



Inspectie Openbare Orde en
Veiligheid
Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties

Masterthesis Jelle Kort, Universiteit Twente

Open je hart

*Een onderzoek naar de beperkte uitwisseling
van opsporingsinformatie tussen
Nederlandse politiekorpsen*

Masterthesis Jelle Kort, Universiteit Twente

Open je hart

*Een onderzoek naar de beperkte uitwisseling van opsporingsinformatie tussen
Nederlandse politiekorpsen*

Publicatiedatum:

November 2010

Begeleidingscommissie:

Dr. A.J.J. Meershoek

Prof. dr. A. Need

Begeleider Inspectie OOV:

Drs. J.N.M. Groot (MBA)

Voorwoord

Een enorme hoeveelheid, vaak belangrijke informatie vormt het hart van politiewerk. Deze informatie op juiste wijze te beheren en optimaal te delen binnen de politieorganisatie en waar mogelijk met partners, is voor de veiligheid van groot belang. Daarvoor is transparantie nodig; openheid. Vandaar de titel van deze rapportage: open je hart. Door onder meer de opkomst van complexere vormen en door 'ontgrenzing' van criminaliteit in de afgelopen jaren, is het belang van een goede informatiehuishouding voor de effectiviteit van de opsporing nog verder toegenomen. Tegen deze achtergrond stelt de vooruitgang van de computertechniek de politie voor de vraag, hoe zij daarvan optimaal kan profiteren. Grote inspanningen op het terrein van de informatiehuishouding, hebben tot op heden niet tot het gewenste resultaat van een goed werkend systeem van landelijk gedeelde politie-informatie geleid. Zo blijkt uit publicaties van de Inspectie Openbare Orde en Veiligheid.

Dit onderzoek beschrijft wanneer opsporingsgegevens niet optimaal worden uitgewisseld tussen Nederlandse politiekorpsen. Vervolgens wordt getracht daarvoor verklaringen te vinden. Voor dit onderzoek is literatuurstudie verricht, zijn documenten bestudeerd en hebben interviews plaatsgevonden met politiemedewerkers op operationeel, tactisch en strategisch niveau in vijf verschillende korpsen.

Ik ben de geïnterviewde politiemedewerkers bijzonder dankbaar voor hun tijd en openheid. De Inspectie Openbare Orde en Veiligheid gaf opdracht voor dit onderzoek en stelde mij een werkplek ter beschikking. Daardoor heb ik kennis kunnen nemen van het Haagse wereldje waar iedereen zo dol op is, het inspectiewerk zelf en van uiteenlopende discussies in het veiligheidsveld. Dat alles op bijzonder informele en plezierige wijze. Ik wil de medewerkers van de Inspectie daarom hartelijk bedanken voor een leerzame periode in hun midden en in het bijzonder drs. Jos Groot voor zijn intensieve begeleiding. Aan mijn leerervaring heeft ook bijzonder bijgedragen de begeleidingscommissie van Universiteit Twente, bestaande uit dr. Guus Meershoek en prof. dr. Ariana Need. Guus Meershoek begeleidde mij nu voor de tweede keer, hij deed dat ook toen ik het bacheloronderzoek schreef en geldt in mijn ogen als een bijzonder vriendelijke leermeester. Bedankt daarvoor.

Enschede, november 2010

*That's right captain, think I got the ringleader.
If that's what you want, okidoki man, bye bye.*

«clack»

Shit, Texas Rangers!

He wants me to hold off on pickin' this fellow up, until him and his boys get up here.

He wants to get his picture in the newspaper. We do all the work, they get all the glory. That's just the way the world is. Isn't that right Samuel?

Inhoud

Voorwoord	5
1. Inleiding	11
1.1 Informatie Gestuurde Politie in Nederland	13
1.2 Aanleiding: Uitwisseling opsporingsgegevens laat te wensen over	19
1.3 Probleemstelling en onderzoeksvragen	23
1.4 Korte samenvatting van het verklaringsschema	25
1.5 Onderzoeksafbakening	27
1.6 Operationalisatie van te onderzoeken factoren	29
1.7 Onderzoeksontwerp	30
1.8 Relevantie van het onderzoek	36
1.9 Verdere indeling van het rapport	38
2. Informatiedeling is afhankelijk van diverse fronten	39
2.1 Informatiedeling: een kwestie van verschillende belangen	39
2.2 Motivatie voor het gekozen verklaringsschema	42
3. Beleid Uitwisseling Opsporingsinformatie	49
3.1 Doelstelling van het beleid	49
3.2 Basisregels	51
3.3 Werkwijze bij bevestigingen	55
3.4 Beveiligingskader	57
3.5 Toezicht en beheer	61
4. Barrières in de informatie-uitwisseling	63
4.1 Algemeen: informatiesystemen niet meer weg te denken	64
4.2 Invoer	66
4.3 Informatie delen	69
4.4 Tussenconclusie: beperkte invoer, beperkte raadpleegbaarheid	77
5. Juridische omstandigheden: de Wpg in theorie en praktijk	81
5.1 De Wet politieregisters en de Wet politiegegevens (2008)	82
5.2 Versterking van het <i>free-flow</i> principe in de Wpg	85
5.3 Intern ter beschikking stellen van gegevens	88
5.4 Juridische knelpunten	92
5.5 Tussenconclusie: beperkte invloed van juridische knelpunten	104
6. Technologische omstandigheden: de acceptatie van ICT	106
6.1 Acceptatie van nieuwe ICT in organisaties	107
6.2 Beleving van prestaties	108
6.3 Beleving van de benodigde inspanning bij het gebruik	110
6.4 Sociale beïnvloeding	114
6.5 Faciliteren van gebruikers	116
6.6 Tussenconclusie: acceptatie van nieuwe systemen is een knelpunt	119
7. Organisatorische omstandigheden: kunnen én willen delen	123
7.1 De politie als <i>Human Service Organisation</i>	124
7.2 De sturing op informatiedeling op korps- en teamniveau	129
7.3 Organisatiedoelen en evaluatiecriteria	136
7.4 Tussenconclusie	141
8. Politiewerk is en blijft spannend	142
8.1 De aard van het politiewerk	142
8.2 Politie mensen beleven risico's bij informatiedeling	145
8.3 Politiewerk: mensenwerk?	148
8.4 Tussenconclusie: taaiere problemen op organisatorisch vlak	153
9. Conclusie	159
9.1 Slotoverweging	162
9.2 Aanbevelingen	164
Lijst van veelgebruikte afkortingen	166
Literatuurlijst	167
Geraadpleegde bronnen	169
Abstract	170
Summary	172

1. Inleiding

Artikel 2 van de Politiewet 1993 omschrijft de algemene taak van de Nederlandse politie.

De tekst van dit artikel luidt:

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

Informatie is een cruciaal onderdeel van deze politietaak. Informatie speelt een belangrijke rol bij de handhaving van de rechtsorde en bij een goede uitvoering van de hulpverlening. Het verzamelen en bewerken van informatie staat ook centraal bij het uitvoeren van rechercheonderzoek.¹ In sommige gevallen kan bij de politie bekende informatie van levensbelang zijn voor burgers en voor haar eigen medewerkers. Vanwege haar opsporingsbevoegdheden en 24-uurs aanwezigheid in de samenleving, heeft de politie een bijzondere signalerings- en adviesfunctie in de richting van haar partners in het veiligheidsketen, Justitie, gemeenten, reclassering en hulpverleners.

De ontwikkelingen van de laatste decennia op het gebied van informatie- en communicatietechnologie (ICT) hebben nieuwe mogelijkheden geopend voor de informatiehuishouding binnen het politieapparaat. Het gaat daarbij om het beschikbaar maken van de juiste informatie, van de juiste kwaliteit, op het juiste moment op de juiste plek, tegen aanvaardbare kosten.²

De politie werd voor de vraag gesteld hoe de toegenomen mogelijkheden van het gebruik van informatie, tot een vergroting van de veiligheid kunnen leiden. In antwoord op deze vraag wordt het begrip *informatie gestuurde politie* (IGP) omarmd. In *Politie in Ontwikkeling*, het visiedocument van de politie opgesteld door de Raad van Hoofdcommissarissen (RHC), worden informatie gestuurd werken en informatie-uitwisseling met partners als randvoorwaarden genoemd voor het realiseren van een politie die functioneel en lokaal georganiseerd is. Beoogd wordt een gebiedsgebonden politie die behalve een lokale oriëntatie dichtbij de burger, ook een nodale oriëntatie heeft. Hierin wordt de geografische ruimte buiten de woongebieden opgevat als een open infrastructuur. Ontgrenzing, mobiliteit en anonimiteit staan centraal bij de

¹ Poot, C.J. de et al (2004), *Rechercheportret, over de dilemma's in de opsporing*, Alphen aan den Rijn, p. 347

² Zuurmond, A. en Meesters, M.J. (2007), *ICT en de moderne politieorganisatie*, in: *Politie, studies over haar werking en organisatie*, in: Fijnaut, C.J.C.F., Muller, E.R. & Rosenthal, U (red.), *Politie: Studies over haar werking en organisatie*, Deventer, p. 400

veranderingen die zich hebben voorgedaan in de belangrijkste criminogene factoren. De knooppunten (nodes) van de open infrastructuur zijn een belangrijker aangrijpingspunt voor politiewerk gaan vormen. Op deze knooppunten kan de politie controles uitoefenen op stromen van mensen, goederen, geld en informatie, gericht op het identificeren van kwaad in de vorm van potentiële en actuele bedreigingen. De kwaliteit van de informatiehuishouding speelt hierbij natuurlijk een rol van betekenis.³

Een goede informatiehuishouding is van steeds groter belang voor de politie die ook steeds meer op een informatiegedreven strategie inzet. De informatiehuishouding, met name de uitwisseling van opsporingsinformatie tussen Nederlandse politiekorpsen onderling, vormt het onderwerp van dit onderzoek. In Nederland is de politie opgebouwd uit 25 regionale korpsen en het Korps Landelijke Politie Diensten (KLPD). Mensen die in de aandacht staan van de politie bewegen zich zowel over de grenzen van de politieregio's als over landsgrenzen. Het ligt dus voor de hand dat korpsen onafhankelijk van elkaar informatie verzamelen over dezelfde personen. Vaak is het in die situatie voor de opsporing van belang deze informatie samen te brengen. Voor een goede uitvoering van de politietaak is essentieel dat op een efficiënte wijze bruikbare en juiste informatie wordt uitgewisseld tussen de verschillende korpsen en dienstonderdelen die zich bezighouden met de uitvoering van de politietaak. In het oog springend is het belang van informatie-uitwisseling voor het opsporingsproces maar deze kan ook ondersteunend zijn aan strategische en tactische besluitvorming. Wat is belangrijk, wat gaan we doen en hoe gaan we het doen? Vanwege het belang van een effectieve opsporing en gegeven de huidige mogelijkheden op het gebied van ICT, is een goede informatie-uitwisseling een belangrijke peiler onder het regionale bestel geworden. Er is immers vanuit de politiek een sterke roep om eenheid en samenwerking binnen de politie. Informatie vormt het hart van researchewerk en de kwestie is nu, zoals zal blijken uit deze inleiding, dat hart zoveel mogelijk te openen.

³ Raad van Hoofdcommissarissen (2005), *Politie in Ontwikkeling*, Den Haag, pp. 81-92

1.1 Informatie Gestuurde Politie in Nederland

De kerngedachte van informatie gestuurde politie is dat de politie eerst een goede analyse uitvoert van de haar ter beschikking staande informatie, alvorens zij besluit wat ze zal gaan aanpakken en hoe ze dat gaat doen om daardoor effectiever te kunnen optreden. Deze kerngedachte is niet nieuw; de politie is al sinds de jaren '70 bezig deze strategie in de organisatie in te bedden, maar zonder veel succes.⁴ Anders is dat in Groot-Brittannië en de Verenigde Staten waar informatie gestuurde in een deel van de korpsen wordt toegepast, met dalende criminaliteitscijfers⁵ als gevolg.

In 2000 formeerde de Raad van Hoofdcommissarissen de Stuurgroep *informatie gestuurde opsporing*. De vraag van de Raad van Hoofdcommissarissen aan deze stuurgroep was te onderzoeken hoe de politie en het Openbaar Ministerie door middel van een beter gebruik van gegevens en informatie, betere resultaten in de opsporing kunnen bereiken. De stuurgroep concludeerde dat *informatie gestuurde opsporing* zou kunnen dienen als raamwerk waarin lopende zaken en nieuwe ontwikkelingen met elkaar in samenhang kunnen worden gebracht, waardoor er harmonisatie in de opsporing ontstaat. Ze beveelt vervolgens aan om het concept nader uit te werken voor de Nederlandse situatie. Die uitwerking werd ter hand genomen binnen het programmabureau ABRIO, een samenwerkingsverband tussen de politie en het Openbaar Ministerie. Van 2001 tot 2003 worden binnen het project informatie gestuurde opsporing, in nauwe samenwerking met de politiekorpsen, zes elementen ontwikkeld die sturing volgens informatie gestuurde opsporing mogelijk maken.⁶ Het zijn:

1. Sturingsmodel informatie gestuurde opsporing. Het sturingsmodel maakt het verband zichtbaar tussen doelen, strategie, middelen en processen van een organisatie. Vanuit de strategie worden resultaatdoelstellingen geformuleerd en middelen toegewezen ten behoeve van besturing van de verschillende processen.
2. Briefing – debriefing. Het houden van een briefing is het geven van essentiële informatie en duidelijke instructies voorafgaand aan de uitvoering van het werk. Debriefing is het leren en verantwoorden van uitgevoerd werk door het terugkoppelen van het resultaat.

⁴ Stol, W.Ph. (2007), *Informatie voor politiewerk: basisprincipes*, in: Fijnaut, C.J.C.F., Muller, E.R. & Rosenthal, U (red.), p. 381

⁵ *Idem*

⁶ Inspectie OOV (2008a), *Informatiegestuurde politie*, Den Haag, pp. 17-22

3. Informatieorganisatie. Op ieder organisatieniveau is een informatieorganisatie ingericht op het inwinnen, de coördinatie, de veredeling en de verspreiding van toepasbare kennis en informatie.

4. Projectvoorbereiding. De projectvoorbereiding is het op een gestructureerde wijze voorbereiden van opsporingsonderzoeken.

5. Analyseproducten. Producten die de politie en haar bevoegd gezag gebruikt om inzicht te krijgen in de externe omgeving. Deze producten hebben het doel om de prioriteiten vast te kunnen stellen voor een bepaalde periode.

6. Restinformatie. Procedure om restinformatie niet verloren te laten gaan.

Bij het uitwerken van deze elementen is zoveel mogelijk rekening gehouden met relevante ontwikkelingen binnen de Nederlandse politie. Tijdens het Project Landelijke Informatie Coördinatie is bijvoorbeeld het NIK-RIK-DIK-kanaal⁷ ontwikkeld: Een drietal zogeheten informatieknooppunten in de politieorganisatie die functioneren op nationaal, regionaal en districtelijk niveau. Informatie kan zo op ieder niveau worden verzameld en doorgeleid naar het niveau waar het wordt gebruikt. Dit kanaal vormt de kern van de intelligence-organisatie.⁸

In de eerste helft van 2004 is begonnen met de implementatie binnen de korpsen. Het gaat dan niet meer om *informatie gestuurde opsporing* maar om *informatie gestuurde politie*. Begin januari 2004 is *informatie gestuurde opsporing* namelijk door de Raad van Hoofdcommissarissen van toepassing verklaard voor al het politiewerk en daarmee verbreed tot *informatie gestuurde politie*. De redenen om gebruik te gaan maken van *informatie gestuurde politie* zijn:

- Een effectiever ingerichte bedrijfsvoering.
- Het meetbaar maken van de resultaten.
- Het verbeteren van de resultaten.
- Een eenduidige manier van werken en beschrijving van werkprocessen.
- Optimale uitwisseling van informatie tussen korpsen onderling en het OM.
- Het bevorderen van de deskundigheid van de medewerkers.

De ambitie in *Politie in Ontwikkeling* is om “informatie en kennis een grotere rol te laten spelen. Waarneming en het verzamelen van informatie vormen niet alleen de grondslag voor het dagelijks opereren van de politie op lokaal niveau, maar ook voor analyse en veredeling van informatie voor andere

⁷ Nationaal Informatie Knooppunt, Regionaal Informatie Knooppunt, Districtelijk Informatie Knooppunt

⁸ ABRIO (2005), *Informatie-gestuurde politie, sturen op resultaat*.

veiligheidsdoelen. Op die manier vormt de dagelijkse uitvoering van politietaken de uiterst belangrijke basis voor de algehele uitvoering van de politiefunctie. Het concept *informatie gestuurde opsporing* legt een sterke koppeling tussen het opsporingsproces en het informatieproces. Gegevens en informatie moeten leiden tot sturing op strategisch niveau, voor het formuleren van beleid op het gebied van misdaadbesteding en sturing op tactisch niveau, ten aanzien van het maken van concrete keuzes in onderzoeken.”⁹

In 2008 doet de Inspectie OOV de aanbeveling aan de korpschefs om te investeren in het informatiebewustzijn van de medewerkers in hun korpsen. Iedere medewerker van leidinggevende tot uitvoerende, zal gedisciplineerd moeten werken volgens de principes van *informatie gestuurde politie*: sturen op basis van geanalyseerde problemen in plaats van meegaan met de waan van de dag. Volgens de Inspectie hebben korpsen, ieder op hun eigen manier, de instrumenten voor *informatie gestuurde politie* ontwikkeld, maar blijft het daadwerkelijke gebruik daarvan achter.¹⁰

Eveneens in 2008 heeft de Raad van Hoofdcommissarissen het Nationaal Intelligence Model (NIM) vastgesteld. Hierin werd gesteld dat op 12 december 2012 alle korpsen informatie gestuurd moeten werken. Het programma Intelligence ondersteunt de implementatie van het Nationaal Intelligence Model en kent de volgende doelstelling: “De politie leert in de sturing en in de uitvoering van het politiewerk concernbreed veel beter met intelligence te werken en daarmee effectiever te worden. Door de informatieorganisatie van de politie moeten verbanden tussen delicten en dadergroepen, op (inter)lokaal, (boven)regionaal en (inter)nationaal niveau, sneller en beter worden gelegd.”¹¹

De ICT-basisvoorzieningen vormen een belangrijke stap op weg naar al deze doelstellingen zoals blijkt uit *Wenkend Perspectief*, de visie van de Raad van Hoofdcommissarissen op het informatiemanagement van de politie uit 2006. De wens van een landelijk uniforme informatiearchitectuur was overigens niet nieuw. In 2000 werd al een masterplan gepresenteerd voor de ontwikkeling van de informatiehuishouding, dat binnen vijf jaar gerealiseerd had moeten zijn. Opzet was uniforme applicatiesuites te ontwikkelen voor de primaire en ondersteunende politieprocessen. Een beoogde mijlpaal daarbij was de oplevering van de zogeheten gemeenschappelijke opsporingsapplicatie ‘Politie

⁹ Raad van Hoofdcommissarissen (2008), p. 17

¹⁰ Inspectie OOV (2008a), pp. 7-8

¹¹ Raad van Hoofdcommissarissen (2008), *Programmaplan Intelligence 2008: Sturing, Informatieorganisatie, Verbetering en Innovatie*

Suite Opsporing' in 2004. Deze werd niet gehaald; de systeemontwikkeling werd voortijdig beëindigd. Vanaf 2004 wordt besloten de strategie te veranderen.¹² De keuze wordt gemaakt om de weg der geleidelijkheid te bewandelen. In *Wenkend Perspectief* wordt gesteld dat – om in een veranderende samenleving de functies handhaven, opsporen, noodhulp, signaleren en adviseren adequaat te kunnen blijven uitvoeren – informatie gestuurd politiewerk en informatie-uitwisseling in het totale veiligheidsdomein voorwaarden zijn. Samenhang en samenwerking zijn vereist om de kwaliteit en efficiency tot stand te kunnen brengen, die steeds meer van de politie worden gevraagd. Geconstateerd wordt dat ICT-harmonisatie noodzakelijk is en gekozen wordt, bij wijze van tussenstap, bestaande ICT-systemen te integreren die technisch gezien teruggaan tot de jaren '80 en '90.¹³ Korpsen gebruiken verschillende systemen en de uniformering houdt in dat elk korps in de toekomst Xpol moet gebruiken voor handhaving en het Recherche Basissysteem (RBS) voor de opsporing.¹⁴ Dat zijn ICT-systemen die in een deel van de korpsen al werden gebruikt. Het doel bleef één politieke informatievoorziening.

“De korpsen verzamelen informatie op basis van waarneming ter plaatse, door contacten met de burgerij en via netwerken waarin zij participeren. De belangrijkste operationele informatie ligt per regio vast in een van de drie primaire systemen en een van beide opsporingssystemen. Met de bouw van BlueView (...) is in 2005 het grootste deel van deze informatie landelijk bevroegbaar gemaakt. Op deze manier is een grote stap gezet richting één landelijke politieke informatiehuishouding. De komende jaren zullen standaardisatie van primaire processen en meer professionele sturings- en verantwoordingsmechanismen onherroepelijk leiden tot aanpassingen in de bedrijfsvoering van de korpsen. Onnodige verschillen zullen stap voor stap worden weggewerkt. Deze onontkoombare modernisering en uniformering (...) leiden tot operationele voordelen en veiligheid (betere en snellere invoer, zoek- en analysemogelijkheden) en tot kostenbesparingen. De inrichting van de basisvoorzieningen wordt geüniformeerd en het gebruik wordt verplicht gesteld.”¹⁵

1.1.1 Goede informatiehuishouding: een lastige opgave

¹² Bekkers, V., M. Thaens, G. van Straten en P. Siep (2009), *Informatiemanagement binnen de politie. Van praktijk naar normatief kader*. Politiekunde 23, Politie & Wetenschap, Apeldoorn, p. 54

¹³ Raad van Hoofdcommissarissen (2006), *Wenkend Perspectief*, Driebergen, pp. 15-18

¹⁴ *Idem*, p. 27

¹⁵ *Idem*, p. 19

Een goede informatiehuishouding blijkt een complexe opgave voor de politie. Rond 2000 stelt de Minister van Binnenlandse Zaken en Koninkrijksrelaties (BZK) dat de politieautomatisering en informatisering niet meer aan de eisen van de moderne tijd voldoen. Hij meldt aan de Tweede Kamer dat er op verschillende terreinen een zorgwekkende achterstand bestaat. De infrastructuur is verouderd, de vernieuwing van applicaties en systemen is onvoldoende, de coördinatie tussen de korpsen is onvoldoende en de voorwaarden voor een transparante bedrijfsvoering zijn niet optimaal.¹⁶ Een verklaring voor de opgelopen achterstand is volgens het ministerie dat de korpsen zich na de reorganisatie (c.q. de regionalisatie in 1993-1994) te veel met hun eigen korps(opbouw) bezig hebben gehouden en niet met informatie-uitwisseling.¹⁷

Uit het coalitieakkoord van het kabinet CDA-PvdA-ChristenUnie blijkt het streven om deze problemen aan te pakken: “De samenwerking en het gemeenschappelijk functioneren van politiekorpsen moeten worden verbeterd. (...) Er dient een geïntegreerd politie-informatiesysteem en ICT-netwerk te komen.”¹⁸

Ook de Raad van Hoofdcommissarissen heeft dit streven verwoord: “De politieorganisatie deelt kennis en informatie binnen de eigen organisatie tussen alle onderdelen, zoals regionale korpsen en landelijke diensten, en in internationale verbanden. Informatie moet binnen de eigen organisatie zoveel mogelijk een neutraal productiegoed worden ten gunste van de effectiviteit van het gehele primaire proces. De informatiesystemen van de politie, zoals HKS (Herkenningsdienstsysteem), dienen hierop te worden toegespitst. Verder deelt de politie informatie met andere partners met een veiligheidsfunctie in het totale veiligheidsdomein.”¹⁹

Samengevat is de bedoeling van dit alles dat medewerkers van verschillende korpsen bijvoorbeeld bij een opsporingsonderzoek snel en gemakkelijk informatie kunnen delen. Bovendien moet de uitwisseling van gegevens met externe partners, nationaal maar zeker ook Europees (Schengen: SIS II, Europol: EIS), aanmerkelijk verbeterd worden.

Om de gewenste samenwerking en informatiedeling te realiseren, hebben de ministers van BZK en van Justitie met de korpsbeheerders medio 2007 op 19

¹⁶ Tweede Kamer (2000), *Brief van de minister van Binnenlandse Zaken en Koninkrijksrelaties, Beleidsplan Nederlandse Politie*. 26345, nr. 11

¹⁷ BZK (1999), *Brief aan de Tweede Kamer over de stand van zaken politieke informatiehuishouding* (U76403)

¹⁸ Coalitieakkoord *Samen werken, samen leven*. Kamerstukken II, 2006-2007, 30891, nr. 4, p. 33

¹⁹ Raad van Hoofdcommissarissen (2005), p. 94

punten afspraken gemaakt; de zogeheten samenwerkingsafspraken politie 2008.²⁰ Onderdeel van de samenwerkingsafspraken was dat de Inspectie Openbare Orde en Veiligheid (Inspectie OOV) vanaf medio 2008 de behaalde resultaten in de korpsen zou toetsen.

Onder meer de ICT-systemen Basisvoorziening Handhaving (BVH) en de Basisvoorziening Opsporing (BVO) behoorden tot de onderzochte samenwerkingsafspraken en werden getoetst door de Inspectie OOV. BVH is een landelijk geautomatiseerd basissysteem voor alle kernprocessen van de politie en wordt tevens gebruikt voor sturings-, informatie- en ondersteuningsdoeleinden. Met dit systeem kunnen bijvoorbeeld meldingen worden geregistreerd, aangiftes worden verwerkt en incidenten worden afgehandeld. BVO is een informatiesysteem dat op landelijk uniforme wijze de informatiehuishouding en informatiedeling in het opsporingsproces ondersteunt. Daarnaast werd BlueView getoetst; een zoekmachine waarmee registraties van alle politiekorpsen over handhaving en opsporing direct kunnen worden geraadpleegd. Gegevens uit BVH en bepaalde gegevens uit BVO worden in dit systeem ontsloten, naast gegevens uit diverse andere informatiesystemen die gefaseerd door BVO worden vervangen. Voorbeelden van uit te faseren systemen zijn het Recherche Basissysteem (RBS) en Octopus.

Uit het onderzoeksrapport van de Inspectie OOV dat werd gepubliceerd in november 2008, bleek dat onder meer aan de genoemde drie samenwerkingsafspraken niet volledig werd voldaan. Geconcludeerd werd dat van de door het kabinet beoogde landelijke informatiedeling door politiekorpsen nog niet volledig sprake was.²¹ Uit het onderzoek bleek onder meer een zekere terughoudendheid bij politiekorpsen in het beschikbaar stellen van opsporingsinformatie aan elkaar.²² Vanwege deze conclusies heeft de Inspectie opdracht gegeven voor dit verdiepende onderzoek.

De volgende paragraaf gaat nader in op het onderzoek van de Inspectie OOV, dat de directe aanleiding vormt voor deze studie. De ICT-basisvoorzieningen worden hierin behandeld, in relatie tot het probleem van de beperkte uitwisseling van opsporingsinformatie tussen korpsen.

²⁰ *Samenwerkingsafspraken politie 2008*. Kamerstukken II, 2007-2008, 30880, nr. 6

²¹ Inspectie OOV (2008), *Samenwerkingsafspraken politie 2008*, p. 9

²² *Idem*, p. 23

1.2 Aanleiding: Uitwisseling opsporingsgegevens laat te wensen over

De Inspectie OOV constateerde bij haar onderzoek naar de samenwerkingsafspraken in 2008 een aantal technische gebreken die de landelijke deling van opsporingsgegevens verhinderden. Daarnaast achtte de Inspectie een organisatorische oorzaak waarschijnlijk voor de geconstateerde onvolledigheid van de gedeelde opsporingsgegevens.²³ Deze laatste conclusie vormt zoals vermeld de directe aanleiding voor dit onderzoek, waarvoor door de Inspectie OOV opdracht is gegeven. Het onderscheid tussen technische en organisatorische knelpunten wordt later toegelicht.

1.2.1 De Inspectie over BlueView

De Inspectie weerlegde met haar onderzoek een uitspraak van het Korpsbeheerdersberaad (KBB) betreffende BlueView. Het KBB rapporteerde in april 2008 dat “met deze nieuwe versie zowel handhaving- als opsporingsgegevens uit de afgelopen vijf jaar met één zoekvraag bevroegd kunnen worden. Hiermee is de bulk van de politie-informatie landelijk deelbaar gemaakt.”²⁴ Ten tijde van het onderzoek door de Inspectie OOV naar de Samenwerkingsafspraken in 2008, was in vijf van de zes verzorgingsgebieden (VG's) de koppeling tussen BVO en BlueView niet operationeel, waardoor het leeuwendeel van de informatie in BVO niet landelijk werd gedeeld. De Inspectie verwachtte dat dit probleem voor het einde van 2008 zou zijn opgelost.²⁵ De Inspectie stelde verder dat BlueView wel gegevens bevatte uit *alle systemen* waarvan dit was afgesproken, maar niet *alle relevante gegevens* uit die systemen.²⁶

Behalve BVO dienen onder meer opsporingssystemen het Recherche Basissysteem (RBS) en Octopus te worden ontsloten in BlueView. De laatste twee zijn voorgangers van BVO en worden uitgefaseerd. Uit de gebruikersstatistieken en uit de interviews kwam het beeld naar voren dat niet alle opsporingsinformatie via BlueView raadpleegbaar was die op basis van het *Beleid Uitwisseling Opsporingsinformatie* beschikbaar had moeten zijn. Korpsen konden onderzoeken op een hoger autorisatieniveau wegzetten dan was afgesproken, waardoor ze niet werden gedeeld via BlueView.²⁷ De Inspectie oordeelde dat medewerkers in alle korpsen in meer of mindere mate

²³ *Idem*, p. 9

²⁴ *Voortgangsrapportage april 2008*, Kamerstukken II, vergaderjaar 2007-2008, 30880, nr. 8

²⁵ Inspectie OOV (2008), p. 28

²⁶ *Ibidem*

²⁷ *Idem*, p. 51

terughoudend waren in het beschikbaar stellen van opsporingsinformatie aan elkaar. Er werden ten tijde van het onderzoek door de Inspectie nog geen maatregelen getroffen om de gebleken terughoudendheid in het beschikbaar stellen van informatie aan te pakken.²⁸

1.2.2 De Inspectie over BVO

De Inspectie stelde in haar rapport dat korpsen hun eigen afweging maken betreffende het delen van informatie. Korpsen kunnen beslissen om zaken wel of niet in BVO te verwerken dan wel met een extra zware rubricering af te schermen van zicht daarop buiten de Criminele Inlichtingen Eenheid (CIE). Met name zware criminaliteitszaken wilden de eenheden, volgens de Inspectie, niet zonder meer in BVO zichtbaar hebben (zodat die ook buiten het landelijke zicht van BlueView konden blijven).

De Inspectie constateerde ook dat zaken die eigenlijk wel in BVO thuishoren, bewust 'kleiner gemaakt' werden.²⁹ Zaken die minder dan 40 uur onderzoek vergen hoeven niet in BVO ingevoerd te worden, met als gevolg dat deze niet landelijk worden gedeeld in BlueView.

Vastgesteld werd dat de werkwijze voor BVO nog niet op alle onderdelen volledig was beschreven. Voor de onderdelen waarbij wel een beschrijving voorhanden was, conformeerden niet alle medewerkers in de korpsen zich hieraan. Op die manier werden niet alle relevante gegevens ingevoerd, die wel in BVO thuis horen. Uit het onderzoek bleek dat in vijftien korpsen gegevensopslag plaatsvond in andere systemen dan BVO, zoals Excel en MS-Word.³⁰ Gegevens werden ook wel alleen in het handhavingregistratiesysteem (bijv. BVH) geregistreerd, met onder meer gevolgen voor de beveiliging en de volledigheid van de informatie.³¹

1.2.3 Technische knelpunten in het gebruik van BVO

Er bestaat geen koppeling tussen BVH en BVO, waardoor recherchemedewerkers in districten genoodzaakt zijn in veel gevallen een dubbele invoer te verrichten. Als gevolg van tijdgebrek werden volgens de Inspectie, om die reden de criteria voor het gebruik van BVO opgerekt.³² De Inspectie noemde verder de grote

²⁸ *Ibidem*

²⁹ Inspectie OOV (2008), p. 22

³⁰ *Idem*, pp. 22-23

³¹ *Idem*, p. 53

³² *Ibidem*

hoeveelheid mutatiesoorten in BVO als knelpunt in het gebruik van dit systeem.³³

BVO ondersteunde aanvankelijk de vastlegging van zogeheten bruto CIE-verslagen niet. Ruwe gegevens, die bijvoorbeeld nog de volledige namen van verdachten en onderzochte personen bevatten, konden niet worden ingevoerd. In 2008 werd daarover landelijk besloten dat bruto (ruwe) informatie in een extra beveiligde 'rode' omgeving ingevoerd moest gaan worden.³⁴

Uit de interviews die de Inspectie in de korpsen heeft gehouden, blijkt dat politiemensen nog meer motieven voor het beperkte gebruik van BVO naar voren hebben gebracht. Politiemensen beklagden zich onder meer over het feit dat bestaande functionaliteiten vanuit oude systemen niet meegenomen konden worden naar BVO. Het invoeren van gegevens kost meer tijd dan voorheen in bijvoorbeeld RBS en de gebruiksvriendelijkheid is afgenomen, stellen de gebruikers. Waar men bijvoorbeeld gewend was om grafische bestanden bij rapporten op te slaan, bestaat deze mogelijkheid niet meer in BVO. Verder moest door instabiliteit van het systeem aan het begin, regelmatig met medewerking van een systeembeheerder informatie hersteld worden.

Deze problemen hebben samen bijgedragen aan het beperkte gebruik van BVO, met als belangrijkste gevolg een beperkte invoer van opsporingsinformatie in het systeem. Tot op heden konden deze wensen van politiemedewerkers met betrekking tot extra functionaliteiten en gebruiksvriendelijkheid, maar zeer ten dele tegemoet worden gekomen bij nieuwe versies van BVO.

1.2.4 Organisatorische knelpunten in het gebruik

Een organisatorisch knelpunt voor het gebruik van BVO dat de Inspectie noemde, was de beperkte toepassing van gestandaardiseerde werkprocessen. Medewerkers in korpsen lopen daardoor kans producten op te leveren die niet geschikt zijn voor BVO. De Inspectie heeft vastgesteld dat het werkproces Algemeen Rechercheren bij zeventien korpsen niet of niet volledig was gestandaardiseerd in 2008. Ondanks dat dit proces landelijk is voorgeschreven, bleven deze politiekorpsen toch de volgens hen meest werkbare werkmethoden toepassen. Deze zijn vaak afgestemd op eigen structuur en werkwijze en kunnen daarmee afwijken van de landelijke gestandaardiseerde opsporingsprocessen. De uniformiteit van de landelijke werkwijze kwam daarmee in het gedrang.³⁵

³³ *Idem*, p. 52

³⁴ *Idem*, p. 50

³⁵ *Idem*, p. 22

1.2.5 Opsporingsinformatie niet willen delen

Behalve bovenstaande knelpunten, werd in de interviews die de Inspectie heeft gehouden, ook het recherchetactische motief door politiemensen genoemd voor het niet willen delen van opsporingsinformatie. Dit verschijnsel en de door de Inspectie gesignaleerde neiging van korpsen, hun eigen werkwijzen te blijven hanteren – kunnen niet met technische aanpassingen van informatiesystemen worden ondervangen. Om aan deze problemen het hoofd te bieden, moet aandacht worden gegeven aan de werkprocessen en organisatiecultuur van korpsen.

