerende gegevens en gevoelige gegevens). Het betreft het bevelen medewerking te verlenen aan het ontsleutelen van de gegevens door de ver-	Bij of terstond na de toepassing van art. 126nd lid 1 Sv, 126ne lid 1 of 3 Sv, 126nf lid 1 Sv (dus bij of terstond na vordering m.b.t. identificerende gegevens, andere dan identificerende gegevens of gevoelige gegevens).	In het belang van het onderzoek.	Officier van justitie.	Degene van wie redelijkerwijs kan worden vermoed dat hij kennis draagt van de wijze van versleuteling van de in deze artikelen bedoelde gegevens.

Vorderen van:	**Aard gegevens:**	**Benodigde verdenking:**	**In welk geval:**	**Bevoegd tot vorderen:**	**Van welke derde:**
	sleuteling ongedaan te maken, dan wel deze kennis ter beschikking te stellen.				
Doorzoeking *uitsluitend* ter vastlegging van gegevens. Art. 125i Sv.	Gegevens die, hetzij op papier, hetzij op enige andere gegevensdrager, daaronder begrepen een geautoriseerd werk, zijn opgeslagen. Betreft alle gegevens (identificerende gegevens, andere dan identificerende gegevens en gevoelige gegevens).	- ontdekking op heterdaad van een strafbaar feit of - een misdrijf als omschreven in art. 67 lid 1 Sv.	In het belang van het onderzoek. Slechts mogelijk indien andere bevoegdheden, zoals het vorderen van gegevens of het vorderen van	Rechter-Commissaris, (hulp)officier van justitie, opsporingsambtenaar. - Rechter-Commissaris: doorzoeken van elke plaats (art. 110 lid 1 en 2 Sv). Op vordering van de officier van justitie en in het GVO	

Vorderen van:	Aard gegevens:	Benodigde verdenking:	In welk geval:	Bevoegd tot vorderen:	Van welke derde:
	NB: het betreft het onderzoek doen naar, inzage verkrijgen in en kopie maken van deze gegevens.		de uitlevering van een voorwerp ter inbeslagneming niet effectief zijn.	ambtshalve. - (Hulp)officier van justitie: doorzoeken van een andere plaats dan een woning en een kantoor van een verschoningsgerechtigde (art. 96c lid 1, 2 en 3 Sv). doorzoeken van een woning en een kantoor van een geheimhouder indien: - dringende noodzakelijkheid en optreden	

Vorderen van:	Aard gegevens:	Benodigde verdenking:	In welk geval:	Bevoegd tot vorderen:	Van welke derde:
				RC niet kan worden afgewacht (schriftelijke machtiging RC nodig) (art. 97 lid 1 t/m 4 Sv). - opsporingsambtenaar: doorzoeken van een vervoermiddel, m.u.v. het woongedeelte (art. 96b Sv).	

Bijlage 2 Samenstelling van de begeleidingscommissie

Prof. mr. E. Stamhuis (voorzitter), Open Universiteit.

Dr. F. Beijaard, Wetenschappelijk Onderzoek- en Documentatiecentrum, ministerie van Justitie.

Mr. M. Jongeneel-van Amerongen, Directie Wetgeving, ministerie van Justitie.

Mr. I.C.M.E. Meissen, Landelijk Parket.

Mr. F.B.M. Olijslager, ING Bank.

Bibliografie

AID 2008

AID, *Jaarverslag 2008*. Via: www.vwa.nl (geraadpleegd 20 december 2010).

Blom 2009

T. Blom, 'aant. 3 bij art. 126n Sv', in C.P.M. Cleiren en J.F. Nijboer (red.), *Tekst & Commentaar Strafvordering,* achtste druk*,* Deventer, Kluwer, 2009.

Bokhorst e.a. 2002

R.J. Bokhorst, C.H. de Kogel en C.F.M. van der Meij, *Evaluatie van de wet BOB – fase 1. De eerste praktijkervaringen met de Wet Bijzondere opsporingsbevoegdheden*, Den Haag, Boom Juridische uitgevers, 2002.

Borgers en Kooijmans 2010

M.J. Borgers en T. Kooijmans, 'Verruiming, vereenvoudiging en verbetering? Het wetsvoorstel verruiming mogelijkheden voordeelontneming', *Delict en Delinkwent*, Afl. 3/16, 2010, p. 205-270.

Van Daele en Van Geebergen 2007

D. van Daele en B. van Geebergen, *Criminaliteit en rechtshandhaving in de Euregio Maas-Rijn, Deel 2*. Antwerpen/Oxford, Intersentia, 2007.

Van de Griend 2002

E. van de Griend, *Hiaten in de strafrechtelijke rechtsbescherming*, (dissertatie Universiteit van Tilburg), Nijmegen, Wolf Legal Publishers, 2002.

Groenhuijsen en Knigge 2004

M. Groenhuijsen en G. Knigge, *Afronding en verantwoording. Eindrapport onderzoeksproject Strafvordering 2001*, Deventer, Kluwer, 2004.

Hoekendijk 2009

M. Hoekendijk, *Zakboek Proces-Verbaal en Bewijsrecht 2010-2011*, Deventer, Kluwer, 2009.

Jongeneel-van Amerongen 2005

M. Jongeneel-van Amerongen, 'Wet bevoegdheden vorderen gegevens', *Ars Aequi,* (54), 2005-11, p. 954-961.

Knigge 2009

G. Knigge, 'De verkalking voorbij', RM Themis 2000, p. 83-96, in J. de Hullu, *Materieel strafrecht. Over algemene leerstukken van strafrechtelijke aansprakelijkheid naar Nederlands recht*, Deventer, Kluwer, 2009.

Mac Gillavry 2006
E.C. Mac Gillavry, 'aant. 4 op art. 126nc' (suppl. 154, april 2006), in Melai/Groenhuijsen e.a. (red.), *Het Wetboek van Strafvordering,* Deventer, Kluwer, 2006.

Mevis 2002
P. Mevis, 'Gegevensvergaring is iets anders dan een informatieplicht', *RM Themis* 2002, p. 30-35.

Michiels 2009
F. Michiels, *Hoofdzaken van het bestuursrecht,* Deventer, Kluwer, 2009.

De Poot e.a. 2004
C. de Poot, R. Bokhorst, P. van Koppen en E. Muller, *Rechercheportret. Over dilemma's in de opsporing*, Alphen aan den Rijn, Kluwer, 2004.

Rapport Commissie Mevis 2001
P. Mevis e.a., *Gegevensvergaring in strafvordering. Nieuwe bevoegdheden tot het vorderen van gegevens ten behoeve van strafvorderlijk onderzoek, rapport van de Commissie Strafvorderlijke gegevensvergaring in de informatiemaatschappij*, 2001. Via: www.ejure.nl (geraadpleegd 23 november 2010).

Smits 2006
A. Smits, *Strafvorderlijk onderzoek telecommunicatie* (diss. Universiteit van Tilburg), Nijmegen, Wolf Legal Publishers, 2006.

Smits 2008
L. Smits, 'Art. 81 Awr als lex specialis door de ontwikkelingen in het commune strafprocesrecht achterhaald?', *WFR* 2008, p. 907-913.

Spapens 2006
T. Spapens. *Interactie tussen criminaliteit en opsporing*. Antwerpen/Oxford, Intersentia, 2006.

Wiemans 2006
F.P.E. Wiemans, 'aant. 3 op art. 125la' (suppl. 156, augustus 2006), in Melai/Groenhuijsen e.a. (red.), *Het Wetboek van Strafvordering,* Deventer, Kluwer, 2006.