Korpsen zijn voorzichtig maar ook terughoudend met het uitwisselen van informatie die is ingewonnen bij informanten. Het risico bestaat dat de verdachte ontdekt wie de informant was als hij met de informatie wordt geconfronteerd. Als dat gebeurt, is er mogelijk sprake van groot gevaar voor de informant en tevens voor de continuïteit van het onderzoek.³⁶ Deze risico's moeten soms zoveel mogelijk worden uitgesloten door het team dat de informant runt, waardoor ingewonnen informatie dan niet kan worden gedeeld. Deze verklaring voor de terughoudendheid van korpsen om opsporingsinformatie c.q. informanteninformatie te delen met andere korpsen, is algemeen bekend. Verdere verklaringen voor beperkingen in de informatiedeling tussen politiekorpsen, nadat informatiesystemen zijn ontwikkeld en toegepast, zijn voor de Nederlandse situatie niet eerder wetenschappelijk beschreven.

³⁶ *Idem*, pp. 135-137

1.3 Probleemstelling en onderzoeksvragen

Het doel van dit onderzoek is tweeledig, namelijk enerzijds het nader beschrijven van de door de Inspectie OOV geconstateerde beperkingen in de informatie-uitwisseling tussen politiekorpsen. Anderzijds wil het onderzoek voor deze beperkingen verklaringen vinden. Deze tweeledige doelstelling leidt tot de volgende centrale vraagstelling:

In hoeverre en onder welke omstandigheden wordt opsporingsinformatie niet (optimaal) uitgewisseld tussen Nederlandse politiekorpsen?

Aan de hand van onderstaande deelvragen zal deze probleemstelling in dit rapport van een antwoord worden voorzien:

1. Wat is het beleid binnen de Nederlandse politie ten aanzien van de uitwisseling van opsporingsinformatie tussen korpsen?

Om een inschatting te kunnen maken van de mate waarin de informatiedeling beperkt is, dient met deze eerste deelvraag helder te worden gemaakt wat de politie hierover landelijk heeft afgesproken. Met deze deelvraag worden deze landelijke afspraken in kaart gebracht.

2. Welke kenmerken heeft opsporingsinformatie die niet (optimaal) wordt gedeeld en door welke actoren wordt informatie niet (optimaal) gedeeld?

Met deze deelvraag wordt in beeld gebracht welke kenmerken informatie heeft, die niet volledig of niet met alle korpsen wordt gedeeld. Op die manier kunnen de factoren die van invloed zijn op het probleem uit de centrale vraagstelling, uiteindelijk in hun context worden weergegeven. De bedoeling is daarbij het verklaringspad te volgen van bepaalde kenmerken van informatie en factoren die bij de betreffende kenmerken een rol spelen, naar de beslissing die er wordt gemaakt over het al of niet delen van deze informatie. In deze deelvraag ligt ook de gedachte besloten dat informatie die door korpsen niet in de geëigende systemen wordt aangeboden, wellicht wel via andere kanalen wordt gedeeld.

3. In hoeverre beperken wettelijke regels de uitwisseling van opsporingsinformatie tussen Nederlandse politiekorpsen?

Zoals in de volgende paragraaf zal worden besproken, bestaat er wettelijke regelgeving voor de opsporingspraktijk. Juridische knelpunten betreffende het delen van informatie worden met deze deelvraag beschreven.

4. In hoeverre beperkt technologie de uitwisseling van opsporingsinformatie tussen Nederlandse politiekorpsen?

Om tot deling van informatie over te kunnen gaan, hebben politiekorpsen te maken met geautomatiseerde informatiesystemen. In het verleden ging het dan om onder meer RBS en Octopus, tegenwoordig worden BVO en BlueView gebruikt om opsporingsinformatie uit te wisselen. Bij deze deelvraag wordt beschreven in hoeverre de geautomatiseerde systemen voor politiemensen een barrière vormen om informatie te delen.

5. In hoeverre beperken organisatorische omstandigheden de uitwisseling van opsporingsinformatie tussen Nederlandse politiekorpsen?

Specifieke organisatorische kenmerken van de politie zijn van invloed bij het sturen van de organisatie en in het bijzonder bij het doorvoeren van vernieuwing. Het probleem van beperkte informatiedeling bij de politie, wordt bij deelvraag 5 aan de hand van deze kenmerken bestudeerd.

1.4 Korte samenvatting van het verklaringsschema

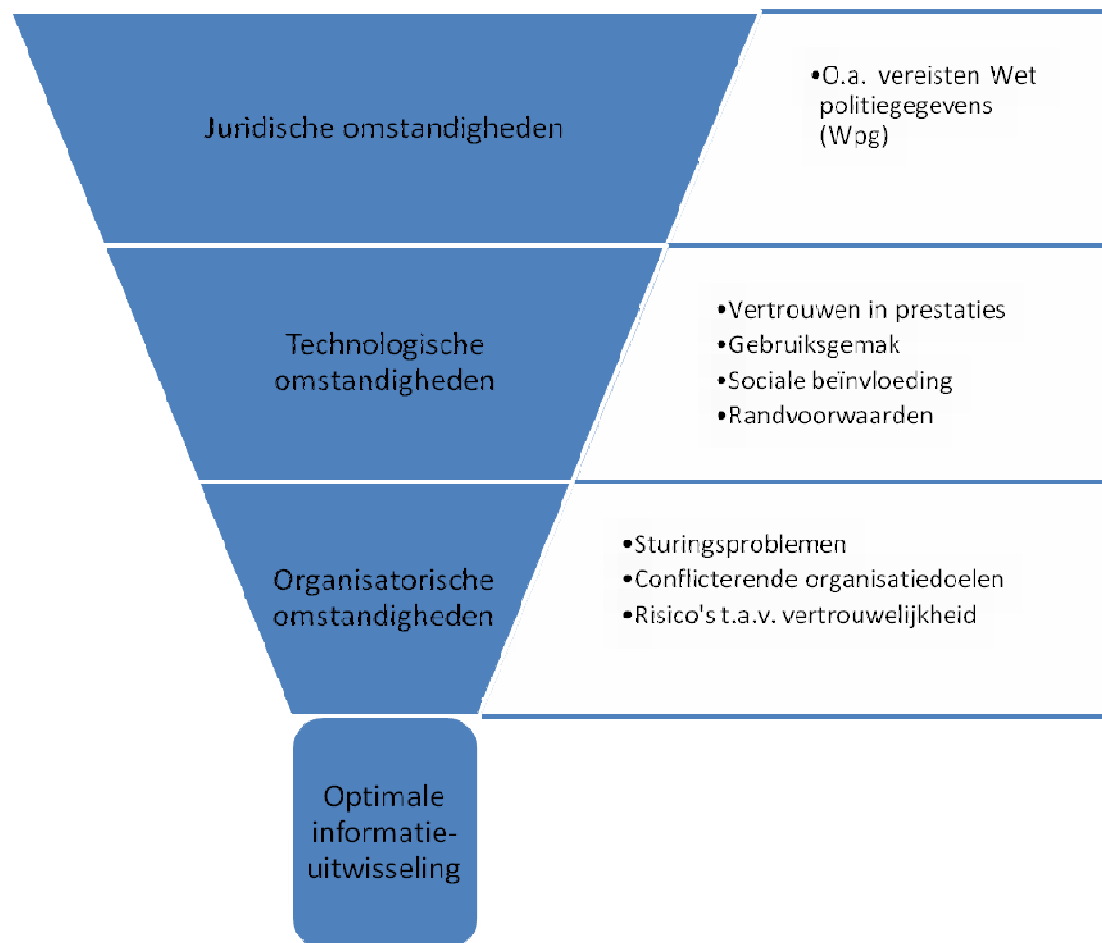
In deze studie ligt de focus op de beperkingen in de informatie-uitwisseling tussen Nederlandse politiekorpsen. Het verklaringsschema in dit onderzoek, onderwerp van het volgende hoofdstuk, gaat ervan uit dat een optimale informatie-uitwisseling van opeenvolgende factoren afhankelijk is, zoals in onderstaand schema is weergegeven.

In dit model wordt verondersteld dat een optimale informatie-uitwisseling ten eerste afhankelijk is van juridische omstandigheden. Behalve de noodzakelijke wettelijke bepalingen om informatie-uitwisseling überhaupt mogelijk te maken, worden met omstandigheden ook andere juridische facetten van het opsporingsproces bedoeld die negatief van invloed kunnen zijn op informatie-uitwisseling.

Vervolgens beïnvloeden in dit model, technologische omstandigheden de mogelijkheden voor een optimale informatie-uitwisseling. Hierbij gaat het niet om de noodzakelijke techniek *sec*, maar veel meer om de kwaliteit van de techniek en de acceptatie ervan door de uitvoerende organisatie.

Als laatste worden in het gekozen verklaringsschema organisatorische omstandigheden van invloed geacht op de informatie-uitwisseling bij de politie. Hiermee wordt enerzijds de aard van de organisatie bedoeld in organisatiesociologische termen. Anderzijds wordt ook de aard van het politiewerk, het opsporingswerk in het bijzonder, van invloed geacht op de mogelijkheden om informatiedeling te optimaliseren. Deze laatste invalshoek is meer een politiewetenschappelijke.

Het aldus ontstane verklaringsschema kan als een trechter worden voorgesteld, zoals in onderstaand schema. In de rest van deze studie worden de verschillende elementen uit dit model onderbouwd dan wel weerlegd. Dit model komt zoals aangegeven, in het volgende hoofdstuk uitgebreider aan de orde. Theoretische achtergronden van het model worden later ook in de diverse hoofdstukken aan de orde gesteld. In de volgende paragrafen wordt de opzet van dit onderzoek uiteengezet.



1.5 Onderzoeksafbakening

In de opsporingspraktijk zijn veel verschillende actoren actief, maar het is niet mogelijk om in dit onderzoek uitspraken te doen over hoe met informatiedeling wordt omgegaan in de volle breedte van het werkveld. Daarom dient verduidelijkt te worden waarop en op welke tijdsperiode dit onderzoek betrekking heeft.

1.5.1 Actoren

Behalve de politieregio's hebben bovenregionale, nationale en supranationale rechercheorganisaties een relatie met Nederlandse opsporingsinformatie. Daarnaast speelt het gezag van het Openbaar Ministerie een belangrijke rol. In dit onderzoek worden echter uitsluitend de regionale politiekorpsen onderzocht. Externe relaties van de politiekorpsen zullen aan bod komen maar zullen vooral vanuit het perspectief van die korpsen worden behandeld. Daarmee wordt aangesloten op het rapport van de Inspectie OOV, waarin werd gemeld dat politiekorpsen zelfstandig besluiten tot het niet delen van informatie via de geëigende systemen.

Bij de ontwikkeling en implementatie van de ICT-basisvoorzieningen zijn de korpsen afhankelijk van verschillende landelijke organisaties, waaronder de vtsPN. De ontwikkelings- en implementatiefase van BVO behoren echter niet tot het bereik van dit onderzoek, omdat het zich beperkt tot de actuele situatie. In de actuele situatie is ook de rol van de zes Verzorgingsgebieden (VG's) uitsluitend een technische: zij verrichten het beheer van een aantal systemen maar hebben geen invloed op beslissingen over het wel of niet delen van informatie en zijn daarom evenmin van direct belang voor dit onderzoek.³⁷

1.5.2 Context

In paragraaf 1.1 werd vermeld dat de relatie die regionale politiekorpsen hebben met het Rijk niet eenduidig is. Als het gaat om informatiedeling is de context voor de korpsen een specifieke. Daarop zal uitgebreid worden ingegaan, bijvoorbeeld door te kijken naar de relaties met het Openbaar Ministerie en met het ministerie van BZK. In dit onderzoek zullen deze relaties van de politiekorpsen zoals vermeld vooral vanuit hun perspectief worden behandeld. De in- en externe relaties en belangen van relevante beslissers binnen politiekorpsen zullen

³⁷ Zie voor een beschouwing van de technische aspecten: Inspectie IOOV (2008) en het vervolgonderzoek over de samenwerkingsafspraken van de IOOV, dat in juli 2010 is gepubliceerd.

daarbij centraal staan. Het gaat dan steeds om de vraag welke factoren in deze relaties van invloed zijn op de beslissing om opsporingsinformatie al dan niet met andere korpsen te delen.

1.6 Operationalisatie van te onderzoeken factoren

Het operationaliseren of het definiëren van de factoren die worden onderzocht is nodig om duidelijkheid te geven over wat beoogd wordt te onderzoeken en naar welke verbanden wordt gezocht.

Bij de analyse van de factoren die op het delen van opsporingsinformatie van invloed zijn, wordt gefocust op beslissingen op drie verschillende niveaus in de korpsen: strategisch, tactisch en operationeel niveau. Deze niveaus komen bij het onderzoeksontwerp nader aan de orde. Het gaat hier om beslissingen waarmee onder meer wordt gereageerd op de volgende kwesties:

Welke functionarissen moeten opsporingsinformatie invoeren? Welke informatie moet worden ingevoerd, welke niet en welke informatie wordt alleen na goedkeuring ingevoerd? Welke functionarissen kunnen deze goedkeuring geven? Onder welke autorisatieniveaus moet informatie worden ingevoerd? Welke functionarissen hebben de bevoegdheid om autorisatieniveaus aan informatie te geven, en/of de status van een onderzoek te bepalen met gevolg voor het invoeren of het autorisatieniveau van de betrokken informatie?

Beslissingen die op korpsniveau en in de dagelijkse uitvoering worden genomen, met betrekking tot het delen van opsporingsinformatie, worden in kaart gebracht onder deelvraag I.

De mate waarin juridische, technologische en organisatorische omstandigheden uit deelvragen III t/m V op de eerder genoemde beslisniveaus van invloed zijn, is verschillend. Zo heeft het uitvoerende niveau veel meer te maken met de gebruikaspecten van de geautomatiseerde systemen dan de tactische en strategische niveaus. Daarnaast is het instellen van een totaal korps op (vernieuwde) juridische kaders en landelijk beleid een verantwoordelijkheid die in de eerste plaats ligt op strategisch niveau. De sturing op uitvoeringsafspraken ligt vervolgens met name bij functionarissen op tactisch niveau. Risico's t.a.v. vertrouwelijkheid worden met name op operationeel en op tactisch niveau gevoeld. Deze aannames hebben consequenties voor de manier waarop (medewerkers van) de diverse beslisniveaus zullen worden geïnterviewd. Deze verschillen worden behandeld bij het onderzoeksontwerp.

1.7 Onderzoeksontwerp

Zoals eerder vermeld, wil dit onderzoek enerzijds de beperkingen in de informatie-uitwisseling tussen Nederlandse politiekorpsen. Anderzijds wil het onderzoek de factoren beschrijven die korpsen ertoe brengen opsporingsinformatie niet met andere korpsen te delen. Om deze doelstellingen te bereiken, is ervoor gekozen om kwalitatief onderzoek uit te voeren dat zowel beschrijvend als verklarend van aard is. In het beschrijvende gedeelte gaat het erom een minutieuze weergave van gebeurtenissen en hun samenhangen weer te geven. In het verklarende gedeelte worden mogelijke oorzaken onderzocht.³⁸

1.7.1 Bronnen

Er worden in dit onderzoek diverse informatiebronnen gebruikt, te weten wetenschappelijke literatuur, parlementaire stukken, interne beleidsdocumenten en interviews met politiemensen. Met het gebruik van meerdere bronnen, wordt een zo betrouwbaar mogelijk onderzoeksresultaat beoogd.³⁹

De wettelijke toezichthouder op naleving van de Wet politiegegevens (Wpg) is het College Bescherming Persoonsgegevens (CBP). Diverse publicaties van het CBP geven naast het onderzoek van de Inspectie OOV een goed beeld van de knelpunten in de informatiehuishouding bij de politie. Interne beleidsdocumenten laten zien op welke wijze de inrichting van informatiebeheer en informatie-uitwisseling bedoeld zijn.

Verder staat het open- of diepte-interview centraal staan bij het verzamelen van de gegevens voor dit onderzoek. Deze techniek kenmerkt zich door geen of een beperkte structuur aangaande de inhoud, formulering en volgorde van de vragen evenals de antwoordkeuze. De vragen worden binnen een referentiekader gesteld en tijdens het interview veelal bijgesteld waardoor de interviewer vrij is om (eventueel) door te vragen en andere relevante vragen te stellen zodat een zo nauwkeurig mogelijk beeld verkregen wordt van het betreffende onderwerp.⁴⁰ Interviews en bronnenonderzoek worden naast elkaar verricht en zijn bedoeld elkaar te versterken.

Zoals in de volgende subsectie nader zal worden toegelicht, worden binnen de onderzochte korpsen gegevens zo breed mogelijk verzameld. Politied medewerkers uit vijf zeer diverse korpsen vertellen openhartig over uiteenlopende kwesties die een rol spelen bij het invoeren en delen van

³⁸ Geurts, P. (1999), *Van probleem naar onderzoek*, Bussum, p. 29

³⁹ Hutjes, J.M., Buuren, J.A. van (1992), *De gevalstudie: strategie van kwalitatief onderzoek*, Meppel

⁴⁰ Zie voor een uitvoerige beschrijving onder andere Babbie, E. (2004), *The practice of social research*

opsporingsinformatie. Vanuit de verschillende visies van eindverantwoordelijke, direct leidinggevende en uitvoerende medewerkers kan aan de hand van diepte-interviews een divers beeld van de omstandigheden voor informatie-uitwisseling tussen korpsen worden opgebouwd. Daarbij worden binnen de korpsen zowel districts-, als regiorecherche onderzocht alsmede de Criminele Inlichtingeneenheid (CIE).

1.7.2 Selectie en methodologische kanttekening

Omdat dit onderzoek in een relatief kort tijdsbestek uitgevoerd dient te worden is het niet mogelijk om in alle korpsen en op alle niveaus in de politieorganisatie diepgaand te onderzoeken hoe over informatiedeling wordt gedacht en hoe wordt gehandeld op dit terrein. De focus binnen de korpsen, ligt op de recherche en Criminele Inlichtingeneenheden. Er is een selectie van de 26 politiekorpsen gemaakt. Daarbij is gekeken naar de grootte van de politiekorpsen en naar de verdeling van de voormalige ICT-systemen die door de recherches zijn gebruikt. Zodoende zijn vijf politiekorpsen gekozen, te weten *IJsselland, Brabant-Noord, Hollands Midden, Amsterdam-Amstelland en het KLPD*.

De selectie van de onderzochte korpsen is als volgt gemotiveerd. Selectie op korpsgrootte is van belang voor een volledig beeld. Een kleiner korps is wellicht makkelijker te leiden. Daarnaast houdt de korpsgrootte redelijk verband met het aantal en de grootte van de rechercheonderzoeken, wat ook factor van belang zou kunnen zijn. Het tweede selectie criterium dat is gebruikt, het voormalige informatiesysteem voor de recherchefunctie, zou een factor kunnen zijn die van invloed is op de overgang naar het nieuwe BVO. Juist omdat de nieuwe Basisvoorziening Opsporing (BVO) vooral op één van de voormalige systemen is gebaseerd. Daarnaast hebben ook praktische redenen de selectie van de te onderzoeken korpsen mede bepaald. Voor dit onderzoek werd aangesloten bij de korpsbezoeken die de Inspectie OOV ambtshalve verricht. Vijf korpsen zijn onderzocht, waarbij in ieder korps twee tot drie medewerkers zijn geïnterviewd.

Gekozen wordt beslissingen betreffende het delen van opsporingsinformatie op drie niveaus in de organisatie van de korpsen te bestuderen. Deze werkwijze wordt onderstaand beschreven en verantwoord.

- **Strategisch niveau:**

Beslissingen t.a.v. informatiedeling en de sturing hierop op korpsniveau kunnen door de verantwoordelijke voor het opsporingsproces uitvoerig worden

toegelicht. Binnen het politiekorps is dat de directeur opsporing. Deze kan tevens aangeven op welke manier de omgeving van invloed is op zijn korps.

- Tactisch niveau:

De teamleiders vervullen een centrale rol bij de uitvoering van het opsporingswerk. Met hen kan in kaart worden gebracht hoe beslissingen over het wel of niet delen van informatie, over de status van rechercheonderzoeken (met gevolg voor het invoeren of het autorisatieniveau van de betrokken informatie) en over het geven van autorisatieniveaus aan informatie tot stand komen. De teamleider heeft enerzijds met de werkvloer en anderzijds met beleid van bovenaf te maken. Daarnaast zal hij of zij een redelijke kennis hebben van wettelijke regelgeving, beleid en beslissingen over informatiedeling op zowel team-, als op korpsniveau. Hierbij kan aandacht worden gegeven aan zowel beslissingen die tot uiting komen via de formele commandostructuur als aan beslissingen die op operationeel niveau worden gemaakt.

- Operationeel niveau:

Ook op het operationele niveau (bijv. rechercheurs) wordt invloed uitgeoefend op het delen van opsporingsinformatie, met name waar het om de invoer van informatie in BVO. Daarmee hebben met name functionarissen op operationeel niveau te maken. In kaart gebracht moet worden hoe groot de beslissingsruimte is op dit niveau, gelet op beleidsregels enerzijds en de sturing door leidinggevenden anderzijds.

In ieder van de eerder genoemde politiekorpsen is gesproken met recherchefunctionarissen op operationeel en tactisch niveau (uitgezonderd Brabant-Noord) en op strategisch niveau met de directeur opsporing (uitgezonderd Amsterdam-Amstelland). Alleen indien relevant, wordt het onderscheid tussen de niveaus in deze rapportage aangeduid. In twee korpsen zijn medewerkers van de Criminele Inlichtingen Eenheid (CIE) geïnterviewd. In totaal werden 13 interviews gehouden met rechercheurs, groeps- en teamchefs van zowel recherche- als CIE teams en met drie directeuren opsporing. In de rapportage worden hun namen en de korpsen niet genoemd. Dat is voor het doel van dit onderzoek niet nodig en wanneer geïnterviewden worden geanonimiseerd vergroot dat de kans op openhartige antwoorden.

Op deze plek past een methodologische kanttekening over de selectie van de informanten binnen de korpsen. Deze zijn, binnen de gevraagde functies, door de geselecteerde politiekorpsen zelf aangewezen. Daardoor bestaat de mogelijkheid dat politiekorpsen hebben geselecteerd op bijvoorbeeld houding ten aanzien van

informatiedeling of kennis van de betrokken informatiesystemen. In sommige gevallen bleken de rechercheurs, naast hun reguliere functie inderdaad kerninstructeur of kwaliteitsmedewerker te zijn. Zij hadden waarschijnlijk een kennisvoorsprong op de meeste van hun collega's. Bij het trekken van conclusies over de onderzoeksresultaten dient hiermee rekening te worden gehouden.

1.7.3 Onderzoeksstrategie per deelvraag

In onderstaande wordt per deelvraag beschreven welke onderzoeksstrategie gehanteerd wordt om tot beantwoording van de betreffende vraag te komen:

1. Wat is het beleid binnen de Nederlandse politie informatie-uitwisseling ten aanzien van de uitwisseling van opsporingsinformatie tussen korpsen?

Aan de hand van interne beleidsdocumenten van de politie, wordt het beleid ten aanzien van de uitwisseling van opsporingsinformatie in kaart gebracht.

2. Welke kenmerken heeft opsporingsinformatie die niet (optimaal) wordt gedeeld en door welke actoren wordt informatie niet (optimaal) gedeeld?

Aan de hand van interviews met politiemensen, zal deze deelvraag van een antwoord worden voorzien. In deze inleiding werd vooruit gelopen op de beantwoording van deze deelvraag. Daarbij werd wetenschappelijk onderzoek en onderzoek van de Inspectie OOV aangehaald. Gekozen wordt, zoals eerder aangegeven, functionarissen op het laagst leidinggevende niveau binnen de recherche en CIE teams aan diepte-interviews te onderwerpen. Dat zijn de team- en groepschefs. Gekozen wordt verder deze deelvraag toe te spitsen op BVO. Hierin moeten alle zaken worden bijgehouden die langer duren dan 40 uur. Alleen de allerkleinste zaken vallen hier dus buiten. Hierop wordt niet ingegaan. Op het delen van opsporingsinformatie is indirect van invloed de mate waarin informatie in BVO wordt ingevoerd. Ook hierop wordt ingegaan binnen het verband van deze deelvraag.

3. In hoeverre beperken wettelijke regels de uitwisseling van opsporingsinformatie tussen Nederlandse politiekorpsen?

In het kader van deze deelvraag is ten eerste van belang in kaart te brengen hoe wettelijke regelgeving van invloed is op informatiedeling. Zoals eerder vermeld zijn de Wpg en het Besluit politiegegevens (Bpg) van toepassing op de informatiedeling binnen de politie (en die met derde partijen). Daarnaast is op de verwerking van gegevens die door de CIE worden verzameld bij informanten, de

zogenoemde ZwaCris-gegevens, de CIE-Regeling van toepassing.⁴¹ In welke opzichten werkt wetgeving stimulerend en in welke opzichten belemmerend voor deling van opsporingsinformatie? Door bestudering van wetteksten, secundaire bronnen en het stellen van interviewvragen op alle drie genoemde niveaus wordt antwoord gegeven op deze vraag. Bij de interviews is de vraag hoe in de organisatie met wettelijke regelgeving wordt omgegaan en of langs die weg belemmeringen ontstaan voor de informatie-uitwisseling. Verder wordt gekeken of afwijkingen van wettelijke voorschriften zoals die werden geconstateerd door het College Bescherming Persoonsgegevens (CBP), belemmeringen voor de informatie-uitwisselingen hebben opgeleverd.

4. In hoeverre beperkt technologie de uitwisseling van opsporingsinformatie tussen Nederlandse politiekorpsen?

Om tot deling van opsporingsinformatie over te kunnen gaan, hebben politiekorpsen in veel gevallen te maken met BVO. Een geautomatiseerd informatiesysteem waarin gegevens ingevoerd moeten worden. Behalve een technisch hulpmiddel, voor sommige gebruikers wellicht een barrière. Door het stellen van interviewvragen aan medewerkers op operationeel niveau wordt gekeken in hoeverre de techniek barrières opwerpt voor het landelijk delen van opsporingsinformatie. Dit gebeurt aan de hand van een specifiek theoretisch model dat in het volgende hoofdstuk aan de orde komt.

5. In hoeverre beperken organisatorische omstandigheden de uitwisseling van opsporingsinformatie tussen Nederlandse politiekorpsen?

Specifieke organisatorische kenmerken van de politieorganisatie, alsmede de aard van het opsporingswerk worden in dit onderzoek als invalshoek genomen voor het probleem van de beperkte informatie-uitwisseling. Ter beantwoording van deze deelvraag worden interviews gehouden met functionarissen op zowel tactisch als strategisch niveau. Geanalyseerd wordt in hoeverre de gekozen theoretische inzichten die worden uitgewerkt in het volgende hoofdstuk, van toepassing zijn. Daarbij wordt met de directeurs opsporing in het bijzonder ingegaan op specifieke sturingskenmerken van de politie. De aard van het politiewerk is een gesprekstema dat met name bij de team- en groepsleiders aan de orde wordt gesteld. In hoeverre bijvoorbeeld, bestaat behoefte aan

⁴¹ Staatscourant, 12 oktober 2000, nr. 198

afgescheiden trajecten met het oog op de betrouwbaarheid van de betrokken ICT-basisvoorzieningen.

1.8 Relevantie van het onderzoek

In onderstaande worden de maatschappelijke en wetenschappelijke relevantie van dit onderzoek aangegeven.

1.8.1 Maatschappelijke relevantie

Het ligt voor de hand dat de samenleving rekent op een effectieve uitvoering van de politietaak. Voor de politie zelf kreeg deze opdracht vanaf de jaren '90 een nieuwe dimensie. Langzaam laaide de discussie over de maatschappelijke betekenis van de politie op. Onvrede over toegenomen onveiligheid leidde tot een roep in de samenleving om een daadkrachtiger aanpak van criminaliteit. Individualisering, 'ontgrenzing' en meer complexe vormen van criminaliteit vragen steeds meer om een informatiegedreven strategie. Zoals aangegeven kan met de moderne middelen van vandaag de dag een goed werkende informatiehuishouding, die tevens goed in het functioneren van de organisatie is ingebed, voor een toename van de effectiviteit veel betekenen. In dit onderzoek wordt getracht verklaringen te vinden voor een probleem dat een vitaal onderdeel van de informatiehuishouding binnen de politie betreft, namelijk de beperkte deling van opsporingsgegevens tussen politiekorpsen. In de eerste plaats draagt dit onderzoek bij tot een beter begrip van dit probleem; in de tweede plaats kan het daardoor wellicht bijdragen aan een verdere oplossing ervan.

1.8.2 Wetenschappelijke relevantie

Er bestaat veel ICT literatuur over de acceptatie van informatiesystemen in organisaties. Ook is wel gepubliceerd over de implementatie van informatiesystemen bij de politie. Daarnaast zijn er vele publicaties verschenen over het belang van informatie voor het uitvoeren van de politietaak. Ook is wel bekend onder welke omstandigheden informatiesystemen binnen de strafrechtketen worden ontwikkeld en toegepast. Met onderzoek op de snijvlakken van deze onderzoeksgebieden, waar het onder meer gaat over de rol van nieuwe of extra informatie (uit informatiesystemen) binnen het politiewerk, is sinds enkele jaren een begin gemaakt. Relatief nieuw is de vraag waardoor beperkingen in de informatie-uitwisseling ontstaan, nadat de systemen eenmaal ontwikkeld en toegepast zijn. In dit onderzoek wordt bijzondere aandacht gegeven aan de bereidheid van de in Nederland vrij zelfstandig opererende korpsen enerzijds en individuele politiemedewerkers anderzijds, om met de genoemde systemen te werken en informatie te delen. Dergelijk onderzoek is (in

Nederland) niet eerder uitgevoerd maar biedt mogelijk een belangrijke invalshoek om het traag verlopende transitieproces naar meer informatie gestuurde politie, beter te begrijpen.

1.9 Verdere indeling van het rapport

In het volgende hoofdstuk wordt aangegeven van welke theoretische inzichten wordt onderzocht of ze een verklaring kunnen bieden voor de beperkte uitwisseling van opsporingsinformatie tussen Nederlandse politiekorpsen. Deze hebben betrekking op deelvragen III t/m V: op het verklarende deel van de doelstelling.

Dit verklaringsschema wordt vanaf hoofdstuk 5 met behulp van de resultaten van de interviews onderbouwd of weerlegd. Ieder hoofdstuk begint met een uitgebreide introductie van de theoretische achtergronden, daarop volgen de resultaten van de interviews en tussenconclusies. Voorafgaand worden resp. in hoofdstuk 3 en 4, deelvragen I en II van een antwoord voorzien. Deze hebben betrekking op het beschrijvende deel dit onderzoek. In hoofdstuk 3 worden interne politie afspraken behandeld. Deze afspraken dienen als achtergrond voor de beschrijving van de barrières in de informatiedeling in hoofdstuk 4.

De onderzoeksresultaten en tussenconclusies betreffende deelvragen III en IV worden resp. gegeven in hoofdstukken 5 en 6. De behandeling van deelvraag V gebeurt aan de hand van twee onderscheiden thema's in hoofdstukken 7 en 8.

2. Informatiedeling is afhankelijk van diverse fronten

Met de ontwikkeling van de basisvoorzieningen de laatste jaren is de aandacht sterk op de techniek komen te liggen maar dat is niet helemaal terecht. Ook de organisatorische context is naast de juridische context van invloed op de ontwikkeling en toepassing van die systemen.

In dit hoofdstuk wordt het theoretisch kader voor deze studie geïntroduceerd. In paragraaf 2.2 wordt het verklaringsschema dat wordt gebruikt in deze studie, nader gemotiveerd en toegelicht. In paragraaf 1.4 van de inleiding werd het al kort aangestipt. Om te beginnen wordt in paragraaf 2.1 het probleem van beperkte informatiedeling bij de politie binnen een algemener kader beschouwd. De problematiek blijkt niet alleen binnen de politie te spelen.

2.1 Informatiedeling: een kwestie van verschillende belangen

Algemeen kan een aantal zaken worden gezegd over de uitwisseling van informatie tussen organisatieonderdelen, die kunnen worden toegepast op het probleem van beperkte informatiedeling bij de Nederlandse politie. Bij deze beschrijving wordt gebruik gemaakt van de begrippen centraal en decentraal. Dit onderscheid wordt gewoonlijk niet toegepast op de politie, omdat het gezag over de politie lokaal is verankerd.¹ Echter bij het probleem van de informatie-uitwisseling blijkt dat om deze reden respectievelijk het Rijk en de korpsen als centrale en lokale instituties kunnen worden beschouwd, aangezien het ministerie van BZK als centrale institutie hierover afspraken heeft gemaakt met de korpsen.

De kenmerkende rol van de centrale institutie (het moederbedrijf, het Rijk) is in dit verband dat zij toeziet op een optimale deling van informatie, vanwege het belang hiervan voor de totale organisatie. Als door het afschermen van informatie door organisatieonderdelen de effectiviteit van de gehele organisatie in het gedrang komt, is er sprake van een belangenconflict tussen het centrale en het decentrale niveau.² Op centraal niveau wordt vervolgens beleid gemaakt over het delen van informatie, om daarmee de effectiviteit van de totale

¹ In artikel 12 van de Politiewet is geregeld dat de politie bij de handhaving van de openbare orde en bij de uitvoering van de hulproces verbaalerleningstaak, onder gezag staat van de burgemeester. Politieoptreden ter handhaving van de rechtsorde valt onder gezag van de officier van Justitie, volgens art. 13 PW.

² Dijkstra et al (2006), *Towards a Multi-agent system for regulated information exchange in crime investigations*. Artificial Intelligence and Law, nr. 13, pp. 133-151

organisatie te vergroten. Op centraal niveau moet de organisatie verantwoording afleggen over de legitimiteit en de effectiviteit van haar optreden, aan het parlement of aan aandeelhouders ingeval van een bedrijf. Het centrale niveau houdt bij het vaststellen van beleid gewoonlijk rekening met lokale belangen: door ruimte te geven aan inpassing van het centrale beleid in de lokale situatie en door beslissingsruimte te geven aan de lokale instituties. Maar uiteindelijk legt het centrale niveau normen op die bedoeld zijn om het probleem van conflicterende belangen tussen het centrale en decentrale niveau op te lossen. Daarnaast geldt in het algemeen dat informatiedeling kan worden beperkt door wettelijke normen en het beleid van de uitwisselende organisaties.

De situatie bij de politie is niet heel anders. Ten eerste wordt de verwerking en uitwisseling van informatie door de politie door wettelijke normen beperkt, zodat de privacy van personen waarop de informatie betrekking heeft wordt beschermd. Daarnaast worden binnen politiekorpsen diverse regels gehanteerd betreffende informatiedeling. Zoals eerder vermeld is de effectiviteit van de opsporing maar ook van de totale politieorganisatie, in principe gebaat bij een goede informatie-uitwisseling. Uiteraard wil een korps in ieder opsporingsonderzoek zoveel mogelijk relevante informatie verzamelen – ook afkomstig van andere korpsen. Anderzijds kan het in het belang van een korps, een team of van individuele politiemensen zijn om informatie niet te delen. Dan ontstaat een conflict tussen de effectiviteit van de totale organisatie en het decentrale belang bij het afschermen van informatie.

Het Rijk (c.q. de wetgever), de centrale institutie op het gebied van informatiedeling binnen de politieorganisatie, heeft beleid gemaakt om dit conflict in voorkomende gevallen op te lossen. Daarbij wordt voorzien in een bepaalde beslissingsruimte voor het lokale niveau; voor de korpsen. De wetgever spreekt zich uit over dit onderwerp in art. 15 van de Wet politiegegevens (Wpg).

Artikel 15. (ter beschikking stellen van politiegegevens)

1. De verantwoordelijke stelt politiegegevens ter beschikking aan personen die door hemzelf dan wel door een andere verantwoordelijke overeenkomstig artikel 6, tweede lid, zijn geautoriseerd voor de verwerking van politiegegevens, voor zover zij deze behoeven voor de uitvoering van hun taak.

2. In bijzondere gevallen kan, indien dit noodzakelijk is voor een goede uitvoering van de politietaak, de terbeschikkingstelling van politiegegevens door de verantwoordelijke worden geweigerd dan wel kan de verantwoordelijke beperkende voorwaarden stellen aan de verdere verwerking. Bij algemene maatregel van bestuur kunnen nadere regels worden gesteld over de

gronden waarop de terbeschikkingstelling kan worden geweigerd en over de beperkende voorwaarden die kunnen worden gesteld.

De norm die de wetgever hier tot uitdrukking heeft gebracht is dat politiegegevens ter beschikking dienen te staan aan geautoriseerde personen (lid 1), behalve in bijzondere gevallen (lid 2). Eenvoudig gezegd, moet informatie worden gedeeld, tenzij er bijzondere omstandigheden zijn. In latere hoofdstukken wordt nader ingegaan op de Wpg en de uitwerking van juridische kaders in protocollen binnen de politie. Voor nu is het goed op te merken dat onder meer met lid 2, analoog aan de algemene beschrijving, wordt tegemoet gekomen aan een beperkt aantal belangen van het lokale niveau; van de korpsen. De wetgever geeft in het Besluit politiegegevens (Art. 2:13 Bpg), expliciet een aantal condities waaronder terbeschikkingstelling van politiegegevens (voor een beperkte termijn) kunnen worden geweigerd. Bijvoorbeeld wanneer bij het delen van die gegevens gevaar voor leven of gezondheid van betrokkene of derden is te duchten. Ook kan onderzoek krachtens dit wetsartikel als embargo-onderzoek worden aangemerkt, indien sprake is van een zeer groot belang van afscherming vanwege afbreukrisico's, levensbedreigende risico's, politieke gevoeligheid of publiciteitsgevoeligheid van het onderzoek. De zogeheten weigeringsgronden komen uitgebreider aan bod in hoofdstuk 5 van deze rapportage.

Uit gesprekken met politiemensen is bekend dat de ruimte die de wet biedt voor informatiedeling niet volledig wordt benut.³ Kennelijk levert de norm uit art. 15 Wpg in de praktijk spanning op. Politiemensen hebben vaak meerdere gesprekken nodig om zeker te weten dat ze bij het delen van informatie volgens de wet en daarnaast in het belang van hun korps handelen. Deze terughoudendheid staat op gespannen voet met de wensen van het kabinet en van de korpschefs, die de veiligheid willen vergroten door een toename van informatiedeling tussen de korpsen. In deze spanning worden de vermelde, typisch verschillende belangen van het centrale en decentrale niveau ook weer duidelijk zichtbaar. Deze algemene beschouwing is van betekenis voor het verklaringsschema dat in dit onderzoek wordt gebruikt en in de volgende paragraaf wordt toegelicht.

³ *Idem*, p. 136

2.2 Motivatie voor het gekozen verklaringsschema

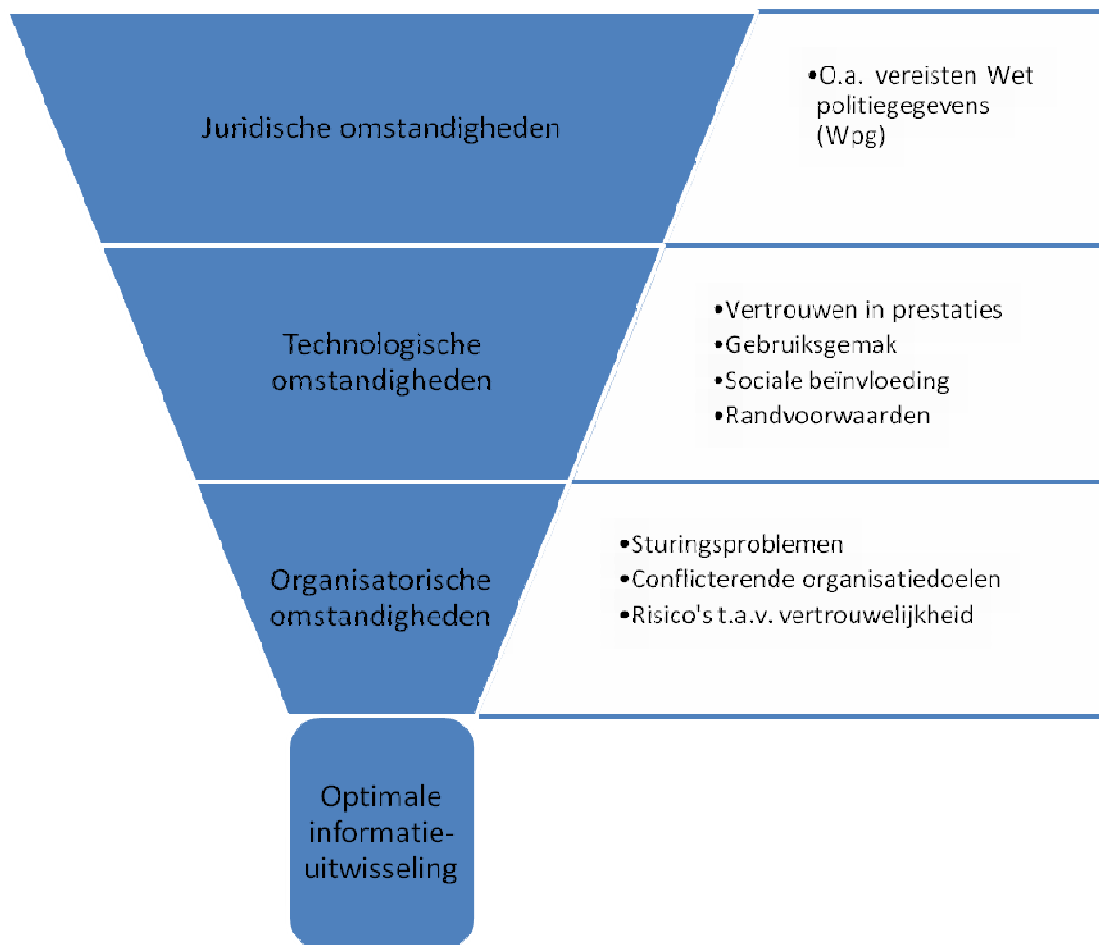
Uit onderzoek⁴ is bekend dat de ontwikkeling en de toepassing van informatiesystemen binnen de strafrechtketen (dus ook bij de politie) door diverse factoren worden beïnvloed. Hierbij is in de eerste plaats een juridisch kader voor de verwerking en uitwisseling van informatie van belang. Verder wakkeren ontwikkelingen in hard- en software de ontwikkelingen aan in het werkveld van de politie. Ook de organisatiecultuur waarin de informatiesystemen worden geïmplementeerd; de kwaliteit van de informatie input en output; de mate van betrokkenheid van het personeel bij ICT projecten en de training van uitvoerders en managers beïnvloeden de ontwikkeling en toepassing van informatiesystemen bij de politie.

De genoemde factoren mogen onderscheiden thema's lijken, maar dat zijn zij niet. Zo hangt bijvoorbeeld de ontwikkeling van wetgeving en intern politiebeleid samen met mogelijkheden op het gebied van ICT, in de ontwikkelings- en implementatiefase. Beleid kan niet los worden gezien van organisatiecultuur en beleid moet ook inspelen op de reacties vanuit de uitvoering als informatiesystemen eenmaal zijn ingevoerd. Diverse invalshoeken die genoemd zijn blijven een rol spelen na invoering van nieuwe informatiesystemen. Daarom worden ook in dit onderzoek, zoals blijkt uit de gestelde deelvragen, de meeste van de genoemde invalshoeken gehanteerd om het probleem van de beperkte informatiedeling bij de politie te bestuderen. Daarbij is naast het uitgebreide onderzoeksgebied over ICT acceptatie, ook een organisatiesociologische en politiewetenschappelijke invalshoek gekozen.

2.2.1 Verklaringsschema

Het verklaringsschema in dit onderzoek gaat ervan uit dat een optimale informatie-uitwisseling door opeenvolgende factoren beperkt kan worden. Dit schema kan daardoor als een trechter worden voorgesteld, zoals in onderstaand weergegeven. Wanneer bijvoorbeeld juridische mogelijkheden om informatie te delen ruim zijn, kan deze vervolgens nog worden beperkt door technologische en/of door organisatorische omstandigheden.

⁴ Pattavina, A. (2005), *The future of information technology in criminal justice*, in: Pattavina, A. (ed.), *Information technology and the criminal justice system*, p. 261



2.2.2 De invloed van wettelijke regels op informatiedeling

Zoals vermeld is wetgeving van invloed op de ontwikkeling en toepassing van informatiesystemen bij de politie. Bij het verwerken en invoeren van opsporingsinformatie, kunnen juridische knelpunten van negatieve betekenis zijn voor de beslissing om die informatie te delen. Omdat recent, in januari 2008 de Wet politiegegevens (Wpg) van kracht is geworden, speelt hierbij ook hoe in de organisatie van de korpsen op de nieuwe wet is gereageerd en hoe met de wetgeving en de kans om regels te overtreden, in de praktijk wordt omgegaan.

Het verklaringsschema in dit onderzoek veronderstelt dat een optimale informatie-uitwisseling ten eerste afhankelijk is van juridische omstandigheden. Behalve de noodzakelijke wettelijke bepalingen om informatie-uitwisseling überhaupt mogelijk te maken, worden met omstandigheden ook andere juridische facetten van het opsporingsproces bedoeld die negatief van invloed kunnen zijn op informatie-uitwisseling. Vanuit juridisch oogpunt worden een viertal mogelijke knelpunten onderzocht die voor rechtermensen aanleiding kunnen vormen om te kiezen opsporingsinformatie niet te delen:

- Rechtmatigheid van de verwerking van informatie
- Juistheid en volledigheid van informatie
- De recente invoering van de Wet politiegegevens (Wpg)
- Knelpunten op Wpg vereisten

Genoemde vier onderwerpen worden van hun theoretische achtergrond voorzien in hoofdstuk 5.

2.2.3 De invloed van technologie op informatiedeling

Vervolgens wordt in het verklaringsschema, een optimale informatie-uitwisseling afhankelijk geacht van technologische omstandigheden. Hierbij gaat het niet om de noodzakelijke techniek *sec*: in de jaren negentig is de netwerktechnologie op grote schaal geïntroduceerd en namen opslagcapaciteit en verwerkingssnelheid toe. In dit verklaringsschema gaat het meer om de kwaliteit van de techniek en de acceptatie ervan door de uitvoerende organisatie. Het verklaringsschema in dit onderzoek gaat ervan uit dat de uitwisseling van opsporingsinformatie wordt beperkt door:

- Onvoldoende vertrouwen in de werkprestaties van het systeem, in het bijzonder de kwaliteit van de informatie output en de snelheid waarmee informatie beschikbaar is.
- Onvoldoende gebruiksgemak, in het bijzonder de mate waarin werkprocessen van een korps aansluiten bij het werken met BVO en de afstand van de oude ICT-systemen tot BVO.
- Negatieve sociale beïnvloeding.
- Onvoldoende technische en organisatorische randvoorwaarden.

De genoemde determinanten zijn ontleend aan een studie door Venkatesh et al⁵, die een geïntegreerd verklaringsmodel hebben opgesteld waarmee de acceptatie van nieuwe ICT door gebruikers bestudeerd kan worden. De sterkste constructen op dit gebied zijn uit verschillende onderzoeken bijeen gebracht. Genomde vier constructen zijn aangewezen als directe determinanten voor gebruikersgedrag, waaruit de acceptatie van het systeem al of niet blijkt. Dit geïntegreerde model wordt *Unified Theory of Acceptance and Use of Technology* (UTAUT) genoemd.

In dit onderzoek (hoofdstuk 6) zal binnen de onderzochte korpsen worden gekeken in hoeverre de determinanten uit dit model, verklaringen

⁵ Venkatesh et al (2003), *User Acceptance of Information Technology: Toward a Unified View*, MIS Quarterly, Vol. 27, No. 3, pp. 425-478

bieden voor problemen ten aanzien van het gebruik van de benodigde ICT en daarmee voor problemen met informatiedeling bij de politie in het algemeen.

2.2.4 Gevolgen van de aard van de organisatie voor informatiedeling

Als laatste worden in het gekozen verklaringsschema organisatorische omstandigheden van invloed geacht op de informatie-uitwisseling bij de politie. Hiermee wordt enerzijds de aard van de organisatie bedoeld in organisatiesociologische termen. Anderzijds wordt ook de aard van het politiewerk, het opsporingswerk in het bijzonder, van invloed geacht op de mogelijkheden om informatiedeling te optimaliseren. Deze laatste invalshoek is meer een politiewetenschappelijke.

Yeheskel Hasenfeld heeft geprobeerd de specifieke karakteristieken van organisaties die werken met mensen, waaronder de politie, te beschrijven. Dit type organisatie heeft hij *Human service organization (HSO)* genoemd.⁶ Een centraal staand thema in de theorie van Hasenfeld wordt gevormd door de “loosely coupled systems” die in HSO’s veel worden aangetroffen. Dit begrip wordt in hoofdstuk 7 verder toegelicht, maar voor nu is het belangrijk om te weten dat het lastig is in een organisatie die wordt gekenmerkt door *loosely coupled systems* een centraal beleid te voeren. Eigen initiatieven van de uitvoerders, of in dit verband de *street level bureaucrats*, zorgen ervoor dat deze lastig onder controle zijn te houden binnen een formele structuur.

Doelen uit de omgeving en diverse doelstellingen van de HSO zelf kunnen met elkaar conflicteren, volgens Hasenfeld. Hij besteedt daarbij specifiek aandacht aan de sterke afhankelijkheid die HSO’s ondervinden van hun omgeving. Bij dit onderzoek gaat het er om de afhankelijkheidsrelaties in kaart te brengen die van invloed kunnen zijn op beslissingen van een individueel korps om informatie te delen. Hierbij wordt ingegaan op de relaties die korpsen hebben met het Openbaar Ministerie en met het ministerie van BZK. In deze afhankelijkheidsrelaties speelt de door Hasenfeld beschreven invloed van organisatiedoelen nadrukkelijk een rol.

Het verklaringsschema in dit onderzoek gaat ervan uit dat de uitwisseling van opsporingsinformatie wordt beperkt door:

- Problemen in de sturing van de informatiehuishouding

⁶ Hasenfeld, Y. (1983), *Human service organizations*, Englewood Cliffs

- Conflicterende organisatiedoelen

Zoals in paragraaf 1.9 van de inleiding aangegeven, wordt de vijfde deelvraag a.d.v. twee onderscheiden thema's beantwoord. Enerzijds wordt naar de aard van de politieorganisatie gekeken in hoofdstuk 7. Daarnaast wordt de aard van het politiewerk als invalshoek genomen om de beperkte informatiedeling tussen politiekorpsen te bestuderen (hoofdstuk 8). Op dit thema wordt ingegaan in de volgende subsectie.

2.2.5 Gevolgen van de aard van het politiewerk voor informatiedeling

Volgens Manning is de politie primair gericht op het hier en nu. Hij stelt dat de focus van de politieorganisatie ligt op responsiviteit en beheersing van de vraag. Het is ook deze focus die de succesvolle introductie van complexe criminaliteitsanalyse (d.m.v. het gebruik van ICT-systemen) onwaarschijnlijk maakt.⁷

Dat de werkelijkheid voor de politie niet eenvoudig is een gegeven dat van belang is om haar sturingsproblemen te kunnen begrijpen. "De politie moet werken in een omgeving die door een grote mate van diversiteit en onvoorspelbaarheid wordt gekenmerkt. (...) De politie is nauwelijks in staat om hier sturing aan te geven. Integendeel, het politiewerk wordt in hoge mate gestuurd door meldingen, klachten en aangiften van het publiek. De reactief ingestelde politie is – anders gezegd – de gevangene van een grillige omgeving."⁸ De focus op responsiviteit en als gevolg daarvan, de moeilijkheden bij het sturen van de organisatie, zou ook voor het probleem van de beperkte informatiedeling van betekenis kunnen zijn. Deze thema's sluiten naadloos aan op de organisatorische omstandigheden uit de vorige subsectie. Er wordt tot slot nog één factor toegevoegd. Het verklaringsschema gaat ervan uit dat de uitwisseling van opsporingsinformatie wordt beperkt door:

- Terughoudendheid vanwege risico's betreffende vertrouwelijkheid, welke zijn toegenomen door vervanging van de menselijke door een ICT-relatie.

In het volgende hoofdstuk wordt het interne beleid van de politie ten aanzien van informatie en informatie-uitwisseling besproken. In dit beleid is geprobeerd, de gedachte van art. 15 Wpg volgend, oplossingen te vinden voor de dilemma's

⁷ Manning, Peter K. (2005), *Environment, Technology, and Organizational Change*, in: Pattavina, A. (ed.), *Information technology and the criminal justice system*, p. 236

⁸ Aalberts M.M.J., H.G. van de Bunt (1994), *Politieële waarheden*. Tijdschrift voor de Criminologie, 36, p. 383

die in het algemeen een rol spelen bij informatiedeling. In hoofdstuk 4 wordt deelvraag I van een antwoord voorzien. In dit hoofdstuk worden de barrières voor informatiedeling tussen de korpsen beschreven.

3. *Beleid Uitwisseling Opsporingsinformatie*

In dit eerste inhoudelijke hoofdstuk wordt deelvraag I van een antwoord voorzien: *Wat is het beleid binnen de Nederlandse politie informatie ten aanzien van de uitwisseling van opsporingsinformatie tussen korpsen?*

Afspraken tussen de korpsen ten aanzien van het landelijk delen van opsporingsinformatie zijn vastgelegd in het *Beleid Uitwisseling Opsporingsinformatie*.¹ Dit document dat door de Board Opsporing van de Raad van Hoofdcommissarissen is vastgesteld, vormt het uitgangspunt voor de wijze waarop uitwisseling van opsporingsinformatie in de praktijk vorm heeft gekregen tot nu toe.

3.1 Doelstelling van het beleid

De centrale doelstelling van plateau 1, de eerste in het ontwikkelproces naar een nieuwe informatiehuishouding voor de opsporing, is de volgende: “Voor een beperkte groep infodesk-medewerkers van de 26 korpsen, toegang te realiseren tot de basispolitiezorgsystemen evenals onderdelen van de opsporingssystemen. De opsporingsinformatie die in deze systemen van het ene korps zijn opgeslagen worden zo direct raadpleegbaar voor andere korpsen. Plateau 1 maakt het raadplegen van gegevens uit andere korpsen mogelijk door de bestaande user interface, van de eerder genoemde systemen, van het ene korps via een directe (politie)netwerkverbinding aan te bieden aan bepaalde gebruikers in het andere korps. Om deze raadpleging te realiseren, moet voldaan worden aan een aantal randvoorwaarden.”²

3.1.1 Protocol ‘delen informatie’

In deze paragraaf wordt het afgesproken beleid gepresenteerd en toegelicht. De beheerder heeft de bevoegdheid om – in samenspraak met het OM – gegevens af te schermen. In het *Beleid Uitwisseling Opsporingsinformatie* is een categorisering van gegevens gemaakt, waarbij de indeling analoog is aan de mate van benodigde bescherming. Zie onderstaand schema: de minste bescherming behoeven de Basis Politiezorg gegevens in categorie A, waarop het eerder genoemde *free-flow*

¹ Het *Beleid Uitwisseling Opsporingsinformatie* is gemaakt voordat in 2008 de Wet politiegegevens (Wpg) werd ingevoerd. In het document worden daardoor de begrippen beheerder (Wpolr) en verantwoordelijke (Wpg) (abusievelijk) door elkaar gebruikt. Een geactualiseerde versie van het *Beleid Uitwisseling Opsporingsinformatie* is niet voorhanden.

² *Beleid Uitwisseling Opsporingsinformatie*, p. 1

principe zowel intra- als interregionaal van toepassing is. De meeste bescherming behoeven de onderzoeken in categorie D, waarvoor op grond van bijzondere voorwaarden afscherming mogelijk is.³

Cat	Categorieën van gegevens	Hit / no hit	Inhoud tonen	Toestemming vragen:
A	Gegevens ter uitvoering van de <u>dagelijkse</u> politietaak (handhavingstaak plus eenvoudige opsporingsonderzoeken): Voorbeeld van doelen waarvoor gegevens verwerkt zijn: • Handhaving van de rechtsorde • Surveilleren en verwerken meldingen • Hulpverlenen • Verwerken van aangiftes • Wijkgericht- en gebiedsgebonden werken • Handhaven van de openbare orde en bijzondere wetten • Eenvoudige onderzoeken	Ja	Ja	Nee (wel melding van gebruik)
B	Gegevens ter uitvoering van de handhaving van de rechtsorde in een bepaald geval inclusief afgesloten onderzoeken (de opsporingstaak). Voorbeelden van (projectmatige) doelen waarvoor gegevens verwerkt zijn: • Woninginbraken en heling • Hennekwekerijen • Mensensmokkel en -handel • Overvallen • Overige verdovende middelen • Milieudelicten • Zedenzaken • Geweldsmisdrijven w.o. doodslag	Ja	Ja	Ja

Cat	Categorieën van gegevens	Hit / no hit	Inhoud tonen	Toestemming vragen:
C	Gegevens ter uitvoering van de handhaving van de rechtsorde in een bepaald geval met daarbij een groot belang van afscherming vanwege onderstaande belangen zoals: • Afbreukrisico's door ongewild en ongewenst optreden • Levensbedreigende risico's • Nieuwsgierigheid prikkelende onderzoeken, zoals betrokkenheid van bekende Nederlanders of bepaalde zedenonderzoeken • Politieke gevoeligheid • Onderzoeken met veel publiciteit	Ja	Nee	Ja
D	Gegevens ter uitvoering van de handhaving van de rechtsorde in een bepaald geval met daarbij een zeer groot belang van afscherming. Hier wordt wel een automatisch signaal gegenereerd ten behoeve van het afgeschermd c.q. besloten (embargo) onderzoek zelf.	Nee	Nee	n.v.t.

³ *Idem*, p. 10

3.2 Basisregels

De kolommen geven per categorie aan wat de basisprincipes zijn voor het raadpleeg- en gebruiksprotocol.

Onder “hit/no-hit” in bovenstaand schema wordt een functionaliteit verstaan. Hiermee is vast te stellen of er informatie is betreffende een bepaald object (persoon, lokatie, goed, etc.). Men weet dan wel dat er informatie beschikbaar is, maar niet welke informatie het betreft. Voor een groot deel werd deze functionaliteit afgedekt door VROS.⁴ Voor categorie D wordt een speciale procedure toegepast waarbij de verantwoordelijke een signaal krijgt zodra iemand naar een afgeschermd object vraagt.

In de kolom ‘inhoud tonen’ van het schema is weergegeven of de onderliggende informatie ingezien kan worden.

In de derde kolom ‘toestemming vragen’ wordt de noodzaak tot het vragen van toestemming van de verantwoordelijke voor de informatie aangeduid, alvorens tot doorverstrekking (door de BlueView-geautoriseerde of informatierechercheur aan het betreffende team) en gebruik wordt overgegaan. “Uitgangspunt bij het raadplegen op inhoudsniveau is dat de informatierechercheur voldoende gekwalificeerd is om een correcte beoordeling te kunnen maken. Zowel in de A- als de B-categorie wordt een beroep gedaan op zijn professionaliteit.” Informatie uit deze twee categorieën is voor hem raadpleegbaar. Een infodeskmedewerker of informatierechercheur mag deze niet doorverstrekken zonder hiervan melding te maken (categorie A) of toestemming te vragen (categorie B).

In een voetnoot van het beleidsdocument wordt aangegeven: “Binnen de politie wordt de verantwoordelijke voor informatie veelal aangeduid als eigenaar van de informatie. Dit kan tot verwarring leiden. De term eigenaarschap suggereert immers dat iemand informatie voor zichzelf mag houden, terwijl het uitgangspunt nu juist het delen van informatie is. Zie ook artikel 10 Politiewet 1993.” Deze voetnoot laat de centrale positie zien die de verantwoordelijke (c.q. een bevoegde functionaris) heeft bij beslissingen over het delen van

⁴ Verwijsindex rechercheonderzoeken en subjecten (VROS) is een verwijsindex die werd ingericht om te voorkomen dat onderzoeken elkaar gingen kruisen. Om mee te draaien in deze index is vereist dat een lopend onderzoek dat naar verwachting langer gaat duren dan 5 dagen een Melding Recherche Onderzoek (MRO) wordt aangemaakt. Naast het matchen van de MRO's worden ook de subjecten en de voorlopige subjecten met elkaar vergeleken. Langs elektronische weg kan informatie over actieve opsporingsonderzoeken, opgenomen in de diverse rechercheondersteunende informatiesystemen, tussen en in de politiekorpsen worden uitgewisseld.

opsporingsinformatie. Hij wordt gestimuleerd om het uitgangspunt van informatie delen waar te maken, maar hij heeft tot op zekere hoogte vrijheid om aan zijn bevoegdheid zelf invulling te geven. In latere hoofdstukken komen we hierop terug.

In categorie B wordt op inhoud geraadpleegd in lopende onderzoeken. In de tekst van het *Beleid Uitwisseling Opsporingsinformatie* wordt aan dit aspect een opmerking gewijd: “Deze manier van werken zal voor velen nieuw zijn. Het laten inkijken in lopende onderzoeken zal afhankelijk van de regio in verschillende applicaties kunnen plaatsvinden.”⁵

“Als de informatierechercheur op informatie stuit in een ander onderzoek, zal toestemming gevraagd worden aan de regionale infodesk (de afdeling die verantwoordelijk is voor de informatiecoördinatie) en de teamleider van het onderzoek alvorens deze informatie verstrekt wordt voor verder gebruik. De verantwoordelijke voor de informatie bepaalt in welke categorie de informatie wordt aangeboden. Bij de C-categorie zal dit gaan om een leidinggevende van de leider van het opsporingsonderzoek in overleg met de zaakofficier van Justitie. Bij de D-categorie zal dit het diensthoofd recherche zijn in samenspraak met de CIE/ Recherche Officier van Justitie. Het uitgangspunt is echter dat in principe informatie wordt gedeeld in categorie B. Voor het indelen van informatie in categorie C moet daartoe een werkelijke noodzaak bestaan. De leider van het onderzoek zal daartoe zijn leidinggevende kunnen adviseren, maar deze leidinggevende dient in voorkomende gevallen expliciet te besluiten tot indeling in categorie C in plaats van B. (...) Bij een categorie D onderzoek ligt het initiatief tot verstrekking altijd bij de onderzoeksleiding van dit onderzoek zelf. De informatierechercheur krijgt hier immers geen “hit” of inhoudelijke informatie te zien.”⁶

Aan bovenstaand citaat valt op dat het woord verantwoordelijke slordig wordt gebruikt. Niet duidelijk is welke functie hiermee wordt bedoeld. De verantwoordelijke in de zin van de Wpg is voor een regiokorps, de korpsbeheerder. Zo opgevat wordt in dit citaat a.h.w. voorgesteld aan wie de verantwoordelijke zijn taak kan delegeren. In hoeverre korpsen deze structuur hebben gekozen, is gedurende dit onderzoek niet duidelijk geworden.

⁵ *Beleid Uitwisseling Opsporingsinformatie*, p. 11

⁶ *Ibidem*

Met het hiervoor beschreven schema werd in het *Beleid Uitwisseling Opsporingsinformatie* de basis gelegd voor een praktisch protocol voor bevraging. Bij bevraging van informatie binnen een andere regio kan men op verschillende categorieën van gegevens stuiten. Ook binnen de eigen regio kan de vraag ontstaan vanuit verschillende categorieën van gegevens. Hiervoor waren bij het vaststellen van het *Beleid Uitwisseling Opsporingsinformatie* al verschillende werkwijzen en afspraken ontwikkeld. Genoemd worden de Regeling Infodesk, het CIE werkproces zoals beschreven door ABRIO en de VROS regeling. Hierop wordt niet verder ingegaan. Het beleid voor informatiedeling zoals verwoord in het *Beleid Uitwisseling Opsporingsinformatie* vormt het onderwerp van dit onderzoek en is in lijn met deze kaders.⁷

3.2.1 Tactische risico's

In een beperkt aantal gevallen kunnen onderzoeksgegevens worden afgeschermd. Zowel de Wpolr als de Wpg voorzien in die mogelijkheid. “In geval van gevoelige opsporingsonderzoeken met een hoog afbreukrisico kan behoefte bestaan aan afscherming van de gegevens binnen het eigen korps, maar ook voor afscherming richting een ander korps. De afscherming kan betrekking hebben op gegevens van of over informanten en getuigen. Deze afgeschermd onderzoekgegevens zijn dan slechts voor het onderzoeksteam toegankelijk in verband met het afbreukrisico dat een dergelijk onderzoek loopt. Maar ook opsporingsonderzoeken naar ambtenaren, politici of bekende persoonlijkheden, kunnen om reden van bescherming van de persoonlijke levenssfeer worden afgeschermd. (...) De beheerder blijft de bevoegdheid houden in voorkomende gevallen gegevens af te schermen. Het afschermen van gegevens heeft betrekking op de aard van het onderzoek. De beslissing daadwerkelijk een onderzoek af te schermen, zal in samenspraak gebeuren met het OM.”⁸

3.2.2 Rol van het Openbaar Ministerie

Het Wetboek van Strafvordering kent de bepaling dat een proces-verbaal ten spoedigste moet worden opgemaakt en ingezonden naar het OM. Vanaf dat moment is het OM verantwoordelijk voor het verdere verloop van dit proces-verbaal in de strafrechtketen. Toch blijft de informatie die verwerkt is in dit proces-verbaal achter bij de politie. In de doctrine spreekt men over een vanzelfsprekendheid: de politie werkt met informatie die eenmaal rechtmatig is

⁷ *Idem*, p. 11

⁸ *Idem*, p. 8

verkregen en daardoor eerder is gebruikt voor het oplossen van andere onderzoeken.⁹

Wanneer gegevens moeten worden verstrekt, die zijn verkregen op grond van bevoegdheden die specifiek werden toegestaan door het OM voor dat ene onderzoek, heeft het OM een belangrijke rol. Deze rol bestaat uit het verlenen van toestemming op basis van enerzijds een tactische en anderzijds een juridische afweging.

De tactische reden voor het OM gegevens (tijdelijk) niet beschikbaar te stellen loopt voor een belangrijk deel samen met de redenen zoals deze voor de politie zijn beschreven.¹⁰ De juridische afweging betreft voornamelijk de toepasselijkheid van de vernietigingsbepalingen. “Vanzelfsprekend kunnen in de gegevensvergelijking geen gegevens worden betrokken die op grond van deze wet of op grond van het Wetboek van Strafvordering hadden moeten worden vernietigd, zoals op grond van de artikelen 125n, eerste lid, en artikel 126cc, tweede lid, van het Wetboek van Strafvordering.”¹¹

In het *Beleid Uitwisseling Opsporingsinformatie* is een categorisering van gegevens gemaakt, waarbij de indeling analoog is aan de mate van benodigde bescherming. Zie nogmaals bovenstaand schema: de minste bescherming behoeven de Basis Politiezorg gegevens in categorie A, waarop het eerder genoemde *free-flow* principe zowel intra- als interregionaal van toepassing is. De meeste bescherming behoeven de onderzoeken in categorie D, waarvoor op grond van bijzondere voorwaarden afscherming mogelijk is.¹²

3.2.3 Gebruiksbeleid en protocolbeleid

De basisregel is dat het gebruik van opsporingsinformatie uit een ander onderzoek altijd noodzakelijk moet zijn voor de uitvoering van het werk. “Dit gebruik kan nooit vooraf met exacte regels gedefinieerd worden. Daarom is het belangrijk dat achteraf verantwoording afgelegd kan worden.”¹³

Door vast te leggen welke informatiebronnen zijn geraadpleegd en wat daaruit is gebruikt voor een onderzoek, kan een medewerker achteraf onderbouwen wat de reden van het gebruik was. Een maatregel voor deze toetsing achteraf – bijvoorbeeld bij gebleken ontoelaatbaar gebruik of misbruik – is het vastleggen van raadplegingen (zie later: logging-beleid).

⁹ *Idem*, p. 8

¹⁰ *Ibidem*

¹¹ Memorie van toelichting Wpg

¹² *Idem*, p. 10

¹³ *Idem*, p. 12

3.3 Werkwijze bij bevragingen

“Bij raadpleging van interregionale bronnen vindt verstrekking van informatie van het ene naar het andere korps plaats. Daarbij wordt de volgende werkwijze voorgesteld. Nadat de benodigde informatie in lopende onderzoeken is gevonden, wordt aan de daartoe verantwoordelijke medewerker van het bevraagde korps schriftelijk (per e-mail) aangegeven:

- welke informatie gezocht werd;
- welke informatie gevonden is;
- welke informatie het vragende korps wil gebruiken;
- het doel waarvoor de informatie gebruikt gaat worden.

Binnen twee werkdagen geeft het leverende korps schriftelijk (per e-mail) aan of de voorgestelde verstrekking akkoord is en of er mogelijk nog meer informatie voorhanden is. (...) Door deze terugkoppeling wordt de beoogde informatiecoördinatie bevorderd.”¹⁴

Het gebruiks- en protocolbeleid is gericht op het zelfstandig vanuit een korps zoeken naar informatie, ook naar informatie die bij andere korpsen beschikbaar is. Dit vernieuwende aspect van de samenwerking tussen de regio's wordt als volgt gemotiveerd in het *Beleid Uitwisseling Opsporingsinformatie*: “Korpsen worden minder belast met zoekactiviteiten op verzoek van een collega korps. Toch wordt verwacht dat in bepaalde gevallen een korps aan (alle) andere korpsen een zoekvraag zal stellen. (...) Als een korps vindt dat na implementatie van dit beleid zij nog te veel zoekwerk voor andere korpsen moeten uitvoeren, dan kunnen zij deze korpsen wijzen op dit beleid waarin het zelfstandig zoeken als uitgangspunt is genomen.”¹⁵

Indien zogeheten artikel 8 gegevens worden gebruikt door het vragende korps, hoeft daarvan volgens bovenstaand schema alleen melding te worden gemaakt bij het bevraagde korps. De overige informatie moet formeel ter beschikking worden gesteld door de bevoegde functionaris van het bevraagde korps. Dat betekent dat het vragende team met het bevraagde korps contact moet opnemen. Een efficiënte taakverdeling tussen vragende en het bevraagde korps, m.b.t. het verzamelen van informatie is uitgangspunt van het *Beleid Uitwisseling Opsporingsinformatie*. Echter is ook aannemelijk dat wanneer het contact tussen korpsen eenmaal is gelegd, informatie ook breder en dieper

¹⁴ *Idem*, p. 12

¹⁵ *Ibidem*

gedeeld wordt naarmate de vragende partij beter is geïnformeerd over de informatie. Op deze veronderstelling wordt nader ingegaan in volgende hoofdstukken.

3.4 Beveiligingskader

In het *Beleid Uitwisseling Opsporingsinformatie* wordt het belang van beveiliging van informatie onderkend. “Beschikbaarheid, exclusiviteit en integriteit van gegevens in de diverse informatiesystemen dient te worden gewaarborgd, anders kan dit leiden tot een ernstige verstoring van de bedrijfsvoering of stagnatie van de primaire processen.”¹⁶

De beheerder van de gegevens dient voorzieningen te treffen die de bescherming van gegevens waarborgen. “Dit gebeurt volgens de huidige normen en daarin heeft ieder korps haar eigen verantwoordelijkheid. Ieder korps heeft zowel in technische zin als in organisatorische zin maatregelen geformuleerd en geïmplementeerd.”¹⁷ Deze maatregelen zijn enerzijds gericht op het verlenen van autorisaties zodanig dat aangewezen personen gegevens kunnen raadplegen. Anderzijds op het toetsbaar maken van de rechtmatigheid van het gebruik van geraadpleegde gegevens.

3.4.1 Kader voor verlenen autorisatie

Het is uiteraard niet voor iedereen noodzakelijk om de beschikking te hebben over opsporingsgegevens. Daarnaast wordt in het *Beleid Uitwisseling Opsporingsinformatie* onderkend dat niet iedereen in staat is om de kwaliteit van gegevens te beoordelen, evenmin als nut en noodzaak daarvan ten behoeve van een bepaald onderzoek. Het autoriseren wordt daarom beperkt tot een specifieke groep van personen. Dit zijn medewerkers van de informatie-afdeling (of: Infodesk) binnen een korps die voldoende getraind zijn in het beoordelen van gegevens. Zij zijn daarnaast werkzaam op schaalniveau 7 en 8 en hebben een A-screening ondergaan. “Deze medewerkers van de informatie-afdeling van de korpsen die in aanmerking komen voor autorisatie zullen met naam bekend worden gemaakt bij de andere korpsen (...). Om de geautoriseerde in staat te stellen op een efficiënte en correcte wijze om te gaan met deze vorm van raadplegen bij een ander korps zullen hoge eisen aan het opleidingsniveau gesteld mogen en moeten worden.”¹⁸ De competenties die hiervoor nodig zijn werden als bijlage aan het beleidsdocument toegevoegd.

¹⁶ *Idem*, p. 14

¹⁷ *Ibidem*

¹⁸ *Idem*, p. 15

3.4.2 BVO autorisatiemethodiek

Het *Beleid Uitwisseling Opsporingsgegevens* komt ook tot uitdrukking in de rubricering van gegevens in BVO. Deze is onder meer opgenomen in het document *BlueView Gegevensbeveiliging*.¹⁹ Deze rubricering is voor de volgende hoofdstukken van belang. Als daarin wordt beschreven hoe met de beleidsuitgangspunten in de praktijk wordt omgegaan.

Binnen de Basisvoorziening Opsporing (BVO) wordt aan gegevensgroepen een autorisatieniveau toegekend in het bereik 0 t/m 9. De autorisatieniveau 0 t/m 3 worden gebruikt om gegevens zichtbaar (raadpleegbaar) te maken binnen en buiten de eigen registratie. De autorisatieniveaus 4 t/m 9 worden gebruikt om binnen de eigen registratie onderscheid aan te kunnen brengen wie bij welke gegevens kan. Op basis van hun functie/rol krijgen medewerkers een autorisatieniveau toegekend. Deze worden hier kortheidshalve niet vermeld. Centrale gedachte is dat leidinggevendenden hoger zijn geautoriseerd.

Medewerkers worden geautoriseerd voor gegevensgroepen en/of registraties. De gegevensgroepen zijn te categoriseren in zachte en harde gegevens. Zachte gegevens zijn o.a. informatie uit buurtonderzoeken en informatie verkregen middels een machtiging van de Officier van Justitie zoals een tap of een Observatieteam. Harde gegevens zijn bijvoorbeeld getuigenverklaringen, een proces verbaal van een verhoor of forensische onderzoeksgegevens. Autorisatieniveaus worden door gebruikers toegekend aan verschillende door hen ingevoerde gegevensgroepen zoals registraties, mutaties, objecten etc. Hiermee worden indirect ook autorisatieniveaus toegekend aan gekoppelde gegevens(groepen) zoals kenmerken van mutaties en objecten en relaties tussen objecten.

Daarnaast kunnen medewerkers op basis van hun functie/rol een autorisatie krijgen waarmee zij ook systeembreed doorzicht (buiten de eigen registratie) hebben. Dat zijn medewerkers met een beperkt aantal rollen/functies binnen de politie. Zij krijgen een zogeheten superregistratie. Deze worden toegelicht aan het eind van deze subsectie.

Gegevens uit categorieën A, B en C uit bovenstaand schema mogen volgens het *Beleid Uitwisseling Opsporingsgegevens* gedeeld worden. In de BVO rubricering is aangegeven dat gegevens uit categorieën A en B, tot en met autorisatieniveau 4 toegekend kunnen krijgen. Categorie C tot en met autorisatieniveau 7. Dat betekent dat geautoriseerden tot en met niveau 4, zicht mogen hebben op alle

¹⁹ *BlueView Gegevensbeveiliging*, 15 oktober 2007

categorie A en B informatie. Voor BlueView geautoriseerden is het zicht op deze informatie volledig. Echter een rechercheur uit bijvoorbeeld een districtsteam kan alleen werken in BVO. Voor hem betekent dat in twee opzichten een beperking van zijn zicht op onderzoeken, behalve zijn eigen onderzoek. Ten eerste kan in BVO op dit moment alleen matching plaatsvinden binnen het eigen verzorgingsgebied²⁰ en ten tweede is de inhoud van onderzoeken niet te zien in BVO en wel in BlueView. In veel gevallen zal hij zich moeten wenden tot een BlueView geautoriseerde; meestal een medewerker van de infodesk.

Informatie uit categorie C kan volgens de BVO rubricering ook autorisatieniveau 5 krijgen toegekend door een korps. Met als gevolg dat infodeskmedewerkers in andere korpsen deze informatie niet meer kunnen raadplegen. In veel gevallen zullen de objecten uit het onderzoek op niveau 5 wel op niveau 1 worden gezet, waardoor de uitwisseling van informatie via bijvoorbeeld telefonisch contact op gang kan komen. Echter, dit is niet het uitgangspunt van het *Beleid Uitwisseling Opsporingsinformatie* dat juist, zoals eerder gesteld, als uitgangspunt heeft dat informatie in categorie B thuishoort, tenzij er een werkelijke noodzaak is te kiezen voor C. De leidinggevende van de leider van het onderzoek dient expliciet voor categorie C te kiezen volgens het beleid. Embargo onderzoek uit categorie D wordt niet doorgezet naar BlueView; informatie op autorisatieniveau 7 (informatie voor de leiding) en CIE-informatie evenmin.

Medewerkers uit het opsporingsdomein die op basis van hun functie/rol een superregistratie krijgen in tactisch opsporingsonderzoek van de BVO zijn diverse medewerkers van de CIE op autorisatieniveaus 5 en 6; de Regionaal Informatie Coördinator op niveau 5; de Regionale Inlichtingen Dienst (RID) op niveau 4; en de infodesk op niveau 4. Alleen de Chef van de infodesk is geautoriseerd op niveau 5.²¹

3.4.3 BVO autorisatiemethodiek ZwaCri

Op dit moment is het ZwaCri gedeelte van BVO nog niet landelijk. Toegang is gekoppeld aan de eerder genoemde verzorgingsgebieden. Het ZwaCri gedeelte van BVO staat los van de tactische opsporingsonderzoeken. Het wordt niet doorgezet naar BlueView en is primair ingericht voor gebruik door de CIE. Medewerkers van de CIE hebben een autorisatieniveau 5 of hoger. Andere medewerkers die op basis van hun functie/rol autorisatie krijgen tot ZwaCri

²⁰ De technische informatiehuishouding van de politie valt uiteen in zes onderscheiden landsdelen, met elk een eigen rekencentrum.

²¹ *Autorisatiemodel BVO*, 30 mei 2007

informatie van de BVO zijn de Regionaal Informatie Coördinator; de Regionale Inlichtingen Dienst (RID) en de infodesk. Zij hebben toegang tot en met autorisatieniveau 4.²² Dat is informatie die door de CIE wordt gekwalificeerd als operationeel te gebruiken. De afhandelingscodes voor CIE informatie, neergelegd in de CIE-Regeling staan in onderstaand schema. Daarin worden de autorisatieniveaus tussen haakjes vermeld, zoals ze volgens de BVO rubricering aan de afhandelingscodes zijn gekoppeld.

Afhandelingscodes²³

- | | |
|-----|--|
| 11 | Operationeel te gebruiken (autorisatieniveau 4) |
| 01 | Alleen te gebruiken na overleg met de afzender (autorisatieniveau 5) |
| 00 | Informatie met zware beperkingen voor gebruik (autorisatieniveau 6) |
| 200 | Kan niet operationeel gebruikt worden, maar kan onder bepaalde voorwaarden wel voor coördinatie- en analysedoeleinden worden gebruikt. + Informatie met verhoogd afbreukrisico (autorisatieniveau 7) |
| 300 | Kan niet operationeel gebruikt worden, maar kan onder bepaalde voorwaarden wel voor coördinatie- en analysedoeleinden worden gebruikt. + Informatie met bronbeschermingsbelangen (autorisatieniveau 8) |

²² *Autorisatiemodel BVO*, 30 mei 2007

²³ Regeling criminele inlichtingen eenheden, bijlage I

3.5 Toezicht en beheer

De autorisaties beperken de groep van personen die toegang heeft tot informatie. Strikt wachtwoordbeleid kan volgens het *Beleid Uitwisseling Opsporingsinformatie* helpen bij het voorkomen van bedoeld of onbedoeld misbruik door anderen dan de geautoriseerde. Toen dit beleid werd opgesteld werd gewerkt aan een 'autorisatie beheer service' en werd ten aanzien van wachtwoorden en inlognamen aangesloten bij het bestaande stelsel van veiligheidsmaatregelen.

Ten aanzien de in het beleid vastgestelde uitgangspunten is toezicht nodig. Het is belangrijk te weten wie welke informatie heeft geraadpleegd. De voorgangers van BVO (RBS en Octopus) beschikten daarom al over een logging-mechanisme.²⁴

3.5.1 Loggingbeleid

"Een maatregel voor toetsing achteraf – bijvoorbeeld bij gebleken ontoelaatbaar gebruik of misbruik – is het vastleggen van de raadplegingen. Ook het vastleggen van inlogtijdstippen en dergelijke draagt bij aan toezicht en beheer. (...) Niet alle geraadpleegde gegevens hoeven te worden vastgelegd. Dit zou een overmatige vorm van logging opleveren. Van belang is dat de volgende werkwijze achteraf verantwoord kan worden. Het vastleggen van geraadpleegde bronnen en gebruikte zoekvragen is voldoende. Echter, zodra er informatie gevonden is die relevant wordt geacht voor verstrekking aan het onderzoek, dan dient dat wel inhoudelijk vastgelegd te worden. Daartoe maakt het vragende korps (...) een bevragingsrapport. Het verstreckende korps registreert (...) welke informatie aan wie is verstrekt, bijvoorbeeld door vastlegging van een proces verbaal van verstrekking."²⁵

Naast verantwoording van verstrekkingen is logging volgens het *Beleid Uitwisseling Opsporingsgegevens* ook van belang voor controle op misbruik. Deze logging hoort 'real time' gevolgd te kunnen worden door de beheerders. De logbestanden dienen bovendien, zoveel als mogelijk, periodiek gecontroleerd te worden door het hoofd van de Infodesk.²⁶

"Eventuele incidenten worden direct gerapporteerd aan de Informatie beveiligingsmedewerker (IBF'er) van de regio. Op basis van de rapportage wordt gepaste actie genomen om herhaling te voorkomen. De beheerder heeft altijd de

²⁴ *Ibidem*

²⁵ *Idem*, pp. 15-16

²⁶ *Idem*, p. 16

mogelijkheid medewerkers, van wie het sterke vermoeden bestaat dat zij onjuist gehandeld hebben, de toegang tot de systemen te ontzeggen.”²⁷

Behalve voor de aanmelding in de rechercheapplicatie heeft het *Beleid Uitwisseling Opsporingsinformatie* aandacht voor de beveiliging van het korps- of locatienetwerk. “Tevens wordt op netwerkniveau vastgelegd hoeveel (mislukte) inlogpogingen er plaatsvinden. Hier vindt eveneens, zoveel mogelijk, een dagelijkse controle op plaats. Incidenten worden direct gemeld aan de IBF’er. De log-bestanden hebben een bewaartijd van tenminste 1 jaar.”²⁸

In het volgende hoofdstuk wordt de praktijk in vijf korpsen, vergeleken met de officiële landelijke afspraken ten aanzien van informatie-uitwisseling die in dit hoofdstuk werden behandeld. Er zal in het volgende hoofdstuk dan ook met regelmaat worden verwezen naar het hier besproken beleid.

²⁷ *Ibidem*

²⁸ *Ibidem*

4. Barrières in de informatie-uitwisseling

De rechercheorganisatie heeft de afgelopen jaren met veel ontwikkelingen te maken gehad. Interregionale researcheteams en de Nationale Recherche werden toegevoegd. De samenwerking, coördinatie en informatie-uitwisseling tussen de diverse onderdelen van de politie is daarbij een constant punt van aandacht geweest.

In het vorige hoofdstuk is het beleid van de politie op het gebied van informatiedeling behandeld. Tegen deze achtergrond wordt in dit hoofdstuk beschreven hoe met informatiedeling wordt omgegaan, in de praktijk van vijf politiekorpsen. Deelvraag II van dit onderzoek wordt daarmee van een antwoord voorzien: *Welke kenmerken heeft opsporingsinformatie die niet (optimaal) wordt gedeeld en door welke actoren wordt informatie niet (optimaal) gedeeld?*

Aan de hand van voorbeelden wordt geschetst hoe in de vijf onderzochte politiekorpsen met informatiedeling wordt omgegaan. Dit hoofdstuk heeft een beschrijvend karakter, waar de volgende hoofdstukken gericht zijn op het geven van een beschrijving op de thema's uit het verklaringsschema in hoofdstuk 2. Echter is onvermijdelijk dat bij de beschrijving van de situatie betreffende informatiedeling in vijf korpsen, wordt vooruit gelopen op verklaringen. Vooral omdat informanten de gevraagde situatie beschrijven en daarvoor een verklaring geven, in één zin.

Om bovenstaande deelvraag van een antwoord te kunnen voorzien, wordt beschreven hoe met de invoer van informatie wordt omgegaan in 4.2. Vervolgens worden de beslissingen die worden genomen betreffende het raadpleegbaar maken en beschikbaar stellen van informatie aan andere politiekorpsen beschreven in 4.3. Bij deze beschrijving ligt de nadruk op de kenmerken van opsporingsinformatie en op de functionarissen (actoren) die beslissingen nemen over het invoeren en delen van die informatie. Binnen de paragrafen worden de criminele inlichtingen eenheden apart behandeld omdat deze specifieke werkprocessen kennen.

4.1 Algemeen: informatiesystemen niet meer weg te denken

De informanten in dit onderzoek zeggen bijna geen informatiedeling tot stand te brengen, buiten de geautomatiseerde systemen om. Ook maken de informanten weinig melding van verzoeken om informatie buiten deze systemen om. Dit duidt erop dat informatiedeling tussen politiepolicorpsen onderling, zeker voor het leggen van contact, in belangrijke mate afhankelijk is van geautomatiseerde systemen. Soms wordt spontaan, niet n.a.v. informatie uit een geautomatiseerd systeem (telefonisch) contact gelegd, stellen informanten. Daarbij komt het voor dat in onderling contact informatie wordt uitgewisseld die niet in BVO is opgeslagen.

“De aanleiding is veelal informatie die al in het systeem staat. We zijn bezig met een onderzoek en één van onze subjecten woont in Amsterdam. Dan gaan we naar dat wijkbureau om informatie te halen. Dan heb je een gesprek met een collega en dan zeg je soms meer dingen dan wat in het systeem staat. (...) Het oude borstzakboekje bestaat nog steeds. We komen kortom, nog weleens met informatie terug die niet in de systemen staat.” – Tactisch coördinator regio-recherche (afdeling ZwaCri)

Een Melding Recherche Onderzoek (MRO) is een minimumvoorwaarde aan de invoer om tot informatiedeling via geautomatiseerde systemen te kunnen komen. De MRO vormt dan aanleiding voor teams om contact met elkaar te zoeken. Echter, de overdracht van de informatie wordt, zoals eerder aangegeven, niet altijd via elektronische weg afgewikkeld.

“Vaak is BVO of BlueView aanleiding om informatie bij elkaar op te vragen. Maar het kan zijn dat van buitenaf wordt gebeld, rechtstreeks met de vraag: wat weten jullie van dit of dat? Vaak worden er in BVO en BlueView een hele hoop dingen niet vermeld waarvan de kennis wel bij de collega's onderling in het hoofd zit. Wat weet je over die of die te vertellen? Op die manier wordt wel informatie uitgewisseld. Er zit veel meer in de hoofden en in boekjes van politiemensen dan er in de systemen vermeld wordt. Dat komt met name door de tijd die het kost om informatie weg te zetten; de gebruiksonvriendelijkheid. (...) Het zijn vaak contacten die je door een bepaalde zaak krijgt. Pas gebeurde bij ons een overval op een ABN Amro en via hen kregen we te horen dat er ook eentje in Blerik was geweest met dezelfde werkwijze. Voordat BlueView gevuld is met dat gegeven, dat is pas na een dag of twee, wordt

de lijn al gelegd met de rechercheafdeling daar en worden gegevens uitgewisseld over een bepaalde zaak of persoon. Als je dan mensen kent en er speelt iets buiten de regio, dan is het makkelijk om de telefoon te pakken.” – Senior tactisch coördinator districtsrecherche

Zoals eerder genoemd, is in het *Beleid Uitwisseling Opsporingsinformatie* gekozen om korpsen in staat te stellen de benodigde informatie te verzamelen bij andere korpsen. Hierbij staan centraal de systemen BlueView en BVO. De laatste voor de invoer van opsporingsgegevens. Hierop wordt in dit hoofdstuk de focus gelegd. Kleine opsporingsonderzoeken, de zgn. 40-uurszaken, moeten worden opgenomen in de Basisvoorziening Handhaving (BVH).

4.2 Invoer

Aan informanten op strategisch, tactisch en operationeel niveau zijn vragen gesteld over hoe met de invoer van opsporingsinformatie wordt omgegaan. BVO speelt daarbij een centrale rol.

4.2.1 Het gebruik van BVO

De mate waarin informatie wordt ingevoerd in BVO verschilt sterk per type rechercheafdeling. Een districtsrechercheur uit één van de onderzochte korpsen blijkt praktisch niet te werken met BVO. Van de onderzoeken op zijn afdeling wordt meestal wel een Melding Recherche Onderzoek (MRO) gemaakt, zodat de VROS-meldingen binnenkomen. Op deze manier komt informatie uit andere politiekorpsen wel binnen bij zijn afdeling. Informatie uit het eigen onderzoek wordt echter niet via elektronische weg met de andere politiekorpsen gedeeld, aangezien die niet wordt ingevoerd. Als er geen MRO wordt gemaakt, is bij andere politiekorpsen ook niet bekend dat er een onderzoek loopt op een subject in een bepaalde regio. In een tweede korps werkt de districtsrecherche in een eigen onderzoeksomgeving. In een derde wordt bij de districtsrecherche wel eens afgezien van het werken in BVO. In dat geval worden de onderzoeksjournalen meestal bijgehouden in MS-Word.

Informatie die van belang wordt geacht, wordt door teams van de regiorecherche goed ingevoerd. Dit zou bij de districtsrecherches veel minder het geval zijn, stellen informanten die werkzaam zijn op regioniveau. Door drie informanten wordt aangegeven dat de grootte van het onderzoek, verschil maakt voor de mate waarin BVO wordt betrokken in het werkproces. Genoemd wordt dat het invoeren van informatie in BVO kan helpen overzicht te houden in grote onderzoeken. Voor nu is belangrijk om op te merken dat bij het invoeren van informatie voor het eerst een beslissing wordt gemaakt over de vraag of informatie kan worden gedeeld.

“Ik zou kunnen denken: deze informatie is zodanig gevoelig, die zet ik er niet in. Dat zou ik kunnen doen en dan wordt er dus niet gedeeld. Maar ik kan me geen geval herinneren waarin ik dat gedaan heb.” – Tactisch coördinator regiorecherche (afdeling ZwaCri)

“Als je in een TGO [Team Grootschalige Opsporing] werkt wordt alles in BVO gedaan, als een soort lopend journaal van alles wat je doet. (...) Het onderzoek is

complexer, waardoor het wel in BVO geregistreerd moet worden. Anders ga je het overzicht missen. Vooral de leidinggevendenden. Er wordt ook op toegezien dat je in BVO werkt. Bijvoorbeeld je proces verbaal moet een BVO-nummer hebben, anders wordt het niet geaccepteerd.” – Senior tactisch coördinator districtsrecherche

“Het niveau van de onderzoeken in [mijn korps] zou er weleens voor kunnen zorgen dat ik zeg: we zetten alles erin. Dat is gebiedsafhankelijk. Snap je dat als ik morgen projectleider in Amsterdam zou zijn, ik (...) anders zou kunnen antwoorden? Als ik de moord op Pim Fortuyn zou moeten onderzoeken, wat geen embargo onderzoek is, dan ga ik echt niet alles in de BVO zetten. Als ik een liquidatie onderzoek moet doen, bijv. naar Endstra, dan ga ik niet alles in de BVO zetten. Als projectleider hier, heb ik dat soort ervaring niet.” – Onderzoeksleider TGO

4.2.2 De invoer bij de Criminele Inlichtingen Eenheid (CIE)

De invoer in BVO door de CIE in één van de onderzochte korpsen wordt door de informanten verschillend beschreven. Een CIE teamleider stelt dat zijn team alles invoert in BVO. Terwijl een analist/coach van de CIE in hetzelfde politiekorps aangeeft dat er ook weleens bewust informatie uit BVO wordt gehouden, vanwege een gebrek aan vertrouwen in de veiligheid van BVO. Hetzelfde is ook praktijk binnen de CIE van een ander korps. Wellicht wordt aan zorgen over het veiligheidsniveau in verschillende mate gevolg gegeven door teams van de CIE. Daarnaast wordt door medewerkers tussen en binnen CIE'en scheiding van informatie verlangd. De vertrouwelijkheid van informatie moet absoluut gewaarborgd zijn, zeggen zij.

“Soms [wordt niet alle informatie van mijn mensen] in BVO ingevoerd, vanwege afschermingsbelang. (...) Als bronnen verhalen vertellen over zeer belangrijke figuren. (...) Als onze informant in gevaar zou komen. Als we wel het subject kunnen benoemen maar niet de informatie, dan zetten we het subject in het systeem. Over de tekst wordt dan verwezen naar de bruto omgeving. Dan staat in de bruto het gedeelte dat alleen voor de CIE toegankelijk is.” – CIE teamleider

Hierbij speelt ook de interne toegang tot de informatie een rol volgens twee verschillende informanten.

“Dat zijn gevallen die op een apart schijfje komen. (...) Ook binnen de CIE moet je scheiding van informatie hebben. Dat is ook de reden dat we verschillende bakken hebben waar verschillende mensen in kunnen. We doen dat per vestiging. Dat zijn

zes runners. Er zijn mensen die door alle bakken heen kunnen. Dat zijn de analisten en de chefs. Informatie ligt dan soms al te breed. In uitzonderlijke gevallen zeggen we dan: dit stukje maar even niet. (...) Andere regio's willen ook meer scheiding aanbrengen. Een mooi voorbeeld uit het verleden: Richard Lengton [geval is bekend uit de pers, JK] uit Rotterdam. Die bleek aan de verkeerde kant te staan. Als hij zicht had op alle informatie, dan ben je gewoon alle informatie kwijt. Je kunt beter scheiden. Als er dan iets fout gaat, is er een probleem in één groep en niet in alle groepen. Zeker als bijzondere trajecten gedraaid worden moet dat in aparte bakken. Het idee is dat de informatie op een veilig moment terug gezet kan worden in reguliere bakken. (...) Kroongetuigen, burgerinfiltranten, dat zijn zaken, dat moet niet iedereen weten. Dat moet je zo klein mogelijk wegzetten. De doelstelling is in BVO en als het niet anders kan, dan zullen we wat anders moeten. – CIE teamleider

“In sommige gevallen werken we ook in MS-Word documenten. Als het een bepaald traject is. Als we iemand voor de getuigenbescherming willen krijgen i.p.v. als CIE informant. Dan is die informatie niet in BVO verwerkt omdat de hele afdeling eigenlijk niet mag weten dat we met hem praten.” – Kwaliteitscoach CIE

4.3 Informatie delen

Aan informanten op strategisch, tactisch en operationeel niveau zijn vragen gesteld over beslissingen die worden genomen betreffende het raadpleegbaar maken en beschikbaar stellen van informatie aan andere politiekorpsen. Voordat informatiedeling tussen politiekorpsen plaatsvindt, zijn nadat de invoer is verricht een aantal beslissingen aan de orde. Deze vormen de leidraad bij de beschrijving in deze paragraaf. In volgorde komen aan de orde: beslissingen over de raadpleegbaarheid en de uiteindelijke verstrekking van informatie (voor gebruik). Daarbij komen afspraken betreffende informatiedeling op korpsniveau en het thema restinformatie apart aan de orde.

4.3.1 Raadpleegbaarheid van informatie

Er zijn diverse methoden om informatie, in afwijking van landelijke afspraken, als het ware af te schermen voor andere teams en korpsen. De belangrijkste is geen of een beperkte invoer te doen waardoor van een onderzoek niets of (te) weinig raadpleegbaar wordt bij andere korpsen. Daarnaast is ook het autorisatieniveau dat aan de informatie wordt gegeven van invloed en bestaat de mogelijkheid een onderzoek niet naar BlueView door te zetten. In het laatste geval wordt het onderzoek wel in BVO bijgehouden en is het binnen het verzorgingsgebied ook raadpleegbaar. Zij het veel beperkter dan via BlueView.

Gevraagd naar de mate waarin opsporingsinformatie landelijk wordt gedeeld met geautoriseerde collega's hebben diverse informanten op operationeel en tactisch niveau er als eerste op gewezen dat zij het belang hiervan onderschrijven. Echter, diverse malen is daarbij de opvatting dat via de landelijke matching van MRO's via VROS, een systeem dat al sinds 1999 bestaat, op een juiste manier invulling kan worden gegeven aan informatiedeling tussen politiekorpsen onderling. Hierin is niet de inhoud van onderzoeken te zien, maar worden onder meer wel de subjecten die bij onderzoeken betrokken zijn gematcht. Daarnaast werd door diverse informanten gepleit voor het landelijk invoeren van BVO. Ook hierin wordt minder informatie direct raadpleegbaar voor het vragende korps. Allerlei andere mogelijkheden om informatie te koppelen via BVO en BlueView worden door deze informanten kennelijk niet gemist. Een aantal informanten wist niet op welke manier informatie zichtbaar wordt voor andere teams of andere korpsen, nadat zij het hebben ingevoerd.

In de vorige paragraaf kwam naar voren dat binnen de districtsrecherches in alle onderzochte korpsen de invoer van informatie regelmatig een probleem vormt.

Binnen grotere onderzoeken zoals wanneer op regioniveau in een Team Grootschalige Opsporing wordt gewerkt, is de invoer beter gewaarborgd zowel door de positie van de teamleiding als door het werkproces zoals rechercheurs dat vaak al jaren kennen. Het delen van de ingevoerde informatie vormt een probleem bij zowel de districtsrecherches als bij andere rechercheafdelingen. Onderstaand een behoorlijk compleet overzicht van de verschillende reacties ten aanzien van het raadpleegbaar maken van informatie, zoals die tijdens de interviews naar voren zijn gekomen.

De informanten van één van de korpsen, hebben afgezien van de situatie bij de districtsrecherches, geen afwijkingen van het protocol opgemerkt tijdens de interviews. Door informanten van de andere vier onderzochte korpsen werden diverse signalen afgegeven over het niet of verminderd raadpleegbaar maken van opsporingsinformatie via BVO en BlueView.

Bij één korps ontstaat een ander beeld zoals blijkt uit onderstaande twee citaten. Het blijkt dat in afwijking van het *Beleid Uitwisseling Opsporingsgegevens* de inhoud van onderzoek (mutaties) door dit korps systematisch niet of zeer beperkt raadpleegbaar worden gemaakt. Deze mogelijkheid bestaat alleen wanneer informatie (in termen van het beleid) ingedeeld wordt in de C-categorie. Deze beslissing dient als daartoe een werkelijke noodzaak bestaat, expliciet te worden gemaakt door een leidinggevende van de leider van het opsporingsonderzoek en in overleg met de zaakofficier van Justitie. Uitgangspunt volgens het beleid is dat informatie wordt aangeboden in de B-categorie en daarbij dient ook de inhoud zichtbaar te worden gemaakt. Verder worden volgens de betreffende informanten de leidinggevende en de Officier van Justitie, in afwijking van landelijk beleid, niet betrokken bij deze beslissing tot indeling in categorie C.

“Alle informatie wordt in BVO neergezet en landelijk gedeeld, maar niet de inhoud van de mutaties. De teamleider en de gegevensbeheerders kijken kritisch naar de autorisatieniveaus van de informatie. We stellen ons de vraag: kan dat wel gezien worden? Als dat niet het geval is, zetten we de informatie op zes weg. Rechercheurs kunnen informatie niet hoger wegzetten, dan waarvoor ze zelf geautoriseerd zijn. Teamleiders kunnen informatie wel hoger wegzetten.” – Analist/kwaliteitscoach recherche

“Binnen ons korps zijn heldere afspraken gemaakt m.b.t. invoer van informatie. De rechercheur kan altijd de informatie zelf invoeren. De zogeheten kennisdragers (teamleiders, dossiervormers, analisten) kijken alle informatie na en indien bepaalde informatie operationeel nog niet gebruikt kan of mag worden, wordt het autorisatieniveau van de mutatie door hen verhoogd. Hierdoor blijft de informatie wel zichtbaar voor diegene die hoog genoeg geautoriseerd is om de informatie te zien. Het object waar de informatie over gaat wordt wel gedeeld maar de inhoud niet. Om toch kennis te kunnen nemen van de inhoud van de informatie zal contact opgenomen moeten worden met de bevoegde functionaris, de teamleider danwel de zaaksofficier. Aangezien er altijd een MRO is aangemaakt deel je het object landelijk. (...) Indien informatie vertrouwelijk is en niet gebruikt mag worden, kun je er middels het autorisatieniveau voor zorgen dat een rechercheur die informatie niet kan gebruiken. Als de informatie betrouwbaar is en operationeel gebruikt mag worden, wordt de informatie op een zodanig autorisatieniveau weggezet dat de collegae de informatie kunnen zien en eventueel gebruiken. Alle objecten die binnen een onderzoek voorkomen, worden op autorisatieniveau 1 binnen BVO weggezet. Dit betekent dat binnen je verzorgingsgebied [dat is niet landelijk] iedere geautoriseerde gebruiker het object kan zien en tevens kan zien dat het object binnen een onderzoek danwel een registratie binnen ons korps voorkomt. Doordat bij onze onderzoeken verplicht een MRO wordt aangemaakt, delen we de informatie van objecten landelijk [via BlueView]. We controleren dat wekelijks.” – Directeur Opsporing

De betreffende directeur opsporing maakt geen onderscheid tussen het raadpleegbaar maken van informatie voor een ander korps en het ter beschikking stellen van die informatie aan het onderzoek van een ander team.

“Wat in de praktijk opvalt is dat niet iedereen goed op de hoogte is, hoe politiesystemen met elkaar communiceren. In de huidige situatie dienen alle art. 9 onderzoeken aangeleverd te worden aan BlueView. Dit betekent in de praktijk dat iedereen met een BlueView autorisatie in een lopend onderzoek de inhoudelijke informatie al kan bekijken. Terwijl volgens de Wpg de bevoegde functionarissen, de teamleider en de zaaksofficier, bepalen of de informatie ter beschikking gesteld mag worden. Immers artikel 9 Wpg zegt delen, tenzij...” – Directeur opsporing

Kennelijk strookt de opvatting van de geciteerde directeur opsporing niet met landelijke afspraken, die er moeite mee heeft dat lopende onderzoeken al geraadpleegd kunnen worden door een ander korps voordat over het gebruik

van die informatie is besloten door het bevroagde korps. In deze visie biedt een BlueView autorisatie kennelijk onvoldoende waarborg tegen ongeoorloofd gebruik van de informatie door het vragende team en dus zonder tussenkomst van de bevoegde functionaris en de Officier van Justitie. Het standpunt van de directeur opsporing werd ook vertolkt door de geïnterviewde informant op operationeel niveau in hetzelfde korps.

“Volgens mij loop je de bevoegde functionaris al voorbij als je de informatie kan lezen. In mijn ogen is die informatie dan ter beschikking gesteld. Als wij een MRO aanmaken dan delen we: personen, objecten, telefoonnummers, locaties. Niet de inhoud, die is gewaarborgd. (...) Als wij een verklaring hebben opgenomen, hoeft iemand uit Zeeland dat niet meteen te zien. Binnen je onderzoek kun je informatie zodanig wegzetten dat het niet voor iedereen zichtbaar is. Je kan niveaus 4, 5 en 6 gebruiken (...) Objecten etc. zetten we op niveau 1 weg. (...) Ik weet niet precies wat de afspraken zijn. Je hoort daar zoveel verschillende dingen over. Wij stellen de vraag of onderzoeken wel aan BlueView aangeleverd moeten worden. Als we dat doen, lopen morgen de onderzoeken stuk. De teamleider moet goedvinden of zijn lopende onderzoek aan BlueView aangeleverd wordt. Dat kan hij aanvinken op het moment dat hij een registratie aanvraagt.” – Analist/kwaliteitscoach recherche

Het verlenen van autorisaties voor BlueView (de zgn. superregistratie) is in het *Beleid Uitwisseling Opsporingsgegevens*²⁹ vastgelegd. Mogelijk worden deze afspraken als te ruim ervaren of worden de afspraken op dit punt onvoldoende nageleefd. Het was niet mogelijk binnen het verband van dit onderzoek na te gaan in hoeverre het beleid ten aanzien van de autorisaties wordt nageleefd. Een directeur opsporing van één van de andere onderzochte korpsen was er wel een sterk voorstander van dat andere korpsen kunnen beoordelen wat de bruikbaarheid van informatie is. Zij dienen volgens zijn opvatting zelf een inschatting van de betrouwbaarheid te kunnen maken.

Door overige informanten van andere korpsen wordt minder zwaar getild aan de manier waarop autorisaties worden verleend.

²⁹ Medewerkers uit het opsporingsdomein die op basis van hun functie/rol een superregistratie krijgen in tactisch opsporingsonderzoek van de BVO zijn diverse medewerkers van de CIE op autorisatieniveaus 5 en 6; de Regionaal Informatie Coördinator op niveau 5; de Regionale Inlichtingen Dienst (RID) op niveau 4; en de infodesk op niveau 4. Alleen de Chef van de infodesk is geautoriseerd op niveau 5.

“Uiteraard zijn er risico’s, maar ik ga uit van het standpunt dat iedereen bij de politie is gescreend en geautoriseerd. Ik ga uit van de kracht van het delen en dan moet je niet de beren zien dat het door verkeerden kan worden opgevraagd. Dat vind ik een beperkende gedachte. (...) In elk onderzoek wat wij draaien komen collega’s voor. Dan zou je kunnen zeggen van dat gaan we afschermen en dat doe ik nu juist niet.” – Onderzoeksleider TGO

Niettemin wordt in diverse korpsen de raadpleegbaarheid van informatie beperkt, zoals aangegeven in onderstaand citaat.

“Als we in een TGO werken, zetten we informatie veelal op autorisatieniveau 5 weg zodat het niet door iedereen geraadpleegd kan worden. Zeker met een lopend onderzoek.” – Senior tactisch coördinator districtsrecherche (met ruime ervaring in TGO)

Korpsen gaan verschillend om met het beleid omtrent informatiedeling. In de praktijk wordt een afweging gemaakt tussen het beleid enerzijds en diverse andere belangen anderzijds bij de beslissing om informatie raadpleegbaar te maken. Met verschillende uitkomsten als gevolg.

“Er zijn zware criteria voor het doen van embargo onderzoek³⁰. Ik heb onderzoek gedaan naar overheidsdienaren. Dat lag heel gevoelig en ik noemde dat dus wel een embargo onderzoek, maar volgens de criteria was dat het niet. Ik heb dat niet in BVO gedaan maar op mijn eigen schijf. Samen met nog een collega. Dit betrof een opdracht vanuit het korps.” – Senior tactisch coördinator districtsrecherche (met ruime ervaring in TGO),

CIE-informant X in onderstaand voorbeeld, legde verklaringen af die gebruikt konden worden in opsporingsonderzoek omdat hij in een traject voor getuigenbescherming wilde. De informant geeft aan hoe verschillend vervolgens met dit soort gevoelige informatie wordt omgegaan. Korpsen maken in hun handelwijze hun eigen afweging, zoals eerder aangegeven.

“Over BlueView. Toen wij met X begonnen waren, toen hadden we daarvan proces verbaal opgemaakt en dan staat zijn naam er in en die gaat naar een team toe en wat hij wil. Bij ons [in Amsterdam-Amstelland] gaat het naar een team dat werkt in

³⁰ Zie voor embargo onderzoek hoofdstuk 5

een besloten ruimte. In Utrecht draaide onderzoek op een liquidatie en die hadden zijn verklaringen daarover in X-pol gedaan, maar via BlueView te benaderen. Dus heel Nederland kon dat lezen en wist meteen dat X verklaringen had afgelegd. Dat geeft al een gevaar voor zijn familie etc.. Zij denken daar niet bij na. (...) Eerst was hij informant bij ons. Hij wilde in de getuigenbescherming, dus hij wilde alles tactisch verklaren. Bij ons dan is het geen bewijs. Wordt het tactisch dan kan je het als bewijs gebruiken, maar dan moet wel zijn naam erin. Dan gaat hij in de getuigenbescherming en gaan ze hem nooit meer vinden, bij wijze van spreken. Maar hij heeft hier wel familie wonen. Dus het is helemaal niet van belang om al in een vroeg stadium aan te geven: we zijn met dat onderzoek bezig. Als de tegenpartij dat weet, gaat die al getuigen beïnvloeden. Zodat ze bij jou komen: jij gaat niks vertellen. Terwijl dat een lopend onderzoek is. Doordat het door BlueView door heel Nederland verspreid wordt, is dat een nadeel. Dat is een reden voor Amsterdam geweest om dat niet in X-pol te doen zodat het niet door BlueView wordt opgezogen. Als je een onderzoek op Willem Holleeder doet, is dat niet handig om dat via BlueView benaderbaar te maken omdat iedereen hem kent. Leest een collega dat. Op een verjaardagsfeestje is het interessant om daar over te vertellen. Zo werkt dat gewoon. Dat wordt veel te breed, terwijl het onderzoek nog in volle gang is. Als het onderzoek is afgesloten, dan mag het in BlueView en mag iedereen het weten. Je kan naar de rechtbank gaan en dan weet je het ook. Als een onderzoek nog loopt, dan is dat vaak niet wenselijk. Ze hebben dat besef niet altijd. In Utrecht gooiden ze het er gewoon in.” – Coach bij de CIE

Dit citaat keert terug in hoofdstuk 8, waar het als voorbeeld wordt gebruikt om aan te geven op welke manier de gewenste vertrouwelijkheid van informatie van invloed is op beslissingen omtrent het delen van informatie met andere korpsen.

4.3.2 Informatie ter beschikking stellen aan een ander team

De terughoudendheid bij het raadpleegbaar maken van informatie via BVO en BlueView komt in voorgaande subsectie duidelijk naar voren. In rechtstreeks contact met andere teams geeft één van recherche teamchefs aan beducht te zijn zijn onderzoek niet te schaden. Hij is terughoudend informatie te delen en ter beschikking te stellen voor gebruik. Een andere geïnterviewde teamchef is minder of eigenlijk niet terughoudend.

“In principe deel ik alles met andere korpsen, tenzij het een onderdeel is waar ik mijn eigen onderzoek mee beschadig. Dan ga ik in overleg met de Officier.” – Onderzoeksleider TGO

"Ik kan me niet heugen dat wij hier een onderzoek draaien, wat we afgeschermd hebben. Dat doen we bijna niet." – Onderzoeksleider TGO

Volgens de Wpg moet informatie worden gedeeld tenzij sprake is van één of meer van de weigeringsgronden. In het volgende hoofdstuk wordt op deze bepaling dieper in gegaan. Twijfelgevallen, zoals in het eerder genoemde voorbeeld van een onderzoek waarin 'overheidsdienaren' betrokken waren of het voorbeeld van de informatie afkomstig van informant X, komen voor.

"Er zijn ook nog grijze gebieden. Daar is niet duidelijk wat wel en niet gedeeld mag worden. Dat geldt voor het hele land." – Directeur opsporing

Binnen de CIE is alles erop gericht informatie operationeel bruikbaar te maken. Waar een opsporingsteam veelal zelfstandig kan acteren op basis van informatie, werkt de CIE primair om onderzoeken voor de opsporingseenheden te voeden. In latere hoofdstukken wordt ingegaan op maatregelen die een CIE kan nemen om de hoeveelheid verstrekte, bruikbare informatie te maximaliseren.

4.3.3 Restinformatie

Ook de uitwisseling van restinformatie is in de afgelopen periode meer onder de aandacht gekomen bij de politie. De manier waarop hiermee wordt omgegaan varieert. Volgens een informant wordt er in zijn team van de districtsrecherche een rest-PV [proces verbaal] opgemaakt maar wordt de informatie niet ingevoerd in BVO. Deze aanpak verschilt van die van onderstaand geciteerde informant.

"Bij ons op de afdeling, op districtsrechercheniveau, gebeurt heel weinig met restinformatie. Er wordt wel een mutatie van gemaakt maar een proces verbaal wordt er niet van opgemaakt. We beginnen met een onderzoek, maar we zijn al blij dat we de beperkte zaak goed kunnen afdraaien en tegen de tijd dat de restinformatie verwerkt zou moeten worden, dan staat het volgende onderzoek alweer klaar en daar is ook weer haast bij." –Senior tactisch coördinator districtsrecherche

De citaten laten de afweging zien die in het algemeen binnen teams wordt gemaakt tussen het belang van informatiedeling en de inspanning die gemoeid is met een goede invulling daarvan. Het belang van een goede afwikkeling van

restinformatie wordt binnen korpsen meer en meer onderkend, maar het lukt niet altijd om er voldoende prioriteit aan te geven. Een nieuwe zaak gaat meestal voor en de werkdruk is hoog. In één van de onderzochte korpsen is er in de afgelopen periode verandering gekomen in die prioriteiten.

4.4 Tussenconclusie: beperkte invoer, beperkte raadpleegbaarheid

In dit hoofdstuk werd ingegaan op de invoer, raadpleegbaarheid en het ter beschikking stellen van opsporingsinformatie en op de manier waarop de onderzochte opsporingsteams omgaan met restinformatie. Ten aanzien van deze punten kunnen de volgende conclusies worden getrokken op basis van de interviews:

-In hoeverre informatie niet of niet optimaal wordt gedeeld kan niet exact worden bepaald. De hoeveelheid informatie die wel wordt gedeeld is niet precies bekend en de totale hoeveelheid beschikbare informatie is geheel niet vast te stellen.

-Informatie-uitwisseling bij de politie via geautomatiseerde systemen is niet meer weg te denken. Het contact, soms alleen op basis van een hit op een onderzoekssubject, ontstaat in de meeste gevallen via BVO en BlueView. In onderling contact komt het voor dat informatie uitgewisseld wordt die niet in BVO is opgeslagen.

-Over het algemeen zien informanten het nut van uitwisseling van opsporingsinformatie voor de opsporing als geheel. Echter ze zijn niet allemaal bereid om informatie in te voeren. Voor de informatiedeling in het opsporingsproces is de invoer van informatie een belangrijke voorwaarde. Om diverse redenen, die nader worden beschreven in de volgende hoofdstukken, wordt de invoer van informatie vaak niet of niet volgens protocol verricht. De invoer van opsporingsinformatie in BVO door districtsrecherche teams blijft achter bij die in het kader van meer grootschalige onderzoeken zoals in een Team Grootschalige Opsporing. Onderzoeksjournaals worden bijgehouden in MS Word. Opsporingsgegevens worden opgeslagen in diverse schaduwsystemen. Rechercheurs, met name districtsrechercheurs, kunnen voor een belangrijk deel zelf beslissen welke informatie wordt ingevoerd. Ook binnen de CIE wordt niet alle informatie in BVO ingevoerd.

-Informanten van tactisch en operationeel niveau zijn vaak terughoudend bij het raadpleegbaar maken van informatie via BVO en BlueView. In één van de korpsen heeft de directeur opsporing moeite met de raadpleegbaarheid van informatie uit lopende onderzoeken via BlueView. Uit de interviews komt het beeld naar voren dat de teamleiders, in afwijking van het *Beleid Uitwisseling*

Opsporingsgegevens, een grote zelfstandigheid hebben ten opzichte van hun leidinggevende en de Officier van Justitie, wanneer zij in voorkomende gevallen beslissen de raadpleegbaarheid van informatie in BVO en BlueView te beperken. Dat gebeurt door het autorisatieniveau te verhogen of door onderzoek niet door te zetten naar BlueView. Uit de interviews blijkt dat de raadpleegbaarheid in één van de korpsen in afwijking van het *Beleid Uitwisseling Opsporingsgegevens* op grote schaal wordt beperkt. Ook binnen teams van de andere korpsen is sprake van een beperking van de raadpleegbaarheid. Afwijkingen van het beleid impliceren eveneens afwijkingen van wettelijke en technische mogelijkheden om opsporingsinformatie te delen.

-Uit de interviews blijkt dat in rechtstreeks contact met een ander team, teamchefs soms terughoudend zijn informatie ter beschikking te stellen aan een ander team. Wel wordt over de risico's voor het onderzoek met de Officier van Justitie overlegd. Er zijn twijfelgevallen, waarbij voor veel politiemensen niet duidelijk zou zijn of informatie delen nu wel of niet verplicht is.

-Het verwerken van restinformatie gebeurt in verschillende mate in de onderzochte teams. Volgens informanten worden het belang van informatiedeling en de inspanning die gemoeid is met een goede invulling daarvan afgewogen. Het belang van een goede afwikkeling van restinformatie wordt binnen korpsen meer en meer onderkend, maar het lukt niet altijd om er voldoende prioriteit aan te geven. Nieuw onderzoek, dat in voldoende mate klaarligt, krijgt in de regel voorrang.

Deelvraag II van dit onderzoek wordt onderstaand bondig beantwoord: *Welke kenmerken heeft opsporingsinformatie die niet (optimaal) wordt gedeeld en door welke actoren wordt informatie niet (optimaal) gedeeld?*

De mate waarin een rechercheur opsporingsinformatie relevant acht, blijkt een informatiekenmerk dat van invloed is op de invoer van die informatie. Terwijl de bruikbaarheid van informatie voor een onderzoek, het beste beoordeeld kan worden door het korps dat de informatie vraagt. Zoals eerder aangegeven sluit ook het *Beleid Uitwisseling Opsporingsgegevens* aan bij dit uitgangspunt. Dat is niet voor niets. Binnen de politie overheersen horizontale relaties tussen de korpsen onderling: informatiedeling kan niet worden afgedwongen. Voor een optimale informatie-uitwisseling moeten verschillende partijen het dus eens worden over nut en noodzaak voor het delen c.q. operationeel gebruiken van die

informatie. Een voorwaarde voor het bereiken van overeenstemming is dat alle partijen geïnformeerd zijn, zodat een inhoudelijke discussie plaats kan hebben. Tegelijkertijd zal in de organisatorische context van 26 onderscheiden korpsen, deels een zelfstandige positie voor ieder van die korpsen behouden blijven, inclusief eigen informatiedomeinen.

Opsporingsteams blijken minder geneigd om informatie in te voeren en te delen, wanneer het informatie betreft uit een zaak die bij veel politiemensen, maar ook bij burgers bekend is. Volgens informanten vergroot bekendheid de kans op lekken.

De inhoud van onderzoeken wordt door de meeste informanten van de recherche het liefst niet raadpleegbaar gemaakt voor BlueView geautoriseerden. Bij voorkeur wordt informatie uitgewisseld in rechtstreeks contact, n.a.v. een match op een subject bijvoorbeeld. In die situatie kan de bevraagde teamleider bepalen welke informatie wordt uitgewisseld en kan zodoende informatie afschermen zonder dat de vragende teamleider dat weet.

Een CIE kan het risicovol achten om informatie te delen, indien de informant daarbij gevaar zou kunnen lopen. Dat is uiteraard een legitieme reden om informatie niet of onder zeer strikte voorwaarden te delen, zoals krachtens de CIE Regeling mogelijk is via de zogeheten afhandelingscodes (zie daarover verder hoofdstuk 5). Echter sommige informatie wordt door de CIE helemaal niet ingevoerd in BVO. De kans dat deze informatie uit het zicht verdwijnt wordt daardoor vergroot.

De vraag welke actoren binnen een korps, of binnen een opsporings- of een CIE team nu actief voor het beperken van de informatie-uitwisseling zorgen, is niet eenvoudig te beantwoorden. Eenheden hebben veel vrijheid ten opzichte van de korpsleiding en het beperken van de informatie-uitwisseling gebeurt vaak in teamverband. De teamleider, in de regel als tactisch leider van de onderzoeken heeft daardoor meestal een doorslaggevende stem. De rechercheur heeft beperkt invloed op de raadpleegbaarheid van informatie in BVO en BlueView. Omdat een rechercheur informatie niet op een hoger autorisatieniveau kan zetten dan waarvoor hij zelf is geautoriseerd. Sommige zijn geautoriseerd op niveau 5. Voor hen geldt hetzelfde als voor de teamleider die altijd hoger geautoriseerd is en daardoor de raadpleegbaarheid van informatie kan beïnvloeden.

Wat betreft de invoer van de informatie, hebben individuele rechercheurs wel veel beslissingsruimte. Teamleiders willen niet altijd sturing geven aan het invoerproces maar kunnen dat soms ook niet. Dat thema komt ook in latere hoofdstukken aan de orde.

In hoofdstuk 2 werd beschouwd dat informatie-uitwisseling tussen organisatieonderdelen in het algemeen plaatsvindt in een spanningsveld tussen centrale en lokale belangen. De beschrijving van de situatie bij de politie in hoofdstukken 3 en 4 blijkt hierbij aan te sluiten. In de hoofdstukken 5 t/m 9 wordt het theoretisch kader uit hoofdstuk 2 verder op de proef gesteld. Gekeken wordt of de theoretisch inzichten uit het gekozen verklaringsmodel, kunnen worden onderbouwd of weerlegd moeten worden. In het volgende hoofdstuk wordt de invloed van juridische omstandigheden beschreven.

5. Juridische omstandigheden: de Wpg in theorie en praktijk

Zoals vermeld is wetgeving van invloed op de ontwikkeling en toepassing van informatiesystemen bij de politie. Onderliggende wetgeving schept de mogelijkheden voor de uitwisseling van politiegegevens tussen korpsen, die vervolgens middels geautomatiseerde systemen wordt gerealiseerd. Zoals blijkt uit onderstaand citaat is de Nederlandse wetgeving erop gericht de mogelijkheden voor uitwisseling zoveel mogelijk te stimuleren. In dit hoofdstuk wordt de juridische context gegeven waarbinnen in dit onderzoek het probleem van beperkte deling van opsporingsinformatie tussen politiekorpsen wordt geanalyseerd.

De Memorie van Toelichting¹ op de Wet politiegegevens opent met de zin: “De samenleving verlangt van de politie dat deze op doelmatige en doeltreffende wijze zorg draagt voor de handhaving van de rechtsorde. Voorwaarde voor een goede taakuitvoering door de politie is dat de daarvoor noodzakelijke gegevens kunnen worden vastgelegd en op een efficiënte en effectieve wijze kunnen worden verwerkt. Meer dan ooit drijft het werk van de politie immers op het verwerken en veredelen van informatie. (...) waar aan de ene kant uitdrukkelijk is gekozen voor verruiming van de wettelijke mogelijkheden tot opslag, gebruik en verstrekking van persoonsgegevens door de politie voorziet het wetsvoorstel aan de andere kant in de nodige waarborgen voor de burger tegen ongerechtvaardigde inbreuken op zijn persoonlijke levenssfeer.”

Om zicht te krijgen op de genoemde verruiming van de wettelijke mogelijkheden, worden in paragraaf 5.1 t/m 5.3 de oude en de nieuwe wet geïntroduceerd. Zoals onder meer bleek uit het vorige hoofdstuk worden de huidige wettelijke mogelijkheden onderbenut. Tegelijkertijd kunnen bij het verwerken van opsporingsinformatie, juridische knelpunten ook van negatieve betekenis zijn voor de beslissing om die informatie te delen. In dit hoofdstuk worden de onderzoeksgegevens gepresenteerd, betreffende de derde deelvraag in dit onderzoek: *In hoeverre beperken wettelijke regels de uitwisseling van opsporingsinformatie tussen Nederlandse politiekorpsen?* Deze vraag wordt aan de hand van interviews beantwoord in paragraaf 5.4.

¹ Kamerstukken II 2005-2006, 30327, nr. 3, p. 1

5.1 De Wet politieregisters en de Wet politiegegevens (2008)

De verwerking van gegevens in politieregisters gebeurde tot en met 31 december 2007 onder het regime van de Wet politieregisters (Wpolr) en het Besluit politieregisters (Bpolr). Dit onderzoek richt zich bij het in kaart brengen van de juridische context voor informatiedeling tussen korpsen, op de Wet politiegegevens (Wpg). Echter, in deze paragraaf wordt een korte vergelijking gemaakt met als doel de veranderingen voor de praktijk aan te duiden. In het bijzonder wordt aangegeven waardoor de juridische mogelijkheden voor het delen van opsporingsgegevens zijn verruimd. Immers: “De wet (Wpg) houdt een nieuw evenwicht in tussen de bescherming van de privacy en burger enerzijds en het belang van de rechtshandhaving anderzijds.”²

5.1.1 Wet politieregisters (Wpolr)

De Wpolr ging uit van het registerbegrip (artikel 1, eerste lid onder c Wpolr). De wet concentreerde zich op het opnemen van gegevens in politieregisters en het verstrekken van gegevens uit politieregisters. Een politieregister werd ingevolge artikel 4 Wpolr aangelegd en aangehouden voor een bepaald doel en voor zover dit noodzakelijk was voor de goede uitvoering van de politietaak (zoals omschreven in artikel 2 Politiewet 1993). Voor ieder register moest een reglement worden opgesteld (artikel 9 Wpolr e.v.). Kern van het reglement was de omschrijving van het doel van het register. Voor een politieregister was eindverantwoordelijk de beheerder in de zin van de Wpolr. Bij de regionale politiekorpsen was de korpsbeheerder eindverantwoordelijk, zijnde de burgemeester van de grootste gemeente in de politieregio (artikel 1, eerste lid onder f Wpolr). Deze diende een registerbeheerder aan te stellen die de verantwoordelijkheid voor het register kreeg gedelegeerd. Deze kon op zijn beurt weer iemand met de dagelijkse leiding van het register belasten.

Artikel 7 Wpolr bepaalde dat de beheerder zorg droeg voor de juiste werking van het register. De beheerder droeg ook zorg voor de nodige voorzieningen van technische en organisatorische aard ter beveiliging van het register tegen verlies of aantasting van de gegevens en tegen onbevoegde kennisneming, wijziging of verstrekking daarvan. De beheerder, de registerbeheerder en degene die was belast met de dagelijkse leiding hadden voor het vervullen van hun respectieve rollen toegang tot de gegevens in het betreffende register. Zij konden gegevens verstrekken uit het register overeenkomstig het verstrekkingenregime dat in de Wpolr was vastgelegd. De

² Memorie van toelichting Wet politiegegevens, p. 1

Wpolr kende de mogelijkheid gegevens rechtstreeks langs geautomatiseerde weg te verstrekken. Hiervoor was ingevolge artikel 17 Bpolr een schriftelijke autorisatie van de beheerder vereist. Het wettelijk vastgelegde verstrekkingenregime kon niet door een autorisatie worden doorbroken.

Het gesloten verstrekkingenregime van de Wpolr bestreek zowel de verstrekkingen uit een politieregister binnen de politie (interne verstrekkingen) als aan derden (externe verstrekkingen). Voor interne verstrekkingen gold het uitgangspunt dat uit een politieregister gegevens konden worden verstrekt aan ambtenaren van politie en ander politiepersoneel dat was aangesteld ter uitvoering van de politietaak, indien dat noodzakelijk was voor een goede uitvoering van de politietaak: de zogeheten *'free flow of information'*, zij het dat daarvoor wel het *'need to know'*-principe gold. *'Nice to know'* was onvoldoende grond voor verstrekking. Het reglement regelde ingevolge artikel 10, vierde lid Wpolr ook de verstrekking van gegevens uit het register, daaronder begrepen de rechtstreekse toegang met het oog op de raadpleging van persoonsgegevens. Een reglement kon het wettelijk verankerde verstrekkingenregime niet verruimen maar wel inperken.

5.1.2 Tijdelijke registers

Zoals gezegd, kende de Wpolr (bijzondere) politieregisters. De tijdelijke registers behoren nadere bespreking. Een tijdelijk register kan worden omschreven als een set van gegevens die specifiek wordt verzameld voor een bepaald onderzoek, door een bepaald team. In de Wpolr werd gesproken over het verzamelen van gegevens voor een bepaald *doel*. Dit doel was in beginsel bepalend voor het gebruik van de verzamelde gegevens.

De gedachte van de wetgever was een voorziening in de wet op te nemen die in dringende gevallen de politie in staat kon stellen onmiddellijk te reageren, zonder eerst aan alle formaliteiten voor de vaststelling van een reglement te hoeven voldoen. In een tijdelijk register kon de politie alle informatie kwijt waarvan maar enigszins kon worden gesteld dat deze informatie kon leiden tot opheldering van een bepaald misdrijf. Bijvoorbeeld in een TGO, wordt heel veel informatie verzameld. Bij dit verzamelen hoefde de politie geen rekening te houden met zogeheten *'zachte gegevens'*. Met *zachte gegevens* bedoelt de wetgever dat het om onbetrouwbare informatie kan gaan over personen die geen verdachte zijn. De ratio van de Wpolr was dat vooral met *zachte informatie* zorgvuldig moest worden omgegaan. De wetgever doelde dan op operationeel gebruik van dergelijke *'zachte'* informatie ter bescherming van een

geregistreerde. Tegen doelafwijkend gebruik moest de geregistreerde worden beschermd, volgens de wetgever. Dat leidde de wetgever ertoe aan het raadplegen uit tijdelijke politieregisters en het verdere gebruik van relevante informatie een aantal verstrekingsvoorwaarden te verbinden. Daarmee werd een mogelijke verplichting tot verstrekking voorkomen. Verstrekking uit tijdelijke registers kon plaatsvinden mits de informatie eerst werd opgenomen in het register zware criminaliteit. Alvorens *gebruik* te maken van informatie diende daarvoor toestemming van de verantwoordelijke voor de informatie te worden gevraagd en kon een afweging worden gemaakt of opname in het register zware criminaliteit gelegitimeerd was.

raadplegen binnen verschillende lopende onderzoeken, onder bepaalde voorwaarden beter mogelijk gemaakt.³

³ *Beleid Uitwisseling Opsporingsinformatie*, p. 7

5.2 Versterking van het *free-flow* principe in de Wpg

De Wpolr is in bovenstaande paragraaf op hoofdlijnen aan bod gekomen. Hier wordt de Wet politiegegevens (Wpg) behandeld en daarbij vergeleken met de Wpolr. Vaak worden met de invoering van de Wpg, praktijken in de wet geïntroduceerd die al onder de Wpolr gemeengoed waren geworden.

Het wettelijk kader is uitgebreid onderzocht op bezwaren of beperkingen die verbonden zijn aan het landelijk uitwisselen van opsporingsgegevens. Zowel in de Wet politiegegevens (Wpg) als in haar voorganger de Wet politieregisters (Wpolr) is een duidelijke grondslag voor het zogeheten *free-flow* principe.

In de memorie van toelichting bij de Wpg komt het principe van ‘verplicht delen’ aan de orde in artikel 15, eerste lid. In de toelichting op het tweede lid staat dat de beschikbaarstelling, bij uitzondering geweigerd kan worden. In de Wpolr werd wel gestreefd naar het bovenregionaal gebruik van gegevens, echter in de Wpg is het *free-flow* principe verder versterkt. Daarnaast is het verdwijnen van het registerbegrip dat centraal stond in de Wpolr opvallend.

5.2.1 Evaluatie Wet bijzondere politieregisters

In het onderzoeksrapport⁴ naar de evaluatie van de bijzondere politieregisters wordt de ratio achter de Wpolr nader geduid: “Om te voorkomen dat gegevens uit een tijdelijk register verplicht dienen te worden verstrekt, waarmee het risico zou kunnen bestaan dat dientengevolge een zaak ‘stuk’ gaat of dat ‘zachte’ informatie via de tijdelijke registers verspreid wordt binnen de politieorganisatie, is een beperking aangebracht in het verstrekkingenregime.”⁵ In hetzelfde onderzoeksrapport wordt vastgesteld dat de uitwisseling van onderzoeksgegevens uit tijdelijke registers door geïnterviewden als te knellend wordt ervaren. Uit de wettekst en uit de memorie van toelichting bij de Wpg blijkt dat het registerbegrip mede door deze conclusies is vervallen.

5.2.2 Wet politiegegevens (Wpg)

De Wpg verlaat dus het registerbegrip en gaat uit van het verwerken van politiegegevens. De verantwoordelijke voor die verwerking bij de regionale politiekorpsen is ingevolge artikel 1, onder f Wpg de korpsbeheerder. Eén van de uitgangspunten van de Wpg is dat politiegegevens alleen mogen worden

⁴ *Evaluatie Wet bijzondere politieregisters*, uitgevoerd door de Erasmus Universiteit en Net2legal Consultant & Mazars, in opdracht van het Ministerie van Justitie en BZK, onder begeleiding van het WODC.

⁵ *Idem*, p. 30

verwerkt voor de doelen waarvoor ze zijn verkregen, behalve als de wet uitdrukkelijk in doelafwijkende bepalingen voorziet (artikel 3, derde lid Wpg). Ook doorbreekt de wet de doelbinding door te voorzien in de geautomatiseerde vergelijking en het in combinatie met elkaar verwerken van politiegegevens die voor verschillende doeleinden worden verwerkt, zoals bepaald in artikel 11 Wpg. Het geautomatiseerd vergelijken houdt in dat een verzameling van gegevens wordt bevraagd aan de hand van gegevens uit een andere verwerking.

Een ander uitgangspunt van de Wpg is het autorisatievereiste, neergelegd in artikel 6 Wpg en nader uitgewerkt in het Bpg: de Wpg en het Bpg bepalen wie geautoriseerd kunnen worden tot het verwerken en het geautomatiseerd vergelijken van gegevens. De verantwoordelijke (de onderzoeksleider) dient de politiefunctionarissen te autoriseren tot die verwerkingen van politiegegevens die zij nodig hebben voor het uitvoeren van de aan hen opgedragen onderdelen van de politietaak.

Door de mogelijkheid politiegegevens die voor verschillende doeleinden zijn verwerkt met elkaar te vergelijken, worden meer politiegegevens tegelijkertijd toegankelijk gemaakt. Het autorisatiesysteem opent als het ware het verstrekkingenregime: de schriftelijke autorisatie van de beheerder is vervangen door een standaard autorisatie waarbij politiefunctionarissen eenvoudig op grond van de aan hen opgedragen onderdelen van de politietaak, toegang wordt verleend tot de beschikbare gegevens. De verruiming van de juridische mogelijkheden om informatie tussen korpsen onderling uit te wisselen, wordt met name gevormd door deze combinatie van nieuwe mogelijkheden waarin door de Wpg wordt voorzien. Gegeven deze situatie wordt ook het 'need to know'-principe losgelaten. Door de geautomatiseerde combinatie van gegevens kan de politiefunctionaris die voor bepaalde gegevens is geautoriseerd, deze raadplegen zonder verdere voorwaarden.

Welke gegevens door welke politiefunctionarissen mogen worden verwerkt krijgt kortom vorm door de combinatie van doelbinding en de daarop geformuleerde uitzonderingen en het stelsel van autorisaties dat de verantwoordelijke binnen de gegeven grenzen dient vorm te geven. De privacyfunctionaris, die binnen iedere regio aangesteld moet zijn ingevolge artikel 34 Wpg, krijgt onder meer de taak om een overzicht bij te houden van de verleende autorisaties. De privacyfunctionaris krijgt in de Wpg de taak namens de verantwoordelijke toe te zien op de verwerking van gegevens, waaronder het bijhouden van een lijst met autorisaties en het adviseren van de verantwoordelijke over de naleving van de wet. In de Wpg is tevens de

protocolplicht opgenomen. Niet alleen verstrekkingen van politiegegevens, maar ook aanwijzingen dat gegevens onrechtmatig verwerkt worden, moeten schriftelijk worden bijgehouden. Dit geldt ook voor de toekenning van autorisaties. In het Bpg wordt de wijze waarop moet worden gelogd nader uiteengezet.

5.3 Intern ter beschikking stellen van gegevens

In deze paragraaf worden het intern ter beschikking stellen van politiegegevens en de verruimde mogelijkheden daartoe verder uitgewerkt, omdat deze vorm van informatiedeling in dit onderzoek centraal staat.

De Wet politiegegevens maakt onderscheid in doelen binnen de politietaak. Politiegegevens kunnen worden verwerkt met het oog op de uitvoering van de dagelijkse politietaak (artikel 8), de handhaving van de rechtsorde in een bepaald geval (artikel 9), het verkrijgen van inzicht in de betrokkenheid van personen bij bepaalde ernstige schendingen van de rechtsorde (artikel 10) of ten behoeve van de coördinatie- en ondersteuningsfunctie (artikel 13). De artikelen 9, derde lid, 10, vijfde lid, 11, eerste, tweede en vierde lid en artikel 13, derde lid van de Wpg maken het mogelijk om politiegegevens ter beschikking te stellen voor een ander doel dan waarvoor ze oorspronkelijk zijn verwerkt. Dus gegevens, die zijn verkregen in het kader van de surveillance of de afdoening van eenvoudige verkeersovertredingen, kunnen verder worden verwerkt in een onderzoek naar een bankoverval of in een analyse van een criminele inlichtingendienst en vice versa. De meeste informatie wordt ter beschikking gesteld krachtens art. 9 lid 3 Wpg.

Artikel 9 Wpg. (onderzoek in verband met de handhaving van de rechtsorde in een bepaald geval)

1. Politiegegevens kunnen gericht worden verwerkt ten behoeve van een onderzoek met het oog op de handhaving van de rechtsorde in een bepaald geval.

2. Het doel van het onderzoek wordt binnen een week, nadat is begonnen met de verwerking, bedoeld in het eerste lid, schriftelijk vastgelegd.

3. Politiegegevens die worden verwerkt overeenkomstig het eerste lid, kunnen, na instemming van een daartoe bevoegde functionaris, ter beschikking worden gesteld voor verdere verwerking voor zover dat noodzakelijk is voor een ander onderzoek als bedoeld in het eerste lid, de verwerking, bedoeld in de artikelen 10 en 12, of de uitvoering van de dagelijkse politietaak, bedoeld in artikel 8.

4. De politiegegevens die zijn verwerkt op grond van het eerste lid en niet langer noodzakelijk zijn voor het doel van het onderzoek, worden verwijderd, of gedurende een periode van maximaal een half jaar verwerkt teneinde te bezien of zij aanleiding geven tot een nieuw onderzoek als bedoeld in het eerste lid of een nieuwe verwerking als bedoeld in artikel 10, en na verloop van deze termijn verwijderd.

De afscherming van gevoelige onderzoeksgegevens kan hier in het geding zijn. Daarbij geldt dat de bij deze wet geïntroduceerde 'bevoegde functionaris' moet instemmen met de verdere verwerking voor een ander doel. Welke categorieën van politieambtenaren als zodanig door de korpsbeheerder kunnen worden aangewezen, is bepaald in artikel 2:10 Bpg (bijvoorbeeld de leider van het betreffende onderzoek of zijn plaatsvervanger dan wel de CIE-chef dan wel het hoofd van een eenheid met een vergelijkbare taak of hun plaatsvervanger).

Het doel van de instemming van de bevoegde functionaris is om te toetsen of er een zodanige discrepantie bestaat tussen het oorspronkelijke doel (opsporingsonderzoek) en het doel waarvoor de gevraagde gegevens verder zullen worden verwerkt, dat terbeschikkingstelling – mede gelet op de tactische belangen van de opsporing en de inbreuk op de privacy van betrokkenen – niet proportioneel zou zijn.

Hierboven is aan de orde gekomen dat de Wet politiegegevens uit gaat van een verplichting tot het ter beschikking stellen van politiegegevens, voor zover andere politieambtenaren deze gegevens nodig hebben voor de uitvoering van de politietaak (artikel 15). De gronden voor weigering van terbeschikkingstelling zijn opgenomen in artikel 2:13 van het Besluit politiegegevens. Uitgangspunt van het vereiste van instemming is dan ook dat de gegevens in beginsel intern ter beschikking worden gesteld voor verdere verwerking van een ander doel, tenzij een weigeringsgrond geldt. Het kan echter voorkomen dat er zwaarwegende redenen in verband met de proportionaliteit zijn om dat niet te doen. Daarvoor kan worden gedacht aan gevallen waarin gegevens van een onderzoek naar de betrokkenheid van een persoon bij zeer ernstige misdrijven worden opgevraagd ten behoeve van verdere verwerking in een onderzoek van een geheel andere orde, zoals een eenvoudige verkeersovertreding. Daarnaast kan het voorkomen dat, vanwege het belang van de afscherming op dat moment, bepaalde gegevens nog niet verstrekt kunnen worden. De toetsing kan in een dergelijk geval bijvoorbeeld aanleiding geven tot het maken van aanvullende afspraken tussen degene die de gegevens ter beschikking stelt en ontvanger over het tijdstip van ter beschikking stelling van de gegevens, het verdere gebruik van de gegevens, de terugkoppeling van dit gebruik en de afstemming tussen de verschillende projecten. Het vereiste van instemming biedt daarmee vooral een grondslag voor het maken van nadere afspraken tussen de betrokken politieambtenaren en niet zozeer voor het absoluut weigeren van het ter beschikking stellen van gegevens. De absolute weigering van het ter beschikking stellen van de gegevens kan, behoudens het

bovenbeschreven geval waarin zwaarwegende proportionaliteitsredenen aan de ter beschikking stelling in de weg zouden staan, alleen geschieden in de gevallen waarin één van de in artikel 2:13 Bpg genoemde weigeringsgronden van toepassing is. Om een weigeringsgrond te effectueren moeten gegevens worden gecodeerd om ze buiten een geautomatiseerde vergelijking of gecombineerde verwerking te houden.

Artikel 2:13 Besluit politiegegevens. [Weigeringsgronden (artikel 15, tweede lid)]

1. Het ter beschikking stellen van politiegegevens kan alleen worden geweigerd of aan beperkende voorwaarden worden onderworpen in het geval:

- a. het gegevens betreft omtrent informanten of andere personen als bedoeld in artikel 12, vijfde lid van de wet;
- b. gevaar voor leven of gezondheid van betrokkene of derden is te duchten;
- c. van een verwerking voor een intern integriteitonderzoek onder verantwoordelijkheid van de korpsbeheerder;
- d. van een verwerking door de rijksrecherche onder verantwoordelijkheid van het College van procureurs-generaal;
- e. het gegevens betreft die worden verwerkt op grond van artikel 10, eerste lid, onderdeel b van de wet;
- f. van een verwerking voor een door het College van procureurs-generaal als embargo-onderzoek aangemerkt onderzoek met een zeer groot belang van afscherming vanwege afbreukrisico's, levensbedreigende risico's, politieke gevoeligheid of publiciteitsgevoeligheid van het onderzoek.

2. De terbeschikkingstelling van persoonsgegevens, die worden verwerkt door het Meldpunt Ongebruikelijke Transacties, kan worden geweigerd tenzij:

- a. de terbeschikkingstelling van de gegevens plaatsvindt ten behoeve van verdere verwerking met het oog op het doel, bedoeld in artikel 10, eerste lid, onderdeel a, van de wet;
- b. uit de gegevens zelf een redelijk vermoeden voortvloeit dat een bepaalde persoon een misdrijf heeft begaan;
- c. de terbeschikkingstelling van de gegevens plaatsvindt op grond van artikel 16, eerste lid, onderdeel c, van de wet, en deze gegevens redelijkerwijs van belang kunnen zijn ter voorkoming of opsporing van misdrijven als bedoeld in artikel 3:1.

5.3.1 Ruimere mogelijkheden voor intern delen van informatie

Op voorhand lijkt de juridische context ondersteunend aan een ruimere uitwisseling van opsporingsinformatie tussen korpsen. Door art. 15 Wpg heeft de wetgever het belang van informatiedeling sterk gemaakt door mogelijke bezwaren daartegen terug te brengen tot een beperkt aantal weigeringsgronden. Daarnaast kan worden geconcludeerd dat door de komst van de Wpg

opsporingsinformatie binnen (en buiten) de korpsen breder toegankelijk is gemaakt met het oog op verbetering van de informatiepositie van de politie, voor onder meer het opsporen van verdachten. Of deze theoretische situatieschets ook zo uitwerkt in de praktijk, komt aan de orde in volgende hoofdstukken. In de volgende paragraaf worden specifiek een aantal knelpunten vanuit de juridische context van het researchewerk beschreven.

5.4 Juridische knelpunten

Vanuit juridisch oogpunt zijn een viertal mogelijke knelpunten onderzocht die voor rechtermensen aanleiding kunnen vormen om te kiezen opsporingsinformatie niet te delen. Nagegaan is hoe rechtermensen en hun leidinggevendens oordelen over de rechtmatigheid van de wijze waarop de informatie is verwerkt (1), over de juistheid en volledigheid van de informatie (2) en op grond daarvan menen dat zij niet alle informatie kunnen delen met andere korpsen. Ook knelpunten vanwege de recente invoering van de Wet politiegegevens (Wpg) worden belicht (3). In het bijzonder waar het gaat om wettelijke vereisten waaraan op korpsniveau beantwoord moet worden (4). Genoemde vier onderwerpen worden onderstaand van hun theoretische achtergrond voorzien. Daarbij worden steeds de gevonden knelpunten beschreven.

5.4.1 Rechtmatige verwerking van informatie

Het is voor een goede rechtsgang cruciaal dat de politie rechtmatig verkregen informatie levert. Onrechtmatig is informatie die is verkregen op een wijze die strijdig is met het recht. Voorbeelden van onrechtmatig verkregen informatie zijn:

- de aanleg van een telefoontap zonder rechterlijke machtiging,
- verkregen bewijsmateriaal uit een onrechtmatige huiszoeking of onderzoek aan het lichaam,
- cocaïnebolletjes verkregen uit een onrechtmatig inwendig onderzoek.

Maar ook informatie verkregen uit diefstal, bedrog of afpersing kan onrechtmatig zijn. Dat geldt ook voor informatie verkregen door een verborgen camera of telefoontap zonder machtiging van de Officier van Justitie, of wanneer het zwijgrecht voor een ondervraging niet tijdig is medegedeeld.

In het strafprocesrecht zijn uitgebreide voorschriften over de situaties wanneer iemand mag worden aangehouden en onderzocht, aan of zelfs in het lichaam. Dat zelfde geldt voor huiszoekingen. Ook wordt uitvoerig beschreven wanneer de verdachte moet worden geïnformeerd dat hij een recht tot zwijgen heeft. Wanneer bewijs niet rechtmatig is - bijvoorbeeld als het in Nederland niet volgens de regels van het Wetboek van Strafvordering en de door Nederland gesloten verdragen is verkregen - zal de rechter het bewijsmateriaal buiten beschouwing moeten laten. Hierdoor kan Justitie in bewijsnood komen, tenzij aanvullend rechtmatig bewijs voorhanden is.

Voor een rechtmatige verwerking van informatie, is de rechtmatigheid van verkrijging één van de voorwaarden op grond van art. 4 Wpg. Onrechtmatige verkrijging of een onrechtmatige verwerking van informatie kan een rechter aanleiding geven tot strafvermindering, vrijspraak of een sepot. Het gebruik van ‘rammelende’ informatie kan kortom zeer nadelige maatschappelijke gevolgen hebben, die ook hard aankomen bij het politieteam dat de informatie heeft verzameld of verwerkt. Als informatie wordt gedeeld, kunnen fouten van het ene team uiteraard gevolgen hebben voor het andere.

Een dossier behoeft tijdens de loop van een onderzoek slechts een beperkt aantal keren ‘waterdicht’ te zijn, namelijk alleen dan wanneer de rechter of de rechter-commissaris het moet inzien. Voor een belangrijk deel vindt die inzage plaats na afronding van het onderzoek. Wanneer nodig kan steeds nauwkeurig worden nagegaan of alle daarin aanwezige informatie aan de eisen van rechtmatigheid voldoet. Wanneer lopende het onderzoek niet goed beoordeeld kan worden of de verwerking van informatie rechtmatig is, zou dit aanleiding kunnen vormen om informatie niet met andere korpsen te delen.

De Wet politiegegevens heeft als uitgangspunt genomen dat de vastlegging van gegevens zoveel mogelijk wordt toegesneden op het voornaamste doel, namelijk de controle op de rechtmatige verwerking van politiegegevens. Voor het merendeel van de gegevensverwerkingen binnen de politie geldt de eis van machtiging. Met de eis van machtiging wordt beoogd te waarborgen dat de verwerking slechts plaats vindt voor zover noodzakelijk is voor een goede taakuitvoering van de ambtenaar van politie. De verantwoordelijke dient de nodige maatregelen te treffen om er op toe te zien dat de gegevensverwerking rechtmatig is. Om aan die verplichting uitvoering te kunnen geven dient de verantwoordelijke, in die gevallen waarin er aanwijzingen zijn van misbruik van machtigingen, de betreffende verwerkingen vast te leggen.⁶

Artikel 3 Wpg. (noodzakelijkheid, rechtmatigheid en doelbinding)

1. Politiegegevens worden slechts verwerkt voor zover dit noodzakelijk is voor de bij of krachtens deze wet geformuleerde doeleinden.
2. Politiegegevens worden slechts verwerkt voor zover zij rechtmatig zijn verkregen en, gelet op de doeleinden waarvoor zij worden verwerkt, toereikend, terzake dienend en niet bovenmatig zijn.

⁶ Memorie van toelichting Wpg, p. 65

3. Politiegegevens worden uitsluitend voor een ander doel verwerkt dan waarvoor zij zijn verkregen voor zover deze wet daar uitdrukkelijk in voorziet.

4. Bij de verwerking van politiegegevens op grond van de artikelen 9, 10 en 12 worden de herkomst van de gegevens en de wijze van verkrijging vermeld.

Gevonden knelpunten

Het vermelden van de herkomst en de wijze van verkrijging bij de informatie die wordt ingevoerd is van belang om de rechtmatigheid van informatie te kunnen beoordelen. Daarnaast is de betrouwbaarheid van informatie belangrijk, volgens informanten. Bij het opmaken van het dossier voor Justitie kunnen deze punten worden nagelopen.

“Ik was een tijd dossiercoördinator. Toen maakte ik dossiers op voor Justitie. Dat is ook een laatste controlemiddel voor een dossier. Klopt het allemaal juridisch gezien? Ik merkte dat ik vaak de vraag moest stellen bij collega’s: Je hebt mij die informatie verstrekt, maar wat is de bron hiervan en wat is de juridische basis van deze informatie?” – Tactisch coördinator regio-recherche (afdeling ZwaCrij)

Enkele informanten geven aan dat de bronvermelding niet altijd direct wordt vermeld, maar zeggen dat dit geen directe gevolgen heeft voor de mate waarin informatie wordt gedeeld. Op korpsniveau zijn in de onderzochte korpsen geen maatregelen genomen die een beperking vormden voor informatiedeling met andere korpsen, specifiek vanwege problemen met de rechtmatigheid van informatie.

Een informant op tactisch niveau gaf aan dat de opdrachtformulieren de kans op inschattingfouten minimaliseren. Ook wordt op dit punt gewerkt met een zekere foutmarge, waardoor informatiedeling niet hoeft te worden beperkt.

“Wij hadden in een buurtonderzoek aan een bewoner gevraagd of hij een huis in de gaten wilde houden. Daarover hebben we discussie gehad, die niet door de rechercheur zelf was voorzien. Dat wordt dan gecheckt en overlegd met de Officier van Justitie en uiteindelijk hebben we daar een beslissing in genomen. Mocht dan blijken dat het niet kan, dan schrappen we dat achteraf. Dat kan ook met een tap gebeuren: die loopt nog een dag door en daar komt informatie uit. (...) Wij moeten altijd het brondocument hebben en daar is wel toezicht op. Je kunt tegenwoordig heel veel informatie rechtmatig gebruiken. Als je informatie uit een ander onderzoek wilt gebruiken, dan moet je daarvoor toestemming vragen bij de

Officier. Dat doen wij wel. Het bewustzijn bij rechercheurs is ook: 'Als ik het niet volgens de regels doe, dan heb ik er niet zoveel meer aan'." – Onderzoeksleider TGO

Informanten op tactisch niveau hebben ingrepen genoemd bij fouten die rechercheurs maken op het gebied van rechtmatigheid maar deze waren steeds gericht op een incident en hadden geen structurele gevolgen voor de uitwisseling van informatie.

Binnen één van de onderzochte korpsen is afgesproken dat altijd de bron van de informatie achterhaald moet kunnen worden en het onderzoek waarin de informatie verwerkt is. Voor het verkrijgen van bepaalde informatie is toestemming van de Officier van Justitie nodig. Afspraken met Justitie zouden duidelijk zijn voor alle teamleden. Informanten hebben geen onregelmatigheden gemeld op dit punt. Informatie waarbij het de vraag is of deze ingevoerd moet worden, blijft tussen de teamleider en de Officier. Daarbij zou het volgens één van de informanten bijvoorbeeld kunnen gaan om een ambtsbericht van de AIVD.

"Wij verplichten mensen om de bron te vermelden. Mensen gaan BlueView bevragen en dan komen ze een proces verbaal-bevindingen van een collega tegen, maar die had al lang geschoond moeten zijn. Als de collega dan niet scherp genoeg op het tijdstip let, gaat hij dat klakkeloos gebruiken. (...) De rechercheur wordt nog eens nagelopen door de gegevens- en registratiebeheerders. Dat zijn de zogeheten kennisdragers die verantwoordelijk zijn voor bijv. de betrouwbaarheid van de informatie. (...) Alle informatie die we binnen krijgen is rechtmatig. Daar ligt een bevel onder of een machtiging." – Analist/kwaliteitscoach recherche

De verantwoordelijkheid voor de rechtmatigheid van verwerking wordt door informanten aangeduid als een teamaangelegenheid.

"Het is de vraag of de rechercheur dat allemaal kan overzien. De onderzoekscoördinator is bijvoorbeeld verantwoordelijk voor het toegankelijkheidsniveau van de informatie. Deels zijn teamleiders verantwoordelijk voor het wissen van geheimhoudingsgesprekken. Het is een teamaangelegenheid voor veel meer mensen." – Directeur opsporing

Problemen met rechtmatigheid van verwerking hebben dus niet voor structurele maatregelen gezorgd in de onderzochte korpsen. Op één uitzondering na. Hier is de informatiedeling beperkt, omdat er problemen ontstonden met de rechtmatigheid van de verwerking. Echter de beperking gold interne informatiedeling en niet de externe met andere korpsen, die het eigenlijke onderwerp is van deze rapportage. Onderstaand citaat is echter wel interessant omdat hierin een risico wordt beschreven dat bij het delen van opsporingsinformatie een rol speelt: de kans bestaat dat informatie wordt gebruikt wanneer dat formeel nog niet is toegestaan.

“[De CIE] beoordeelt welke informatie tactisch verstrekt kan worden zonder dat de informant gevaar loopt en zonder dat tactieken van de CIE gevaar lopen. We noemen dat een vier keer viertje. (...) Die vier keer viertjes werden tot op heden als achtergrondinformatie verstrekt aan bijna tachtig mensen in de regio. Districtscheefs, teamchefs recherche en teamchefs blauw. De informatie werd in briefingsdia’s getoond aan de medewerkers. De bedoeling is dat als medewerkers die informatie willen gebruiken, zij de CIE om een proces verbaal vragen. Mensen sloegen nu die informatie in hun hoofd op. Bijvoorbeeld het blauw op straat gebruikten dan die informatie. Soms zonder het zich te beseffen. Er is bijvoorbeeld een vier keer viertje dat een persoon verdovende middelen heeft. Ze zien deze rijden en doorzoeken de hele auto, Als je daar dan een proces verbaal van opmaakt, hoe ga je dan omschrijven dat je een onderzoek naar die auto instelde zonder dat daar een proces verbaal van de CIE voorradig is? Wij hebben het aantal mensen dat kennis mag nemen van de vier keer viertjes terug gebracht naar een stuk of tien teamchefs recherche.” – Directeur opsporing

5.4.2 Juistheid en volledigheid van informatie

Het vinden van informatie die juist en volledig is, vormt de *core business* van het researchewerk. Het delen van informatie is voor de inhoud van dit werk van grote betekenis. Uiteraard in positieve zin, als informatie van een ander korps een bijdrage levert. Maar informatie kan ook negatieve gevolgen hebben. Het kan een team bijvoorbeeld op het verkeerde spoor zetten. Betrouwbaarheid van de informatie is daarom cruciaal. Het oordeel over de waarde van informatie is belangrijk en zo mogelijk, nog belangrijker als rechercheurs van andere teams hiervan gebruik moeten maken. Mogelijk is twijfel ten aanzien van het wettelijke vereiste van juistheid en volledigheid van informatie binnen teamverband beter

te beheersen dan daarbuiten, waardoor vervolgens wordt besloten informatie niet te delen. Een korte toelichting op de werkwijze die de recherche volgt.

In elk rechercheonderzoek, zeker in grotere onderzoeken is sprake van informatie die niet zonder meer past bij de andere informatie die men heeft opgespoord. “Meestal wordt dan verder gerechercheerd op deze tegenstrijdige informatie. De meest gebruikelijke strategie is de betrouwbaarheid van verschillende informatiebronnen te waarderen en vervolgens de informatie die het meest betrouwbaar lijkt, als uitgangspunt te nemen. Zowel informatie als informatiebron worden op hun betrouwbaarheid beoordeeld. De informatie die het best past bij de overige informatie wordt dan het meest betrouwbaar geacht. Een tweede strategie is het zoeken naar overeenkomsten in de informatie en vervolgens op deze min of meer zekere informatie verder te Rechercheren. In dat geval wordt de dubbelzinnige informatie als onbekend beschouwd totdat er nieuwe informatie wordt gevonden waaraan deze kan worden afgewogen. Een derde strategie is het zoeken naar een soort gemiddelde. (...) Van de man die door de ene getuige zwart en door de ander blond werd genoemd, werd bijvoorbeeld aangenomen dat hij donkerblond was.”⁷

Uit deze beschrijving van de wijze waarop de recherche met tegenstrijdige informatie omgaat, blijkt het belang van een goede waardering van de betrouwbaarheid van informatie voor het kiezen van de onderzoeksrichting. Tevens blijkt hieruit dat Rechercheren uiteraard een zoekende strategie volgt, waarbij soms van het ene scenario voor een reconstructie, op een andere wordt overgeschakeld.⁸ “Informatie die afkomstig is uit verschillende bronnen of verschillende onderdelen van het onderzoek, kan lang niet altijd direct met elkaar worden geïntegreerd. Zo kan de ene getuige beweren dat de dader een pistool in handen had, terwijl de ander beweert dat hij dreigde met een mes. Ook zijn signalementen van eenzelfde dader soms onverenigbaar.”⁹ Deze tegenstrijdigheden blijken natuurlijk maar zelden tegelijkertijd. Juistheid en volledigheid van informatie zijn daardoor lopende het onderzoek per definitie moeilijk vast te stellen. Hierdoor kan in sommige gevallen worden voorbijgegaan aan relevante informatie die in eerste instantie niet goed bij het gereconstrueerde verhaal past. Voor de verwerking van politiegegevens zijn juistheid en volledigheid wettelijk vereist.

Artikel 4 Wpg. (juistheid, volledigheid en beveiliging politiegegevens)

⁷ Poot, C.J. de et al (2004), *Rechercheportret over de dilemma's in de opsporing*, Alphen aan den Rijn, p. 347

⁸ Ibidem

⁹ Ibidem

1. De verantwoordelijke treft de nodige maatregelen opdat politiegegevens, gelet op de doeleinden waarvoor zij worden verwerkt, juist en nauwkeurig zijn. Hij verbetert of vernietigt politiegegevens of vult deze aan indien hem blijkt dat deze onjuist of onvolledig zijn.
2. De verantwoordelijke treft de nodige maatregelen opdat politiegegevens worden verwijderd of vernietigd zodra zij niet langer noodzakelijk zijn voor het doel waarvoor ze zijn verwerkt of dit door enige wettelijke bepaling wordt vereist.
3. De verantwoordelijke treft passende technische en organisatorische maatregelen om de politiegegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau, gelet op de risico's die de verwerking en de aard van de politiegegevens met zich meebrengen.
4. De verantwoordelijke heeft toegang tot de politiegegevens die onder zijn beheer worden verwerkt ten behoeve van het toezicht op de naleving van het bij of krachtens deze wet bepaalde.
5. De verantwoordelijke verleent degenen die belast zijn met de controle en het toezicht, bedoeld in de artikelen 33, 34, 35 en 36, alsmede degenen die in zijn opdracht technische werkzaamheden verrichten toegang tot de politiegegevens die onder zijn beheer worden verwerkt, voor zover zij deze behoeven voor de uitvoering van hun taak.
6. De artikelen 14, eerste, tweede, derde en vijfde lid, 49 en 50 van de Wet bescherming persoonsgegevens zijn van overeenkomstige toepassing.

Gevonden knelpunten

Volgens informanten is onzekerheid rondom juistheid en volledigheid van informatie een gegeven dat bij researchewerk hoort. Informatiedeling wordt hierdoor niet in de weg gestaan omdat enerzijds teamleiders, tactisch coördinatoren en analisten mede verantwoordelijkheid dragen voor de invoer die rechercheurs doen. Zij controleren en 'ontzorgen' de rechercheurs. De betrouwbaarheid kan worden beoordeeld, wanneer een ander team die gaat gebruiken. Indien de informatie goed is ingevoerd. Als informatie nog niet (geheel) geverifieerd kon worden, kan dat worden aangegeven.

"Degene die de coördinatie heeft over het onderzoek leest wat iemand anders doet. Daar waar vragen zijn over hoe kom je aan die informatie en is die wel juist, dan zet hij dat weer terug bij die persoon en die moet het dan aanpassen of beter verwoorden." – Senior tactisch coördinator districtsrecherche

5.4.3 Knelpunten vanwege de recente invoering van de Wpg

De recente invoering van de Wpg zou een knelpunt kunnen zijn. Opsporingseenheden moeten leren werken met de nieuwe regels in de dagelijkse praktijk. Medewerkers hebben daarvoor voldoende opleiding nodig en tijd om ervaring op te doen. Als de regels die de Wpg stelt door teams niet goed overzien kunnen worden, leidt dat wellicht tot de keuze informatie niet te delen met andere korpsen.

Gevonden knelpunten

In twee korpsen hebben rechercheurs de door de Wpg gestelde bewaartermijnen als een frustratie aangemerkt, die bij de ene informant ook van invloed is op zijn bereidheid om informatie in te voeren. De ander vindt dat ondanks de frustraties over de bewaartermijnen, de informatiesystemen wel kunnen presteren. Informatie moet na het verstrijken van bepaalde bewaartermijnen bij de infodesk worden opgevraagd. Andere beperkingen zijn niet genoemd.

“Het enige waar ik me druk over maak is dat de informatie niet voor langere tijd geraadpleegd kan worden. Dat geldt voor BVH en BVO. Daar zit frustratie achter. Als informatie niet meer toegankelijk is, dan is dat erg zonde. Het inkloppen van gegevens kost bij veel mensen nogal wat tijd. (...) Als ik in een onderzoek heb gezeten en dat is afgesloten, dan wordt ook mijn registratie afgesloten en kan ik er niet meer bij.” – Senior tactisch coördinator

Een informant merkte op dat de vraag wat wel en niet mag volgens de Wpg, niet erg leeft bij rechercheurs. Daarnaast hadden twee informanten uit één van de onderzochte korpsen hier een afwijkende mening over. Hun opvattingen zijn ook in 4.3 aan de orde geweest.

“Wat in de praktijk opvalt is dat niet iedereen goed op de hoogte is, hoe politiesystemen met elkaar communiceren. In de huidige situatie dienen alle art. 9 onderzoeken aangeleverd te worden aan BlueView. Dit betekent in de praktijk dat iedereen met een BlueView autorisatie in een lopend onderzoek de inhoudelijke informatie al kan bekijken. Terwijl volgens de Wpg de bevoegde functionarissen, de teamleider en de zaaksofficier, bepalen of de informatie ter beschikking gesteld mag worden. Immers artikel 9 Wpg zegt delen, tenzij...” – Directeur opsporing

"Ik ben zelf Wpg kerninstructeur, maar ik ben wel ontevreden over de Wpg omdat er zoveel onduidelijkheid over bestaat. Ik vind dat de Wpg meer mogelijkheden heeft gegeven maar dat het is doorgeslagen. Wij geven aan bij de VTS dat je niet moet willen dat lopende onderzoeken worden doorgezet naar BlueView en dat we informatie al met elkaar kunnen delen op een veilige manier. We wachten nog op antwoord. De landelijke opleidingscoördinatoren voor BVO, geven ons standpunt ook aan. De praktijk is dat als ze het hebben gezien, dat ze het ook gaan gebruiken. De Wpg zegt heel duidelijk dat de bevoegde functionarissen beslissen over het ter beschikking stellen van informatie. Dat omzeilen we gewoon." – Analist/kwaliteitscoach recherche

Bedoeld wordt hier art. 9, lid 3 Wpg, waarin is vastgelegd dat gegevens (ter uitvoering van de handhaving van de rechtsorde) ter beschikking kunnen worden gesteld aan andere onderzoeken, na toestemming van een bevoegde functionaris. In het Beleid *Uitwisseling Opsporingsgegevens* wordt dit artikel door de politie uitgewerkt. De bedoelde bevoegdheid wordt gelegd bij de teamleider van het onderzoek ingeval van art. 9 informatie. Zie voor de details hoofdstuk 3. In dit beleid zijn ook het protocol 'delen informatie' en het kader voor het verlenen van autorisaties vastgelegd.

De geciteerde informanten blijken geen vertrouwen te hebben in de wijze waarop art. 9, lid 3 Wpg via het *Beleid Uitwisseling Opsporingsgegevens* uitwerkt in de praktijk. Het *raadplegen* van opsporingsinformatie door een beperkt aantal informatierechercheurs hoeft volgens het *Beleid Uitwisseling Opsporingsinformatie* niet strijdig te zijn met de bedoeling van de wetgever.

De geïnterviewde CIE medewerkers vinden dat de Wpg duidelijk heeft gemaakt wat wel en niet verstrekt mag worden. Hierbij ervaren medewerkers geen beperkingen. Ook werd opgemerkt dat de CIE al langere tijd werkt volgens voorschriften van de Wpg.

5.4.4 Knelpunten vanwege nieuwe wettelijke eisen aan de korpsen

Ook op korpsniveau leidt de Wpg tot een aantal nieuwe wettelijke eisen. Daaruit volgt dat de recente invoering van de Wpg ook op korpsniveau tot juridische knelpunten kan leiden. Uit onderzoek van het College Bescherming Persoonsgegevens (CBP) zijn enkele tekortkomingen gebleken die het vertrouwen tussen korpsen onderling zouden kunnen schaden. Mogelijk besluiten korpsen informatie niet te delen vanwege deze knelpunten op het gebied van de Wpg.

De Wpg verplicht de verantwoordelijke, voor een regiokorps is dat de korpsbeheerder, zorg te dragen voor het kwaliteitsniveau en de deskundigheid van zijn medewerkers. Dit geldt als één van de waarborgen voor het zorgvuldig gebruik van de ruimere bevoegdheden die de Wpg biedt voor de verwerking van persoonsgegevens. In de aanloop naar de inwerkingtreding van de Wpg heeft het College Bescherming Persoonsgegevens (CBP) onderzoek gedaan naar het functioneren van de infodesk binnen de regionale politiekorpsen. Het onderzoek¹⁰ was er op gericht zicht te krijgen op het functioneren van de infodesk en op de wijze waarop de wettelijke waarborgen voor de bescherming van persoonsgegevens worden gegarandeerd. Het CBP constateerde kort voor de inwerkingtreding van de Wpg dat de meeste regionale politiekorpsen niet toegerust waren op de eisen die deze nieuwe wet stelt. Ten tijde van het onderzoek bleek ruim een kwart van de 25 regionale korpsen niet aan 'logging' van bevestigingen uit het bijzondere register te doen. Het risico hiervan is dat niet te controleren valt of onbevoegden toegang hebben gezocht en gekregen tot de bijzondere politieregisters, die gevoelige persoonsgegevens bevatten. Van de korpsen die de bevestigingen wel loggen bleek het overgrote deel de 'loggingen' niet structureel te controleren. Uit onderzoek van het CBP naar het functioneren van de zogeheten politie-infodesk bleek dat de meeste regionale politiekorpsen ten tijde van het onderzoek geen volledig beeld hadden van de wijzigingen die zij moeten doorvoeren om deze waarborgen te effectueren. Zij waren op dat moment ook niet voornemens wijzigingen door te voeren. Ook wees het onderzoek uit dat er wat betreft de kwaliteitseisen die aan de medewerkers van de infodesk worden gesteld, sprake was van grote verscheidenheid tussen de regio's.¹¹ Het CBP heeft daarom in een drietal regionale korpsen vervolgonderzoek gedaan.

Hierbij heeft het CBP bij drie regionale politiekorpsen onderzocht of deze de autorisatievereisten en de protocolplicht van de Wpg naleven. Daarnaast is onderzoek gedaan naar de wijze waarop de privacyfunctionarissen bij de korpsen hun taak uitoefenen. Uit het onderzoek blijkt dat de onderzochte politiekorpsen op deze punten nog niet of nog niet volledig voldoen aan de vereisten van de Wpg. Verder is nagegaan of de korpsen het autorisatievereiste naleven alsmede de protocolplicht ten aanzien van enerzijds autorisaties en anderzijds ten aanzien van de mogelijkheid aanwijzingen voor onbevoegd gebruik van politiegegevens door de infodesk te controleren. Hoewel de

¹⁰ CBP (2008), *Politie Infodesk; onderzoek naar de inrichting van de politie infodesk en de waarborgen voor de bescherming van persoonsgegevens*, Den Haag

¹¹ *Idem*, p. 3

uitkomsten per korps verschillen, zijn bij geen van de drie korpsen de autorisaties en de controle beide volledig op orde. Ten aanzien van de privacyfunctionaris heeft het CBP geconstateerd dat deze bij geen van de drie onderzochte korpsen zijn advies- en/of controletaak overeenkomstig de wet uitoefent.¹²

In dit onderzoek wordt nagegaan welk effect de bevindingen van het CBP hebben op het onderlinge vertrouwen tussen korpsen waar het gaat om de vraag of informatie gedeeld kan worden of niet. Samengevat gaat het daarbij om de volgende bevindingen:

- gebrekkige 'logging' van bevestigingen;
- gebrekkige controle en
- het niet op orde zijn van autorisaties.

Gevonden knelpunten

De onderzochte korpsen zijn niet terughoudend met het delen van opsporingsinformatie wegens de gebrekkige logging van bevestigingen, die het CBP in bovenstaande onderzoeken heeft geconstateerd bij een aantal van de 26 korpsen. Evenmin zorgt de gebrekkige controle die het CBP heeft vastgesteld voor terughoudendheid met het delen van informatie. Informanten op tactisch niveau zijn soms niet op de hoogte van de situatie bij andere korpsen, en vaak zeggen zij zich er niet mee bezig te houden. Op strategisch niveau herkende één informant zich niet in de conclusies van het CBP; anderen wilden informatiedeling niet met te veel voorzichtigheid afremmen.

"We houden daar geen rekening mee. Je kan altijd uit angst dat er mogelijk ergens in Nederland iets fout gaat de deuren dicht doen. Als een ander verkeerd omgaat met de loggingprocedure, is de ander daarvoor verantwoordelijk." – Directeur opsporing

Wel zijn er beperkingen voor de informatiedeling opgetreden wegens beveiligingsproblemen m.b.t. CIE informatie. Hierbij was het onderlinge vertrouwen tussen korpsen wel in het geding.

"Er was sprake van ongecodeerde lijnen en automatiseringspersoneel zou ongeautoriseerd bij de informatie kunnen komen. Daar hebben wij wel moeite mee."

¹² CBP (2009), *Politie Infodesk II, onderzoek naar de waarborgen voor de bescherming van persoonsgegevens bij de Infodesk: rapportage van definitieve bevindingen*, Den Haag, p. 3

Soms hebben we informatie niet gedeeld en op hogere screeningsniveaus weggezet. We hebben de opdracht gekregen landelijk, dat er niet gedeeld mocht worden omdat de transcriptie/encryptie niet goed was geregeld. Het probleem is nog niet opgelost: we zijn nog aan het discussiëren.” – Directeur opsporing

“Over de Nationale Recherche. Door onze chef zijn we op de hoogte gesteld dat wij geen informatie meer met hun delen, totdat ze het goed op de rails hebben. Het is van de zotte dat analisten van tactiek zo in de CIE bak kunnen inloggen. Transparantie noemen ze dat. Ze zitten niet in ons verzorgingsgebied, dus het gaat om verstrekkingen. Die doen we mondjesmaat.” – Teamleider CIE

5.5 Tussenconclusie: beperkte invloed van juridische knelpunten

In de vorige paragraaf werden de onderzoeksgegevens gepresenteerd, betreffende deelvraag III in dit onderzoek: *In hoeverre beperken wettelijke regels de uitwisseling van opsporingsinformatie tussen Nederlandse politiekorpsen?*

Om deze vraag te beantwoorden werden een aantal mogelijke juridische knelpunten onderzocht. Deze werden genoemd aan het begin van de paragraaf 5.4. Ten aanzien van deze vier knelpunten kunnen de volgende conclusies worden getrokken op basis van de interviews:

-Er is bij een aantal van de onderzochte teams sprake van incidentele fouten. Deze worden gecorrigeerd, met hooguit tijdsverlies tot gevolg voor de invoer van de informatie, stellen de informanten. Problemen met het beoordelen van de rechtmatigheid van informatie leiden dus alleen indirect tot een beperking van informatiedeling.

-Het vereiste van juistheid en volledigheid van informatie leidt ook niet tot een direct knelpunt voor de informatie-uitwisseling tussen korpsen. Wanneer de tijd ontbreekt om een goede kwaliteit van de invoer te verzorgen, leidt het vereiste van juistheid en volledigheid mogelijk indirect tot een beperking van informatiedeling tussen korpsen.

-Art. 9, lid 3 Wpg leidt tot een knelpunt aangezien er tussen korpsen verschil van mening bestaat over de wijze waarop dit artikel zou moeten worden uitgewerkt. Door onder meer de directeur opsporing van één van de onderzochte korpsen wordt het raadplegen van opsporingsgegevens door een ander korps opgevat als ware het daarmee ter beschikking gesteld, echter zonder toestemming van de bevoegd functionaris.

-Ten aanzien van de recente invoering van de Wpg in het algemeen kan geconcludeerd worden dat de hierin opgenomen bewaartermijnen bij sommige informanten tot onbegrip leiden, met een lagere bereidheid om informatie in te voeren als gevolg.

-De bevindingen van het CBP ten aanzien van tekortkomingen op nieuwe wettelijke eisen aan de korpsen, lijken het vertrouwen tussen korpsen onderling niet of nauwelijks te beïnvloeden. Het onderlinge vertrouwen tussen korpsen is

wel in het geding doordat autorisaties onzorgvuldig werden verleend. Fouten die bekend zijn geworden hebben tot beperkingen van de informatiedeling geleid.

De beperking van informatie-uitwisseling door wettelijke regels blijkt relatief klein. Ten aanzien van het verklaringsschema uit hoofdstuk 2 kan worden geconcludeerd dat de juridische omstandigheden nauwelijks de uitwisseling van opsporingsgegevens in de weg staan.

6. Technologische omstandigheden: de acceptatie van ICT

In dit hoofdstuk zal de vierde deelvraag uit dit onderzoek van een antwoord worden voorzien: *In hoeverre beperkt technologie de uitwisseling van opsporingsinformatie tussen Nederlandse politiekorpsen?*

Hierbij staat centraal een verklaringsmodel voor de acceptatie van ICT in organisaties. Gekeken wordt in hoeverre beslissingen betreffende het delen van opsporingsinformatie worden beïnvloed door factoren uit dit model.

Achtereenvolgens worden in dit hoofdstuk de volgende thema's behandeld: De verwachting van de prestaties van het systeem (6.2); de verwachting van de benodigde inspanning bij het gebruik (6.3); sociale beïnvloeding (6.4) en het faciliteren van de gebruikers (6.5). Van iedere paragraaf maakt onderdeel uit een beschrijving van de onderzoeksresultaten op het betreffende thema. Aan informanten op operationeel niveau zijn bij ieder thema stellingen voorgelegd. Doel hiervan was in beeld te brengen in hoeverre de gebruikte techniek van invloed is op de bereidheid van rechercheurs en runners van de CIE om informatie in te voeren.

6.1 Acceptatie van nieuwe ICT in organisaties

Venkatesh et al¹³ hebben een geïntegreerd verklaringsmodel opgesteld waarmee de acceptatie van nieuwe ICT door gebruikers bestudeerd kan worden. Ongeveer 40% van de variantie in individuele bereidheid om technologie te gebruiken kon door onderscheiden theorieën uit ICT onderzoek, psychologisch en sociologisch onderzoek worden verklaard. De constructen (of verklarende variabelen) die in het geïntegreerde model zijn samengebracht kunnen tot 70% van die variantie verklaren. Vier constructen zijn aangewezen als directe determinanten voor gebruikersgedrag, waaruit de acceptatie van het systeem al of niet blijkt:

1. Verwachting van de prestaties van het systeem;
2. Verwachting van de benodigde inspanning bij het gebruik;
3. Sociale beïnvloeding;
4. Faciliteren van de gebruikers.

Dit geïntegreerde model wordt *Unified Theory of Acceptance and Use of Technology* (UTAUT) genoemd. Steeds een aantal van de items waarop de genoemde constructen zijn gebaseerd, hebben als onderwerp gediend voor de interviewvragen. Gezien het beperkte aantal geïnterviewden is het niet mogelijk om goed gebruik te maken van de schalen waarmee het oorspronkelijke verklaringsmodel werkt. Tijdens de interviews werd echter niet gesproken over de 'verwachting' van gebruikers maar over hun 'beleving'. De onderzochte ICT is relatief nieuw voor de gebruikers, maar wel al enige tijd in gebruik. Verwachtingen en beleving lopen daardoor als het ware in elkaar over. Gekeken wordt in hoeverre de uitwisseling van opsporingsinformatie wordt beperkt door:

- Onvoldoende vertrouwen in de werkprestaties van het systeem, in het bijzonder de kwaliteit van de informatie output en de snelheid waarmee informatie beschikbaar is.
- Onvoldoende gebruiksgemak, in het bijzonder de mate waarin werkprocessen van een korps aansluiten bij het werken met BVO en de afstand van de oude ICT-systemen tot BVO.
- Negatieve sociale beïnvloeding.
- Onvoldoende technische en organisatorische randvoorwaarden.

¹³ Venkatesh et al (2003), *User Acceptance of Information Technology: Toward a Unified View*, MIS Quarterly, Vol. 27, No. 3, pp. 425-478

6.2 Beleving van prestaties

In het model van Venkatesh et al geldt de mate waarin een individu vertrouwen heeft dat het gebruik van het onderhavige systeem hem zal helpen zijn werkprestaties te verhogen als definitie voor de verwachting van de prestaties van een systeem. Daarbij gaat het er om of de uitoefening van de beroepstaak gemakkelijker is geworden en of productiviteit en effectiviteit zijn toegenomen.

Productiviteit is voor veel fabrieksarbeiders een helder begrip, voor politiemensen ligt dat ingewikkelder. Het is voor een rechercheur niet in de eerste plaats het systeem dat de productie kan verbeteren. Maar de kwaliteit en de beschikbaarheid van de informatie die in het systeem is ingevoerd zijn van cruciaal belang voor de prestaties van het systeem. Rechercheonderzoek gaat om het verzamelen en bewerken van informatie.¹⁴ Een slechte output zou ervoor kunnen zorgen dat politiemensen de waarde van informatiesystemen voor hun werk lager inschatten, met een verminderde acceptatie en in het bijzonder een slechtere invoer, tot gevolg. In dit onderzoek wordt daarom als het gaat om prestaties van de ICT, zowel ingegaan op de kwaliteit van het systeem als op de kwaliteit van de ingevoerde informatie.

Hoe worden prestaties beleefd?

T.a.v. de kwaliteit van de beschikbare informatie zijn alle informanten het niet eens (3) of helemaal niet eens (2) met de volgende stelling: Ik ben minder bereid om informatie in te voeren in BVO door de kwaliteit van de beschikbare informatie in BVO en BlueView. Zij het dat de beschikbaarheid van informatie als beperkt wordt ervaren, de bereidheid om te investeren in de invoer en het delen van informatie wordt niet in de weg gestaan door de kwaliteit van de informatie in BVO en BlueView.

Als het gaat om de benodigde tijd voor het opvragen van informatie zijn informanten onverdeeld positief. Alle informanten zijn het niet eens (2) of helemaal niet eens (3) als zij de volgende stelling kregen voorgelegd: Ik ben minder bereid om informatie in te voeren in BVO door de tijd die het kost voordat door mij opgevraagde informatie beschikbaar is. Informanten zijn tevreden over de tijd die de Infodesk neemt om informatieverzoeken te verwerken. Een aantal zijn geneigd om vooruit te wijzen naar problemen met het gebruiksgemak of de compatibiliteit van BVO met andere informatiesystemen waarvan de recherche gebruik maakt.

¹⁴ Poot, C.J. de et al (2004), p. 347

Alle informanten zijn het niet eens (4) of helemaal niet eens (1) met de stelling: Ik ben minder bereid om informatie in te voeren in BVO door de prestaties van dit systeem. Sommigen geven aan dat er geen alternatief is, zoals ook in onderstaand citaat.

“Ook al is er niet zoveel vertrouwen dat alles teruggevonden wordt, dat is nog geen reden om informatie niet in te voeren. Want dan ben je het helemaal kwijt.” – Coach bij de CIE

Een andere informant:

“Het gaat niet over de prestaties, je kan er best iets in terugvinden.” – Senior tactisch coördinator districtsrecherche

Het veiligheidsniveau van de bruto omgeving van BVO waarin de gespreksverslagen met informanten van de CIE worden opgeslagen, is al enige tijd onderwerp van zorg binnen politie Nederland. Op dit moment wordt er aan gewerkt om deze verder te verbeteren. Eén van de informanten was nauw bij dit proces betrokken. Een belangrijk punt voor CIE medewerkers is de vraag of informanteninformatie uitsluitend door geautoriseerden van de CIE benaderd kan worden.

“ICT’ers kunnen de onderwerpregel lezen. Als wij zeggen: Gesprek met Pietje Puk over getuigenbescherming, dan lezen zij dat. Dat kan betekenen, als ze dat aan een crimineel zouden vertellen, dat ze hem doodschieten. Zo werkt het. We hebben er geen vertrouwen in, dus werken we niet in BVO.” – Kwaliteitscoach CIE

Eén informant wees erop dat er ook meer praktische redenen zijn om informatie niet in te voeren in BVO.

“Een informantengesprek netto gaat er allemaal wel in. Als het gaat om vragen van teams over Jantje op een bepaalde locatie. Is dat minder goed. Als je die goed vastlegt, kun je daar soms maanden later op reageren. Dan krijg je hits op subjecten. Je moet er bovenop zitten. Als het gebruiksgemak beter was, dan wordt meer vastgelegd.” – CIE teamleider

6.3 Beleving van de benodigde inspanning bij het gebruik

De mate waarin gemak wordt geassocieerd met gebruik van het systeem (kortweg: gebruiksgemak), geldt als definitie voor de verwachting van de benodigde inspanning of werklast. In relatie tot dit construct, wordt in dit onderzoek specifiek aandacht gegeven aan de achtergrond van verschillende korpsen op twee punten:

1. de mate waarin de bestaande werkprocessen van een korps aansluiten bij de nieuwe ICT-basisvoorzieningen, en
2. de afstand van de nieuwe voorzieningen tot de oude systemen.

Zowel korpsen die met Octopus hebben gewerkt als korpsen die met het Recherche Basis Systeem (RBS) hebben gewerkt, werden onderzocht.

Hoe wordt het gebruiksgemak beleefd?

Vier van de vijf informanten zijn het helemaal oneens met de stelling: Ik ben beter bereid om informatie in te voeren in BVO door het gebruiksgemak van BVO. De vijfde informant is het met deze stelling eens en vindt de klachten over gebruiksmak “onzin”. De informanten zijn ontevreden over het gebruiksgemak van BVO, vooral als het gaat om de invoer. Ze klagten over de volgende punten:

- BVO is lastig om in te leren werken. Er is veel kennis van de “truckjes” nodig en mogelijkheden om snel te zoeken bijvoorbeeld, blijven daardoor onbenut.
- BVO zit niet logisch in elkaar.
- Er zijn veel (naar de stand van de computertechniek overbodige) handelingen nodig.
- De ontbrekende koppeling tussen BVH en BVO. Hierdoor moet veel informatie dubbel worden ingevoerd, wat de informanten nog wel het vervelendst schijnen te vinden.

Het effect van de ontevredenheid over gebruiksgemak op de bereidheid om informatie in te voeren is duidelijk aanwezig. Het invoeren van gegevens in BVO wordt regelmatig om deze reden vermeden.

“In RBS [Recherche Basis Systeem] kon je veel makkelijker werken dan in BVO. Hetzelfde geldt voor BPS [Basis Processen Systeem] en BVO. We werkten al zoveel jaren met BPS dat je de handelingen weet. (...) Nu mis je informatie in BVH, die we vroeger wel in BPS invoerden. We proberen wel in BVH te gaan werken. Verklaringen die op je eigen recherschijf staan zijn voor anderen niet zichtbaar,

dat is een probleem. Maar het is te gebruiksonvriendelijk en door het niet dagelijks te doen, wen je er niet aan. (...) Onze afhandelunit doet de kleinere zaken, wij draaien de grotere onderzoeken van vier tot acht weken. Maar we zitten niet dagelijks verdachten en getuigen te horen.” – Senior tactisch coördinator districtsrecherche

Routine en opleiding zijn erg van belang stellen diverse informanten. Voor een districtsrechercheur is deelname in een Team Grootschalige Opsporing nuttig, zowel omdat het nut van BVO dan beter wordt ingezien en routine kan worden opgebouwd. Ook denken informanten dat een aanvullende opleiding nuttig kan zijn. Om de kennis op te halen, maar ook om die uit te breiden (in een follow-up). Diverse informanten kennen niet alle mogelijkheden en tijdsbesparende ‘truckjes’ in BVO.

“Er wordt dan wel een cursusdag gegeven door iemand die daar heel handig mee is. Een half jaar of een jaar verder, wordt het ingevoerd en is de kennis niet meer aanwezig.” – Senior tactisch coördinator districtsrecherche

Het probleem voor de CIE is de zoekfunctie in BVO en juist niet de invoer:

“Het gebruiksgemak is 0,0. Bij de invoer valt het nog wel mee. Het zoeken en terugvinden is niet goed. (...) Als een journaal opgemaakt is gaat het naar mij of naar de projectleider. Zij zetten in de onderwerpregel ../. als ze klaar zijn. Als ze bezig zijn staat er ///. Als ik het nagekeken heb staat er FG/... Als ik moet weten welke nagekeken moeten worden, zoek ik op ../. en dan krijg ik er honderden. Ook waar mijn initialen voor staan. Hij zoekt dus niet goed. Als je twee keer zoekt krijg je verschillende resultaten. Als men zoekt op een naam is het vertrouwen weg dat je ook alles vindt. Je gaat op tekst zoeken en op andere manieren. Zo sprokkel je informatie bij elkaar. Nu kost het veel meer tijd.” – Coach bij de CIE*

Aansluiting van de werkprocessen op BVO

Over de aansluiting van de werkprocessen zijn de meningen verdeeld. Echter geven de informanten die ontevreden zijn met de aansluiting van het werkproces van hun korps bij BVO, de doorslag (3). Slechts één informant is het eens met de stelling (1 neutraal): De werkprocessen van mijn korps sluiten goed aan op BVO, waardoor hier goed mee gewerkt kan worden. De komst van BVO bepaalt volgens enkele informanten wel de richting van de manier waarop gewerkt

wordt. Echter volgens geen van de informanten is de aansluiting op dit moment optimaal.

“Het systeem brengt een eenheid van werken met zich me, zodat ook het overzicht wordt gehouden in onderzoeken. Maar in het gebruiksgemak moet nog veel gebeuren.” – Senior tactisch coördinator districtsrecherche

“Als [de werkprocessen] wel zouden aansluiten, zou je sneller van BVO gebruik maken. Het nodigt niet uit om met BVO te gaan werken.” – Senior tactisch coördinator districtsrecherche

In de praktijk kan een zaak gedraaid en afgerond worden zonder dat invoer in BVO daarvoor noodzakelijk is. Het dossier kan worden aangeleverd bij Justitie. In ieder geval in één van de onderzochte korpsen vormt hierop een uitzondering: Een MRO [Melding Recherche Onderzoek] is daar noodzakelijk om informatie te kunnen opvragen bij de infodesk. Er is sturing vanuit het korps en de teamleiding nodig om de invoer in BVO en het delen van informatie op gang te brengen. Zoals eerder gesteld past het werkproces van een projectmatig onderzoek over het algemeen beter bij het werken in BVO dan een kleiner onderzoek aan het district, omdat het dan een handig middel is om overzicht te houden.

Ook van de andere kant, bij het zoeken naar informatie, sluit de manier van werken niet altijd aan bij de inrichting van de informatievoorziening. Een informant wees in dit verband op de huidige toegankelijkheid van BlueView.

“Het delen van informatie is ontzettend beperkt, dat houdt op bij de regio. Er is bepaald dat alleen de informatieafdeling BlueView mag gebruiken om over de informatie heen te kijken. Iemand van de financiële recherche moet eerst naar de informatieafdeling om te kijken of een fraudezaak ook elders voorkomt. Heel veel mensen haken daardoor af en nemen niet de moeite om verder te kijken.” – Hoofd recherche expertise (namens Hoofd informatie en opsporing)

Aansluiting van het voormalige informatiesysteem op BVO

Zoals eerder aangegeven is BVO gebaseerd één van de voormalige informatiesystemen waarmee de opsporing werkte: het Recherche Basis Systeem (RBS). Het andere heet Octopus.

Het voormalige informatiesysteem waarmee in een korps werd gewerkt, is geen goede voorspeller voor de bereidheid om informatie in te voeren. De voorgelegde stelling luidt: Het oude informatiesysteem voor de recherchefunctie van mijn korps, verschilt zodanig van BVO dat het erg moeilijk is hiermee te leren werken. BVO is gebaseerd op RBS. De enige voorstander van de stelling, voorheen een gebruiker van dat systeem, zou juist minder moeite moeten hebben gehad om BVO onder de knie te krijgen. Echter omdat het een medewerker van de districtsrecherche betrof, was dit afwijkende antwoord verklaarbaar. Vele districtsrechercheurs werkten voorheen niet in RBS.

“We draaiden alles met BPS [Basis Politie Systeem]. Als je een groter onderzoek kreeg, een TGO of een RBT [Regionaal Bijstandsteam], dan werkte men in RBS [Recherche Basis Systeem]. Formulieren, verklaringen en aangiften nam ik vroeger allemaal op in BPS. Kleine dossiers, met bijv. een aangifte en twee verklaringen konden daar ook makkelijk in worden opgemaakt. Grotere onderzoeken, met een ambtelijk verslag, werden in MS-Word opgemaakt. Informatie uit BPS werd erachter gezet [voor het dossier].” – Senior tactisch coördinator districtsrecherche

Eén van de beide gebruikers van het meer afwijkende Octopus was het niet eens met de stelling en de ander stond neutraal tegenover de stelling. De overige twee voormalige RBS gebruikers waren het geheel niet eens met de stelling. Kortom: vanuit beide beginsituaties kan het mee- en tegenvallen om met BVO te werken. Eén informant kende beide systemen en was van mening dat BVO elementen bevat van beide voorgangers.

6.4 Sociale beïnvloeding

Sociale beïnvloeding wordt gedefinieerd als de mate waarin een individu ervaart dat belangrijke anderen van mening zijn dat hij of zij het nieuwe systeem zou moeten gebruiken.

Hoe is de sociale beïnvloeding door collega's en leidinggevenden?

Twee informanten zijn het eens (1 helemaal eens) met de volgende stelling: Collega's en leidinggevenden hebben mij gestimuleerd om opsporingsinformatie in te voeren en landelijk te delen. Twee antwoordden neutraal. Driemaal werd een toelichting gegeven van de volgende strekking: Er is een systeem waarmee gewerkt moet worden. Gestimuleerd wordt het niet, er wordt ook niet gezegd dat je er niet mee mag werken.

Overtuigde gebruikers, bijvoorbeeld districtsrechercheurs die ervaring hebben in een TGO, vinden het moeilijk om anderen te overtuigen maar zijn wel gemotiveerd om dat te doen. Zij krijgen daarnaast veel vragen van collega's maar kunnen het tekort aan kennis vaak niet compenseren. Binnen de CIE, zo werd door een informant opgemerkt, is het werken in BVO de enige manier om volgens de CIE-Regeling te werken.

De sociale beïnvloeding die blijkt uit de interviewgegevens heeft geen duidelijk karakter in de zin dat deze niet positief of negatief van invloed is op de bereidheid van politiemedewerkers om informatie in te voeren. Wel is het opvallend te noemen dat er kennelijk geen in het oog springende beïnvloeding plaatsvindt door de teamleiders, gelet op de recente invoering van de nieuwe basisvoorzieningen.

De overtuiging van de geïnterviewde teamleiders is dat informatiedeling de moeite waard is en zij geven daar vanuit die gedachte ook prioriteit aan. Die opvatting leeft bij de CIE en eveneens bij de teamleiders van de recherche. Verder wordt over een aantal onderwerpen verschillend gedacht. Echter geen van de geïnterviewde teamleiders geeft aan zijn prioriteiten te hebben bijgesteld vanwege problemen met het gebruik, de tijd die gemoeid is met het opvragen van informatie bij de infodesk of de kwaliteit van de informatie die beschikbaar is via BVO en BlueView. Dit beeld is in tegenspraak met de beschrijving die sommige rechercheurs hebben gegeven in hoofdstuk 4: volgens hen zou er op de invoer nauwelijks sturing plaatsvinden.

De geïnterviewde CIE teamleiders denken enigszins verschillend over het gebruiksgemak van BVO. De één vindt het gebruiksgemak bij de invoer verminderd, de ander heeft problemen met de zoekfunctie, maar beide proberen de invoer zoveel mogelijk te bevorderen.

“Ik vind het gebruiksgemak door de schil die erom heen zit achteruit gegaan. Je moet te veel handelingen doen. Ze hebben wel het handje ervan om niet alles vast te leggen. Een informantengesprek netto gaat er wel in. Vragen op tactische teams minder. Als je die goed vastlegt, kun je daar soms maanden later op reageren. Dan krijg je hits op subjecten. Je moet er bovenop zitten. Als het gebruiksgemak beter was, dan wordt meer vastgelegd.” – Teamleider CIE

Over de benodigde tijd voor de invoer, een belangrijke reden om elkaar minder te stimuleren, hebben twee tactische teamleiders verschillende opvattingen.

“Onze afdeling legt alles vast in BVO (...). Heel veel legt de infodesk zelf vast in BVO, dus dat scheelt onze rechercheurs werk.” – Onderzoeksleider TGO, politiekorps IJsselland

“Ik ben er wel bang voor dat de tijd die de invoer kost, mensen demotiveert. (...) Ik kijk alleen naar de journaalmutatie. Hebben ze de informatie met betrekking tot dit onderzoek goed verwerkt? Daar ben ik verantwoordelijk voor.” – Onderzoeksleider TGO, politiekorps Hollands Midden

6.5 Faciliteren van gebruikers

De laatste determinant voor de mate waarin nieuwe ICT wordt geaccepteerd in het bovengenoemde model, is het faciliteren van gebruikers. De mate waarin gebruikers worden gefaciliteerd wordt in het model gedefinieerd als de mate waarin een individu meent dat er een organisatorische en technische infrastructuur bestaat om het gebruik van systemen te ondersteunen. Hierbij moet niet alleen worden gedacht aan ondersteuning door bijvoorbeeld een helpdesk maar ook aan andere randvoorwaarden voor succesvol gebruik: compatibiliteit met andere systemen die door de opsporing worden gebruikt en kennis van de systemen (opleiding). Deze thema's komen achtereenvolgens aan bod in onderstaande beschrijving.

Hoe worden gebruikers gefaciliteerd?

In onderstaand citaat komen diverse thema's uit dit hoofdstuk als het ware bij elkaar. De wijze waarop informanten denken over gebruiksgemak en het uitblijven van een sterke sociale beïnvloeding lijken ook door de in onderstaand citaat genoemde dubbele invoer verklaard te worden. De dubbele invoer is voor researchers een gewichtige reden om onvoldoende invoer te doen. Teamleiders, met name van districtsteams, zien dat soms door de vingers: zij geven geen sturing. Dit thema komt in latere hoofdstukken nader aan de orde.

“Die vrijheid [om informatie niet in te voeren] neem je ook zelf. Je hebt geen keus omdat we de tijd niet hebben. Belangrijk daarbij is dat BVH en BVO niet op elkaar zijn afgestemd, waardoor je een dubbele invoer moet doen.” – Senior tactisch coördinator districtsrecherche

Aansluiting van BVO op andere ICT toepassingen (compatibel)

BVO kan worden toegepast in combinatie met andere ICT systemen die voor de opsporing van belang zijn. Drie informanten waren het niet eens (2) of helemaal niet eens met deze stelling (1). Eén informant was het helemaal eens met de stelling en lichtte toe:

“[BVO kan worden toegepast i.c.m.] onder andere VROS, dat werkt hartstikke goed.” – Analist/kwaliteitscoach recherche

Andere informanten waren eensgezind in hun kritiek. De ontbrekende koppeling met BVH is een belangrijke barrière voor de invoer en uitwisseling van opsporingsinformatie.

“Uit BVH kunnen geen objecten worden overgehaald naar BVO. Er zit geen GBA [Gemeentelijke Basis Administratie] check achter BVO. Het zou ideaal zijn als je een persoon uit één database kan vissen, of ik nu werk met BVO of BVH. (...) Je zit vaak met een dubbele invoer en hebt meer kans op invoerfouten. Dat is bezwaarlijk en kost extra tijd.” – Tactisch coördinator regiorecherche (afdeling ZwaCri)

De CIE kent haar eigen specifieke problemen. Verschillende onderdelen van BVO werken niet prettig in combinatie.

“In de bruto kan ik er helemaal niks mee; niet knippen en plakken. Je kan geen andere applicaties gebruiken in combinatie met BVO.” – Coach bij de CIE

Kennis

Kennis over de mogelijkheden van BVO is bij een drietal informanten te weinig aanwezig, vinden ze zelf. Twee informanten zijn het wel eens met de stelling: Ik heb voldoende kennis van BVO. Er zitten mogelijkheden in BVO waar informanten niet aan toe komen. Niet noodzakelijk door een gebrek aan kennis, maar ook door een gebrek aan tijd. Ook dan speelt onzekerheid over de vraag of de opleiding voldoende is geweest wel een rol.

“Je weet niet wat je niet weet. Ik weet bijvoorbeeld niet of ik op de juiste manier zoek. Ik heb een spoedcursus gehad maar eigenlijk moet je nu een update hebben. Je werkt er nu een tijdje mee, maar ken je handigheidjes ook? Dat kan mensen een hoop tijdwinst en irritatie schelen.” – Coach bij de CIE

Alle informanten zijn het eens met de stelling: Ik heb voldoende kennis om keuzes te maken over het invoeren en landelijk delen van opsporingsinformatie met geautoriseerden. Toch is het ook hier niet alles goud wat er blinkt. Een aantal informanten lijkt te willen aangeven dat zij niet naïef zijn.

“Ik maak een bewuste keuze over welke informatie op straat mag komen te liggen en welke niet.” – Senior tactisch coördinator districtsrecherche

Kennisvermeerdering en beslissingsondersteuning

Informanten denken verschillend over de algemene stelling: Ik kan zo nodig benodigde kennis over BVO gemakkelijk opdoen. Meer specifiek: over beslissingsondersteuning bij keuzes over het delen van informatie zijn de informanten overwegend tevreden. Drie informanten zijn het eens met de stelling: Er is voldoende ondersteuning beschikbaar bij het maken van keuzes over het invoeren en landelijk delen van opsporingsinformatie met geautoriseerden (1 neutraal, 1 mee oneens).

“Dat overleg ik met een collega of leidinggevende. Iemand die met de tactische strategie bezig is. Dan overleg ik: doen we dat wel of niet naar buiten?” – Senior tactisch coördinator districtsrecherche

Een informant die vindt dat benodigde kennis gemakkelijk is op te doen wijst op de rol die een TGO kan spelen en op de rol die collega's vervullen.

“Je wordt er wegwijst in door andere gebruikers, veel meer dan door cursussen of schriftelijk materiaal. Vooral binnen een TGO [Team Grootchalige Opsporing].” – Senior tactisch coördinator districtsrecherche

Voor een team aan het district betekent dat tegelijkertijd dat het lastig kan zijn om de benodigde kennis op te doen. Dat zou ook een verklaring kunnen zijn voor de verschillende opvattingen van informanten.

“Ik kan te weinig terugvallen op mensen die zeggen: Ik weet hoe dat allemaal werkt. Die weten wat je moet invoeren. Een enkeling die ik kan raadplegen.” – Senior tactisch coördinator districtsrecherche

“Er zijn heel veel mails van de BVO guru van de afdeling, waardoor hij moest beginnen met nummers want hij raakte zelf ook de weg kwijt. De wijzigingen waren niet bij te houden. Ze hebben kaartjes gemaakt over hoe je moest invoeren. Die werden vervangen omdat er zoveel op gekrast was. De nieuwe zijn ook alweer bekrast. Er zijn boeken waarin staat hoe het precies moet, maar tijdens je werk kan je niet steeds kijken waar je een streepje en een puntje moet zetten etcetera.” – Coach bij de CIE

6.6 Tussenconclusie: acceptatie van nieuwe systemen is een knelpunt

In dit hoofdstuk stond de vierde deelvraag uit dit onderzoek centraal: *In hoeverre beperkt technologie de uitwisseling van opsporingsinformatie tussen Nederlandse politiekorpsen?* In antwoord op deze vraag werd gekeken in hoeverre het delen van opsporingsinformatie wordt beperkt door factoren ontleend aan het UTAUT model. De volgende conclusies kunnen worden getrokken:

-Uit de interviews blijkt dat prestaties van BVO, in de zin dat het politiewerk door dit systeem wordt ondersteund, de bereidheid van informanten om informatie in te voeren nauwelijks negatief beïnvloeden. Er is tevredenheid over de kwaliteit en de snelheid waarmee (ook via de infodesk) informatie gevonden kan worden. Veel informatie staat niet in BVO opgeslagen. De beschikbaarheid is dus nog beperkt, maar dat is voor informanten geen reden om informatie niet in te voeren.

-Het gebruiksgemak van BVO vormt een drempel voor voldoende invoer van informatie, met name bij de recherche. De CIE kent ook wel problemen met het gebruiksgemak van BVO, echter heeft zij veel minder mogelijkheden om het gebruik ervan te omzeilen. De werkprocessen bij de CIE, zoals ook vereist door de CIE-Regeling, zijn veel meer gericht op het invoeren van informatie in BVO, terwijl de reguliere opsporing de mogelijkheid heeft dossiers op te maken in schaduwsystemen. Voor een verbetering van de situatie verlangen informanten:

- voldoende opleiding;
- minder (overbodige) handelingen;
- sturing, zodat ervaring bij medewerkers kan ontstaan;
- inpassing van BVO in het werkproces.

-De sociale beïnvloeding ten aanzien van het gebruik van BVO heeft geen duidelijk karakter in de zin dat deze niet positief of negatief van invloed is op de bereidheid van politiemedewerkers om informatie in te voeren. Het is opvallend te noemen dat er geen in het oog springende beïnvloeding plaatsvindt door de teamleiders. De geïnterviewde teamleiders zeggen hun prioriteiten niet te hebben bijgesteld vanwege problemen bij het gebruik van BVO.

-Ten aanzien van het faciliteren van gebruikers kan worden geconcludeerd dat zowel het ontbreken van compatibiliteit tussen de geautomatiseerde informatiesystemen die de opsporing gebruikt als een kennisachterstand,

knelpunten vormen voor informatiedeling. Ten aanzien van de compatibiliteit springt de ontbrekende koppeling met BVH [Basisvoorziening Handhaving] in het oog. Hieruit kunnen geen objecten worden overgehaald naar BVO. Ook de GBA [Gemeentelijke Basisadministratie] is niet gekoppeld aan BVO.

Het is algemeen bekend dat politiemensen in toenemende mate klagen over administratieve lastendruk, waardoor zij minder tijd zouden overhouden voor het 'echte' werk. In die situatie is het extra belangrijk om het gebruik van een nieuw systeem met voldoende kennis en opleiding te ondersteunen en te zorgen dat het systeem werkt in combinatie met andere toegepaste systemen, zodat tijdverlies voorkomen wordt. Afgezien van de prestaties van de systemen, is op de andere determinanten van het UTAUT model steeds sprake van knelpunten in de onderzochte korpsen. De belangrijkste die acceptatie van de nieuwe ICT in de weg staan zijn het gebruiksgemak en het faciliteren van gebruikers. Deze problemen zorgen er bij rechercheurs voor dat er minder informatie wordt ingevoerd in BVO. Op de prioriteiten van teamleiders lijken de problemen minder sterk van invloed.

Kijkend naar het verklaringsschema uit hoofdstuk 2, werd in het vorige hoofdstuk duidelijk dat juridische omstandigheden nauwelijks een beperkende invloed hebben op de informatie-uitwisseling bij de politie in de Nederlandse situatie. Uit dit hoofdstuk blijkt dat de technologische omstandigheden, de informatie-uitwisseling wel in belangrijke mate beperken. Het UTUAT verklaringsmodel blijkt zeer goed toepasbaar op de problematiek van de beperkte informatie-uitwisseling bij de politie.

Hierop moet worden aangevuld dat een verbetering van de techniek op zichzelf het probleem niet geheel zou oplossen. Een vergroting van het gebruiksgemak en het aanbrengen van koppelingen tussen BVO en onder meer BVH, kan niet verhelen dat het invoeren van opsporingsinformatie in de ogen van rechercheurs niet tot de primaire werkprocessen behoren. Aanvullende opleidingen kunnen helpen techniek en organisatie beter bij elkaar te laten aansluiten, maar ook is meer sturing van de teamleiders nodig. Met die conclusie bevinden we ons langzamerhand op het terrein van de organisatorische omstandigheden voor informatie-uitwisseling. Informatie delen is niet alleen een kwestie van kunnen in juridische en technische termen, maar evenzeer een kwestie van willen. Beperkende omstandigheden kunnen met een extra inspanning vaak best overwonnen worden. Dat geldt zeker voor technologische omstandigheden. Maar ook indien er geen harde barrières zijn, wordt in

sommige gevallen geweigerd informatie in te voeren of om informatie na persoonlijk contact met een teamleider van een ander korps te delen. De organisatorische omstandigheden voor informatiedeling staan centraal in de laatste twee hoofdstukken voor de conclusie.

7. Organisatorische omstandigheden: kunnen én willen delen

In hoofdstukken 7 en 8 wordt de vijfde deelvraag uit de inleiding van een antwoord voorzien: *In hoeverre beperken organisatorische omstandigheden de uitwisseling van opsporingsinformatie tussen Nederlandse politiekorpsen?*

Omwille van de overzichtelijkheid worden verschillende thema's onder deelvraag V in aparte hoofdstukken behandeld. In hoofdstuk 8 ligt de nadruk op een thema dat wordt geïntroduceerd met het werk van Peter K. Manning: de gevolgen van de aard van het politiewerk voor hoe binnen de organisatie met informatie-uitwisseling wordt omgegaan. Dit hoofdstuk 7 gaat in op de specifieke sturingskenmerken van de politieorganisatie vanuit de optiek van Yeheskel Hasenfeld. Eigenlijk laten beide auteurs zien hoe lastig het is om de politieorganisatie te sturen. Hasenfeld kijkt daarbij voornamelijk naar de kenmerken van de organisatie, Manning naar de kenmerken van het werk dat gedaan moet worden.

In dit hoofdstuk zal de politie worden beschouwd als een *Human Service Organisation*, een organisatietype dat als zodanig door Hasenfeld werd gedefinieerd. Hasenfeld heeft geprobeerd de specifieke karakteristieken van organisaties die werken met mensen, zoals onder meer de politie, te beschrijven en noemde deze categorie *Human Service Organisations* (HSO's).¹ Dit begrip komt verder aan de orde in paragraaf 7.1.

Zoals aangegeven wordt in dit hoofdstuk ingegaan op sturingskenmerken van de politieorganisatie, zoals ambigue, vage, en tegenstrijdige doelen en een bemoeizuchtige, turbulente omgeving. Gekeken wordt in hoeverre deze kenmerken, zoals ook aangegeven in het verklaringsschema uit hoofdstuk 2, een verklaring vormen voor beperkingen in de informatie-uitwisseling tussen Nederlandse politiekorpsen.

Aan informanten op strategisch, tactisch en operationeel niveau zijn vragen gesteld over sturing op de invoer en het delen van informatie (7.2). Met informanten op strategisch niveau is in het bijzonder ingegaan op de relatie van politiekorpsen met hun omgeving en in verband daarmee, op organisatiedoelen en evaluatiecriteria waar korpsen mee te maken hebben (7.3).

¹ Hasenfeld (1983)

7.1 De politie als *Human Service Organisation*

In de moderne samenleving wordt de gehele levenscyclus van burgers, van wieg tot graf, beïnvloed en gevormd door formele (overheids)organisaties. Hasenfeld duidt een bijzondere categorie van deze organisaties aan, namelijk de *Human Service Organisations*. De primaire functie van dit soort organisaties is het beschermen, behouden en verhogen van het welzijn van mensen door het definiëren, vormgeven en wijzigen van hun persoonlijke eigenschappen. Heel algemeen genomen, kunnen dit soort organisaties worden onderscheiden van andere bureaucratische organisaties door twee kenmerken. Ten eerste werken zij in direct contact met de mensen wier eigenschappen ze proberen te vormen. Ten tweede, verkrijgen ze hun mandaat door het welzijn te bevorderen van de mensen die zij dienen. De relatie tussen burgers en, wat we kunnen noemen 'de welvaartsstaat', komt tot stand via *Human Service Organisations*. Deze registreren en reageren op claims van burgers.²

Human service organisations hebben onder meer tot taak, het resocialiseren van individuen die zich niet conformeren aan hun maatschappelijke rollen. Bij uitstek een rol die door de politie wordt vervuld, zelfs in een frontlijnpositie. Echter behalve de politie houden bijvoorbeeld ook scholen, ziekenhuizen, penitentiare en psychiatrische instellingen zich bezig met het socialiseren en resocialiseren van mensen. Het zijn ook *Human Service Organisations* die groepen mensen in staat stellen om zich sociaal (beter) te integreren. HSO's kunnen, om het samen te vatten, worden ingedeeld aan de hand van het type cliënten dat ze dienen en het soort technieken en procedures die ze gebruiken om veranderingen bij hun cliënten te bewerkstelligen.

Het publiek maken van behoeften en problemen is binnen de welvaartsstaat van de 20^e eeuw voldoende om aanspraak te maken op diensten van de overheid die essentieel zijn voor het welzijn. De mogelijkheid van (financiële) bijstand was daardoor niet langer afhankelijk van sociale klasse. Het waren de *Human service organisations* die de controlefunctie van de familie grotendeels overnamen. Tegelijkertijd, moeten burgers een flink stuk van hun privéleven blootgeven aan de gebureaucratiseerde samenleving. Ze krijgen een publieke identiteit op basis van behoeften en omstandigheden, zoals die worden geïnterpreteerd vanuit het bureaucratische systeem. Deze identiteiten hebben invloed op de sociale status van het individu. Als iemand zich wendt naar een *Human Service Organisation*, krijgt de laatste een zekere invloed over het leven van deze persoon. Invloed andersom, op het beleid van de organisatie, is er

² Hasenfeld (1983), pp. 1-2

nauwelijks en daarbij is de burger in de meeste gevallen gedwongen van *Human Service Organisations* gebruik te maken.³

Belangrijk voor het onderwerp van dit onderzoek is hoe HSO's functioneren. Hasenfeld wijst erop dat onderzoek naar organisatiestructuren uitwijst dat om de efficiency en effectiviteit van organisaties te kunnen verbeteren, een rationele en contingente organisatiestructuur moet worden gebouwd die beantwoordt aan de geschiedenis, de grootte, de omgeving van de organisatie en de daarin toegepaste technieken. Volgens Hasenfeld zijn deze uitgangspunten onomstreden maar kunnen ze niet zonder meer worden toegepast op de HSO.⁴

In de eerste plaats hebben HSO's volgens Hasenfeld te maken met turbulente omgevingen die worden gekenmerkt door meervoudige en veranderende belangengroepen, met verschillende en vaak onverenigbare waarden. Een organisatie die reageert op deze groepen, krijgt daardoor te maken met waarschijnlijk meerdere, vaak tegenstrijdige, doelstellingen die haar vermogen een rationele interne structuur op te bouwen, sterk inperken.

Ten tweede zijn binnen een HSO taken en activiteiten vaak slecht omschreven. Specificaties en definities verschillen tussen organisaties onderling en tussen medewerkers van een HSO. Daardoor kan de interne structuur van een HSO niet gemakkelijk worden geleid op basis van een technische blauwdruk. Want deze is onderworpen aan de ideologische grillen van de professionals die uiteindelijk zelf beslissingen nemen, omdat zij het werk met de mensen doen. De technieken die daarbij worden toegepast creëren moeilijkheden bij het toezicht en de evaluatie van prestaties van het personeel en de output. Deze ontstaan gedeeltelijk uit de vaagheid die aan deze technieken kleeft, de complexiteit van menselijke eigenschappen, het beperkte zicht op activiteiten van het personeel en de beperkte meetbaarheid van de output.⁵

Tot slot, vormen volgens Hasenfeld het contact tussen personeel en cliënten een probleem voor een consequente toepassing van beleidsregels binnen een HSO.⁶ De activiteiten van de organisatie komen in de bedoelde situatie voort uit de werkzaamheden die het uitvoerende niveau onderneemt met cliënten, meer dan via richtlijnen uit de formele commando structuur. De processen die nodig zijn om in individuele situaties juist op te treden, kunnen vooraf meestal niet worden beschreven.⁷ Iedere relatie wordt beïnvloed door

³ Hasenfeld (1983), pp. 3-4

⁴ *Idem*, p. 149

⁵ *Ibidem*

⁶ *Ibidem*

⁷ Hasenfeld (1983), p. 156

zijn eigen context; door de belangen van de betrokken partijen, de achtergronden voor de interactie en door de duur van het contact. Daardoor is er geen garantie dat relaties volgens een vast patroon verlopen.⁸ Gegeven de centraal staande relaties, zijn er volgens Hasenfeld vijf redenen voor het eerder genoemde slechte mogelijkheden voor een effectieve monitoring binnen een HSO. De relaties tussen personeel en cliënt zijn beperkt observeerbaar omdat (1) de vertrouwelijkheid van informatie die hierbij wordt uitgewisseld in het geding is; (2) de overtuiging van medewerkers dat vertrouwen tussen hen en de klant nadelig wordt beïnvloed door externe inmenging; (3) het ontbreken van betrouwbare en valide prestatiecriteria van de medewerkers kan leiden tot een vluchtig gebruik van het toezichthoudende instrument met mogelijk ernstige conflicten over de interpretatie van waarnemingen tot gevolg; (4) de kosten van de directe controle van personeel-client relaties zijn buitengewoon hoog, omdat de organisatie hier niet volledig op kan anticiperen en een toezicht is vereist met substantiële inzet van personeel en tijd, en (5) in het geval dat medewerkers als professionals kunnen worden getypeerd, wordt rechtstreekse controle gezien als iets waarmee vakbekwaamheid in twijfel wordt getrokken en als een inperking van de professionele autonomie.⁹

Bovenstaande kenmerken van het functioneren van een HSO betekenen volgens Hasenfeld onder meer dat de informatie over de relatie tussen cliënten en het uitvoerende personeel door de uitvoerders kan worden beïnvloed. Uitvoerders bepalen welke informatie de organisatie in wordt gestuurd en andersom, welke informatie over de organisatie bij de cliënt komt. Hasenfeld past zijn verhaal over de sturingskenmerken ook toe op het opsporingswerk van de politie: Hoewel politiemensen opdrachten krijgen over wat er onderzocht moet worden, hebben zij veel ruimte om te beslissen hoe het onderzoek uitgevoerd moet worden en hoe met de betrokken informatie omgegaan wordt. Deze ruimte ontstaat doordat uitvoerende politiemensen effectief kunnen controleren welke informatie binnenkomt ter ondersteuning van beslissingen die het uiteindelijke onderzoek bepalen.¹⁰ De sturingskenmerken van de politie-organisatie zijn dus zodanig dat er voor een effectieve sturing van informatiebeleid, vanuit de commando-structuur, diverse hindernissen genomen moeten worden. De beschrijving van de sturingskenmerken van de HSO wordt in onderstaande subsectie nog wat verder uitgewerkt.

⁸ *Idem*, p. 157

⁹ *Idem*, pp. 156-157

¹⁰ *Idem*, p. 157

7.1.1 “Loosely coupled systems” en “street level bureaucrats”

Het organisatieschema van een school, ziekenhuis of een instelling voor geestelijke gezondheidszorg geeft een beeld van rationaliteit, orde en coördinatie. Eenheden en afdelingen lijken actief te zijn in rationeel afgebakende domeinen; sturingslijnen lijken eenduidig ingetekend en de verschillende organisatiedelen lijken geïntegreerd in een functionerend geheel. Echter uit empirische studies van dergelijke HSO's ontstaat een ander beeld. Studies laten zien dat "organisatiedelen slechts losjes met elkaar verbonden zijn en aan de activiteiten van de organisatie; regels worden vaak overtreden, besluiten worden vaak niet uitgevoerd, en indien geïmplementeerd hebben deze onzekere gevolgen; toegepaste technieken zijn niet efficiënt genoeg en evaluatie-instrumenten worden misbruikt of zijn zo vaag geworden dat ze nog maar weinig coördinatie kunnen bieden."¹¹

Een betere beschrijving van de interne structuur van een HSO is volgens Hasenfeld die van een *loosely coupled system*, waarin organisatiedelen elk een grote zelfstandigheid hebben. Deze reageren weinig op elkaar en als het gebeurt, is dat vaak langzaam en zonder grote gevolgen.¹² Samenvattend is belangrijk om te weten dat het lastig is binnen HSO's centraal beleid te voeren aangezien deze worden gekenmerkt door *loosely coupled systems*.

Er is echter wel een verklaring voor de ontkoppeling tussen de diverse organisatiedelen in een HSO. Los van elkaar kunnen ze op veranderingen en ontwikkelingen in de omgeving reageren, zonder daarbij in toom te worden gehouden door anderen. Het stelt de organisatie in staat om te gaan met slecht gedefinieerde of slecht definieerbare technieken. Verder is de organisatie als geheel minder kwetsbaar voor het falen van een onderdeel. De losse koppeling maakt ook dat tegemoet kan worden gekomen aan conflicten tussen medewerkers met tegengestelde meningen en de professionele autonomie wordt erdoor vergroot.¹³

Deze professionele autonomie, kenmerkend voor de uitvoerders onderin een HSO, wordt door Hasenfeld nader beschouwd. Door de relaties tussen personeel en cliënt, hebben uitvoerende medewerkers een aanzienlijke discretionaire ruimte nodig die de eenheid van de organisatie belemmert. Smith introduceerde

¹¹ Meyer, J. en B. Rowan (1977), *Institutionalized Organizations: Formal Structure as Myth and Ceremony*, American Journal of Sociology 83, p. 343

¹² Idem, p. 150

¹³ Idem, p. 158

in 1965 de "*front-line*" organisatiestructuur als concept. In een dergelijke structuur zijn de uitvoerders vrij autonoom van de rest van de organisatie, de onderlinge afhankelijkheid voor het verrichten van taken is laag tussen werkeenheden en er zijn aanzienlijke belemmeringen voor een effectief toezicht.¹⁴ Aan deze notie werd door Lipsky in 1980 toegevoegd dat binnen een HSO de dagelijkse verantwoordelijkheid voor de interactie met klanten door het lagere personeel wordt gedragen en hij noemde dit type medewerkers *street level bureaucrats*. Ondanks hun lage positie in de formele gezagsstructuur, hebben *street level bureaucrats* een aanzienlijke discretionaire ruimte, aangezien ze werken in situaties die te complex zijn voor routines; ze werken in situaties bepaald door variabele en menselijke omstandigheden. Ze maken gebruik van hun discretionaire ruimte om hun relatieve autonomie te handhaven en om hun eigen belangen, die vaak verschillen van die van hun superieuren, te bevorderen. Deze verschillen vloeien volgens Hasenfeld voort uit het feit dat *street level bureaucrats* moeten functioneren in een context en onder omstandigheden die zelden worden gedekt door beleid. *Street level bureaucrats* hebben te maken met diverse organisatorische doelen en divers beleid; zoals eerder gesteld met onvoorspelbaar gedrag van cliënten; een vraag die de mogelijkheden en middelen van de organisatie overstijgen en bovendien met overvloedig administratief werk. Alles bij elkaar stelt Hasenfeld, hebben zij behoefte om te gidsen op hun eigen persoonlijke en professionele ideeën en door gebruik te maken van de ruimte die ze hebben, kunnen *street level bureaucrats* de dilemma's waarmee ze te maken hebben in hun dagelijkse bestaan, gedeeltelijk oplossen.¹⁵

Deze nadere uitwerking van de optiek van Hasenfeld op wat hij noemde de *Human Service Organisations*, maakt duidelijk hoezeer deze invalshoek op de politiek van toepassing is. In paragraaf 7.2 worden de beschreven theoretische inzichten verder toegepast op het probleem van de beperkte informatiedeling tussen politiekorpsen.

¹⁴ Idem, p. 157

¹⁵ Idem, pp. 157-158

7.2 De sturing op informatiedeling op korps- en teamniveau

Een centraal staand thema in Hasenfeld's beschrijving van de HSO zijn de *loosely coupled systems*. Zoals eerder aangegeven is het in een organisatie die hierdoor wordt gekenmerkt bijzonder lastig om een centraal beleid te voeren. Eigen initiatieven van de uitvoerders, ofwel de *street level bureaucrats*, zorgen ervoor dat deze beperkt onder controle zijn te houden binnen een formele structuur.

Gelet op voorgaande theorievorming lijkt het voor de hand liggend dat beslissingen op de werkvloer – bij de tactische leiders van opsporingsonderzoeken omtrent het delen van informatie en bij gewone rechercheurs vooral omtrent de invoer van informatie – moeilijk gestuurd kunnen worden. In onderstaande wordt een beschrijving van deze sturingsprocessen gegeven in de vijf onderzochte korpsen. Aan teamleiders en aan het strategische niveau is gevraagd of en zo ja, waarom zij moeite hebben om de invoer van informatie in BVO en het landelijk delen van informatie, te sturen. Bij deze beschrijving worden sturing op de invoer van informatie en sturing op het delen van informatie apart behandeld.

7.2.1 Sturing op de invoer

Eerder werd in deze rapportage aangegeven hoe de invoer van opsporingsinformatie is ingericht en hoe deze in de praktijk verloopt. In deze subsectie wordt ingegaan op de sturing hierop. We hebben gezien dat de mate waarin informatie wordt ingevoerd kan verschillen van team tot team. Onderstaand citaat laat zien hoe deze verschillen tot stand komen.

“We hebben daar afspraken over met de coördinatoren onderling en met de teamleiding. Als er een zaak is, die twee a drie dagen duurt dan maken we niets aan. Als we een langer onderzoek hebben waarin BOB middelen worden gebruikt, als we bijvoorbeeld gaan tappen, dan maken we een MRO aan. Daar blijft het bij.” – Tactisch coördinator districtsrecherche

De teamleider kan de invoer van alle rechercheurs in zijn team inzien. De beperking van de invoer door rechercheurs is daardoor afhankelijk van de ruimte die de teamleider daarvoor geeft. Diverse informanten hebben opgemerkt dat teamleiders van de districtsrecherche minder prioriteit geven aan invoer van informatie, dan teamleiders van een Team Grootschalige Opsporing. Teamleiders hebben bij de sturing op de invoer verschillende posities. Geïnterviewde districtsrechercheurs met ervaring in een TGO geven aan dat er binnen districten minder wordt toegezien op de invoer in BVO. Via de uitgezette opdrachten en

wat er op zijn afdeling leeft, is een teamleider in een projectmatig of TGO-onderzoek vrij goed op de hoogte van wat in de BVO invoer naar voren zou moeten komen. Echter, ook binnen een TGO kan een teamleider niet iedere keuze die een rechercheur bij de invoer maakt beheersen, hoewel hij meer tot in detail op de hoogte is van informatie die ingevoerd kan worden.

De teamleider bij de districtsrecherche is niet volledig betrokken in het verloop van ieder onderzoek. De afstand tussen de rechercheur en een teamleider binnen een team van de districtsrecherche is groter. Bij een teamleider aan een district is het zicht op de bij een onderzoek betrokken informatie minder, waardoor met name districtsrechercheurs een ruime mate van zelfstandigheid bij de invoer van opsporingsinformatie hebben.

“Volgens mij is [de autonomie van rechercheurs bij beslissingen over de invoer en het delen van informatie] vrij groot. Ik kan dat niet kwantificeren. Er is wel een verschil tussen de districtsrecherche en de recherche op regioniveau. Projectmatige onderzoeken worden strak gestuurd. Een rechercheur aan een district die een aantal zaken in portefeuille heeft bespreekt dat wel met een coördinator, maar is autonoom bezig met het oplossen van zaken.” – Directeur opsporing

“Alle namen, afspraken, verklaringen, achtergronden worden in BVO gezet. Niet relevant is een praatje pot. (...) Ik draai een onderzoek en dan lees ik alles wat in BVO staat en als ik dingen mis dan doe ik navraag. Daarnaast hebben we de afspraak dat naast het vastleggen van de verrichte opsporingshandelingen in proces verbaal, we alles in BVO muteren. Dat zijn we vanaf de voorloper van BVO al gewend. (...) Stel dat van de tien vragen aan een getuige maar acht op papier worden gezet, dan weet ik niet wat er met de andere twee gebeurt. We hebben met zijn allen niets aan informatie die iemand heeft gehoord, als we het niet vastleggen. Dat begint ook tussen de oren te komen. Ik spreek voor de onderzoeken die we hier draaien; TGO's. Moord, doodslag etc.. Dat zit strak geregistreerd in elkaar. In principe weten we al wat een rechercheur gaat doen want daarvoor heeft hij opdracht gekregen. (...) Een rechercheur kan niet doen wat hem gezegd is en wat in zijn hoofd zit, niet op papier zetten. Theoretisch is dat mogelijk, maar dat is te verwaarlozen.” – TGO teamleider

“Bij de invoer hebben [rechercheurs] bijna 100% autonomie, hoewel het wordt nagelezen door de teamleider. (...) Het is heel veel werk om dat 100% te sturen. Je

zou er iemand aan moeten zetten om dat te lezen en te controleren en dat gebeurt niet.” – Hoofd recherche expertise, namens Hoofd informatie en opsporing

Op de mate van sturing door de teamleiders van de districtsrecherche lijkt verder van invloed te zijn dat hun mensen meer met belemmeringen in het gebruik te maken hebben bij de invoer van informatie in BVO, dan collega's in projectmatige onderzoeken: er wordt meer door de vingers gezien. Op deze belemmeringen wordt nader ingegaan in de volgende paragrafen. Voor nu is het goed om op te merken dat sturing, zoals in bovenstaand citaat wordt aangegeven, veel werk is. Zeker wanneer rechercheurs met beperkingen zitten waardoor ze niet goed in staat zijn om de invoer (goed) te doen, zijn begeleiding en afspraken nodig.

De sturing op korpsniveau is vooral gericht op het aanmelden van de MRO's. Tijdens de interviews keerde dit onderwerp steeds terug; andere sturingsmiddelen veel minder. Gezien een aantal omstandigheden is het noodzakelijk bij het managen van de informatiehuishouding deze focus aan te brengen.

“Managementtechnisch missen we een aantal truckjes die we konden (...) in BPS [Basis Processen Systeem]. Die moeten we weer terug veroveren. We kunnen minder zien wat er aan invoer wordt gepleegd, maar dat is een tijdelijk probleem. Je hebt ook duidelijke afspraken nodig. Daar zit een knelpunt: dat kun je niet over de hele linie doen omdat daar managementtechnisch te weinig tijd voor is. BVH [Basisvoorziening Handhaving] geeft zoveel problematiek, dat we gefixeerd zijn dat goed te laten verlopen.” – Directeur opsporing

Als onderzoek stelselmatig niet wordt aangemeld, is dat onderwerp van gesprek in functioneringsgesprekken, in twee van de onderzochte korpsen. De ondernemingsraad van één van deze twee korpsen verzet zich tegen deze gang van zaken.

“Ik snap [de ondernemingsraad] wel voor een deel. Waar ze een beetje bang voor zijn is dat wij zullen zeggen: politieagent x registreert twee keer zoveel als y, dan werkt x beter dan y. Je moet ook kijken naar de kwaliteit van de invoer en wie van een koppel toevallig veel heeft ingevoerd. Los daarvan, het is natuurlijk wel een indicatie.” – Directeur opsporing

In één van de onderzochte korpsen heeft de directeur opsporing de volgende maatregel ingevoerd: Zonder MRO registratie geeft de infodesk geen informatie over het betreffende onderzoek.

“Een rechtstreekse maatregel van mij om af te dwingen dat zoveel mogelijk MRO's worden gemaakt. Dan gaat het niet alleen om de vraag of men informatie wil delen, maar ook om de bereidheid een aantal administratieve handelingen te verrichten in BVO. (...) De gemiddelde rechercheur wil zijn eigen zaak rondmaken en wil wel putten uit de informatie maar heeft niet meteen de wil om extra toe te voegen. Dat scoort voor hem geen productie. (...) Soms is het helemaal niet controleerbaar. Als het al controleerbaar is dan zitten mijn tactische mensen, ook ikzelf, daar te weinig op.” – Directeur opsporing

Tot slot kunnen ook binnen de CIE keuzes worden gemaakt als het gaat om de sturing op de invoer van informatie. Informatie delen via processen verbaal, het produceren van operationeel bruikbare informatie is de bestaansreden van de CIE. Vanwege zorgen omtrent de veiligheidseisen komt het voor dat informatie niet in de BVO bruto (het CIE gedeelte van BVO) wordt ingevoerd. Het hoeft niet zo te zijn dat een verstrekking d.m.v. een proces verbaal hierdoor wordt gefrustreerd. Volgens de informanten is op de informatiedeling vooral de kwaliteit van de invoer van invloed.

“Kwaliteit daar gaat het om. Als je een goede kwaliteit bruto gespreksverslagen hebt, dan kan je daar heel goede netto's uit produceren. De één regel tips, daar hebben we net niks aan. (...) Je kan sturen op de kwaliteit. Je kan kiezen of je tweehonderd informanten per jaar wilt hebben, of dat je er tien goed doet. Ik kies liever voor tien goede en dat wat eruit gaat ook van een hoogwaardige kwaliteit is. (...) Uit onderzoek bleek dat op [deze vestiging] het percentage verstrekte informatie en processen verbaal bijna gelijk was. De verstrekte informatie is ook allemaal geverbaliseerd. Bij anderen was er vijf keer zoveel informatie, maar werd er veel minder geverbaliseerd. De doelstelling is om zoveel mogelijk informatie operationeel bruikbaar naar tactiek te krijgen.” – Teamleider CIE

Als een runner informatie niet verwerkt in gespreksverslagen die hij wel weet, heeft dat gegeven de aard van het werk en gezien het werkproces binnen de CIE, mogelijk grote gevolgen voor het vertrouwen in zijn functioneren. Vergelijk dat

met de invoer van een districtsrechercheur, waardoor hij zijn informatie deelt. Hij zal vaak min of meer zelfstandig zijn onderzoeken doen en wanneer hij zijn informatie te weinig deelt, levert dat niet per se een vertrouwensbreuk op met zijn teamleider.

“Wij werken op basis van vertrouwen. Als een runner mij niet alles vertelt, is dat hetzelfde als je ontslag tekenen. Ik mag er niet door verrast raken in ieder geval. Er komt natuurlijk heel veel informatie binnen.” – Teamleider CIE

7.2.2 Sturing op het delen van informatie

De technische managementtools van de korpsleiding zijn, zoals bleek uit de vorige subsectie, nog in ontwikkeling en zijn gericht op de invoer van de informatie. Daarbij is er op strategisch niveau ten tijde van het onderzoek vooral aandacht voor het wekken van vertrouwen bij de medewerkers.

“Het is niet zo dat mensen niet willen delen, omdat ze vinden dat anderen het niet mogen weten. Ze vinden het ook lastig om te delen omdat ze te weinig vertrouwen hebben dat het systeem goed functioneert en er is zorg of mijn collega's elders op de juiste manier om zullen gaan met de informatie. Dat onbedoeld de verkeerde mensen geautoriseerd zijn. Dat kan bijvoorbeeld zitten in de functioneel beheerders. Zij beheren de applicaties. Bij ons waren de functioneel beheerders toebedeeld aan de diensten en nu hebben we dat gecentraliseerd. Dat betekent dat mensen zich er van willen vergewissen of informatie op de goede manier wordt beheerd en dat niet iedereen, dat bijvoorbeeld niet de functioneel beheerders in alle onderzoeken kunnen kijken. We leggen dan ook uit, aan rechercheurs, hoe we dat nu hebben georganiseerd. Het is niet zo dat alle functioneel beheerders, alle rechercheonderzoeken zo maar kunnen inzien. Aan de andere kant, hebben we bij functioneel beheer een extra attentie gevraagd: let op, dat je je strak moet houden aan de protocollen die er zijn. Het is onze bedoeling om daar audits op te gaan plegen.” – Directeur opsporing

Beslissingen over het invoeren en delen van informatie worden bewust aan de teams overgelaten.

“We willen geen hiërarchische lijn, zo ga je niet om met vakvolwassen medewerkers. Men moet ook de logica gaan inzien. (...) Performanceproblemen, systeemtechnische problemen maken het wel lastig om het verhaal te brengen bij

de gemiddelde inspecteur, rechercheur, recherchebaas en de Officier van Justitie.” –
Directeur opsporing

Zoals eerder aangegeven hebben rechercheurs, met name aan een district, een grote beslissingsruimte bij het verrichten van de invoer. Deze verschuift, waar het gaat over het raadpleegbaar maken en ter beschikking stellen van informatie meer in de richting van de teamleiders. De rechercheur heeft beperkt invloed op de raadpleegbaarheid van informatie in BVO en BlueView. Een rechercheur kan informatie niet op een hoger autorisatieniveau zetten dan waarvoor hij zelf is geautoriseerd. Sommige zijn geautoriseerd op niveau 5. Voor hen geldt hetzelfde als voor de teamleider die altijd hoger geautoriseerd is en daardoor de raadpleegbaarheid van informatie kan beïnvloeden. Hij heeft daarbij, blijkt uit de interviews, een grote beslissingsruimte ten opzichte van de korpsleiding en de Officier van Justitie. Hij kan bij het opstarten van een onderzoek het autorisatieniveau bepalen en aangeven of informatie kan worden doorgezet naar BlueView. Ook mutaties kan hij een hoger autorisatieniveau geven dan een gewone rechercheur.

Binnen de CIE wordt zoals eerder aangegeven, gewerkt binnen een vast regime dat scherp door de teamleider kan worden gevolgd en waardoor een runner maar beperkte beslissingsruimte heeft over wat er met informatie gebeurt. Daarbij is ten aanzien van de invoer van belang dat teamleiders sturen op de kwaliteit van de invoer. Actieve sturing op het delen van alle informatie (met de CIE'en van andere korpsen), is eveneens noodzakelijk.

“De runners doen de voorstellen voor de netto informatie. Het bruto gespreksverslag wordt besproken. Het kan zijn dat ik als teamleider zeg dat daaruit meer verstrekt kan worden. (...) Je moet iemand aan het werk zetten om het allemaal op papier te krijgen, te printen en in dubbele enveloppen te versturen. Er zijn ook informaties die je niet via de post wilt versturen. Corruptiegevallen; zware bronbescherming.” – Teamleider CIE

“Ik zit dagelijks bij die jongens op de kamer. Ik vraag altijd waar ze naartoe gaan en hoor altijd als ze terug komen.” – Teamleider CIE

De CIE'en in hetzelfde verzorgingsgebied kunnen via BVO informatie bij elkaar raadplegen. Afgezien van 200 en 300 informatie¹⁶, spreken de geïnterviewde teamleiders niet over restricties bij het delen van informatie.

“Je maakt je eigen professionele afweging. Je probeert zoveel mogelijk uit de 200 en 300 te houden. In moeilijke gevallen bespreek je een bruto verslag weleens met de Officier. Hij bepleit dan wel eens dat er toch iets netto naar buiten moet. Bij heel gevoelige zaken weten we zelf wel dat we naar 200 en 300 moeten. De Officier van Justitie let er sterk op of ontlastende informatie voldoende wordt uitgegeven.” – Teamleider CIE

¹⁶ Zie hoofdstuk 5 voor een bespreking van de afhandelingscodes uit de CIE-Regeling

7.3 Organisatiedoelen en evaluatiecriteria

Zoals in hoofdstuk 2 vermeld, bestaat er vaak spanning tussen de belangen bij informatiedeling op centraal en decentraal niveau. Deze spanning geldt bedrijven, maar ook een HSO kan met deze spanning te maken hebben. Hasenfeld wijst in dit verband op de sterke afhankelijkheid die HSO's ondervinden van hun omgeving. Om de voor het voortbestaan van de organisatie noodzakelijke middelen te verkrijgen ontwikkelt deze bepaalde rollen en relaties met de juiste externe partijen en gaat op zoek naar steun en legitimiteit voor haar activiteiten.¹⁷ Hasenfeld's ideeën over het effect van deze afhankelijkheid op de organisatie, biedt een kader om te kijken naar afhankelijkheidsrelaties van de politie.

Volgens Hasenfeld betekent het toepassen van organisatiedoelen, het toevoegen van nieuwe criteria die organisatieonderdelen beperken bij de vormgeving van hun werkzaamheden. Organisationsonderdelen zullen hun werk zodanig inrichten dat op de nieuwe (evaluatie)criteria goed kan worden gescoord. Als een organisatie (politiekorps) zich committeert aan doelstellingen (prestatieafspraken), dan wordt deze verantwoordelijk gehouden die ook te bereiken door de controlerende organisaties die legitimeert (OM) en middelen ter beschikking stelt (Ministerie van BZK).¹⁸

Een ander belangrijk aspect van organisatiedoelen is volgens Hasenfeld, dat hierin tot uitdrukking wordt gebracht welke morele waarden volgens de organisatie nodig zijn om aan de noden en problemen te werken, van de mensen om wie het voor de betreffende organisatie gaat. Organisationsdoelen laten volgens Hasenfeld zien welke ideologieën de dominante coalitie binnen de organisatie voorstaat.¹⁹ Voor de politie betekent dat bijvoorbeeld dat ideeën over de impact van verschillende criminaliteitsvormen binnen korpsen, tot onderling verschillende prioriteiten kunnen leiden. Hieraan moet worden toegevoegd dat een organisatie meer gelegenheid heeft haar ideologieën tot uitdrukking te brengen in de organisatiedoelen, naarmate zij minder afhankelijk is van externe organisaties. In de afgelopen jaren hebben landelijke actoren, het ministerie van BZK voorop, meer invloed gekregen op het beleid, de organisatie en de inzet van de politie.²⁰

Hasenfeld stelt dat de verschillende doelstellingen voor de organisatie moeten tegemoet komen aan de wensen van verschillende groepen binnen de

¹⁷ Hasenfeld (1983), p. 8

¹⁸ *Idem*, pp. 99-100

¹⁹ *Idem*, p. 100

²⁰ Huberts, L.W.J.C. (2007), *Politiebestel in de praktijk: sturing en invloed*, in: Fijnaut, C.J.C.F., Muller, E.R. & Rosenthal, U (red), p. 153

HSO. Deze doelen hoeven niet complementair te zijn. De activiteiten die aan verschillende doelen zijn verbonden kunnen evenzo met elkaar in strijd zijn. De organisatie kan conflicten tussen strijdige doelen proberen te reduceren door ze te verbinden aan verschillende rollen en verschillende afdelingen. Echter in de resultaten van de totale organisatie blijven tegenstrijdigheden vaak wel zichtbaar.²¹ De vraag die aan het begin van onderstaande beschrijving (7.3.1) wordt beantwoord is: in hoeverre zijn korpsen van mening dat zij tot taak hebben om landelijke informatiesystemen van input te voorzien tegen de achtergrond van het werk dat van dag tot dag op hen afkomt en welke behoefte bestaat er aan de output van die systemen in het licht van de prioriteit die korpsen geven aan problemen die niet door belanghebbenden uit de eigen regio zijn aangebracht?

In deze paragraaf worden verder de afhankelijkheidsrelaties in kaart gebracht die van invloed zijn op beslissingen van individuele korpsen omtrent het delen van opsporingsinformatie. Hierbij komen aan de orde relatie van korpsen met het OM (7.3.2) en met het Ministerie van BZK (7.3.3).

Zoals eerder is aangegeven is het aanbod van zaken die om een oplossing vragen groter dan de organisatie aankan en ligt binnen de politie ook hierop de nadruk. Daardoor ontstaat er druk op de tijd die overblijft voor het invoeren van informatie in de systemen.

Hoewel korpsen enigszins verschillende accenten leggen, zien alle geïnterviewde directeuren opsporing een duidelijk verband tussen de belangrijkste prioriteiten van hun korps en het belang van landelijk gedeelde opsporingsinformatie. In de relatie van korpsen met het OM enerzijds en het Ministerie van BZK anderzijds, is het belang van landelijk gedeelde opsporingsinformatie nauwelijks aan de orde.

7.3.1 Relatie regiokorpsen – Openbaar Ministerie

De mate waarin korpsen informatie delen met anderen, behoort niet tot de prestatie-indicatoren waarop korpsen door het Openbaar Ministerie (OM) worden beoordeeld. Drie van de vier informanten ervaart hierdoor geen conflict tussen de aandacht die nodig is voor informatiedeling en voor het draaien van voldoende zaken.

“De politie heeft meerdere bazen. De wetgever is een baas; de Wpg is helder waarin we moeten delen. We hebben als politie ook landelijk gezegd dat we meer

²¹ Hasenfeld (1983), p. 101

informatie wilden delen. (...) We moeten aan onze prestatienormen voldoen, zowel bij het regionaal college, bij BZK als bij Justitie. Energie en geld kun je maar één keer wegzetten. Alle energie die we steken in de informatiehuishouding zit niet in het vangen van boeven. Maar zo zijn we aan het balansen op tal van fronten om onze verschillende opdrachtgevers gelukkig te maken. Ik zie daar geen rechtstreeks conflict in.” – Directeur opsporing

“Je krijgt de credits niet. Als die zitten in concrete resultaten, waar je bijvoorbeeld door het OM op wordt aangesproken is dat een lastige. Je moet proberen jezelf de credits te geven voor het aandeel dat je geleverd hebt om de problemen op te lossen: een dader voor langere tijd achter de tralies.” – Directeur opsporing

Eén van de informanten ervaart wel een conflict als het gaat om prioriteit geven aan informatiedeling.

“Invoerdiscipline in de volle breedte is echt nog een aandachtspunt. Het is discipline, maar het is ook prioriteit want de volgende zaak ligt alweer op je te wachten. Dat is ook het spanningsveld met het OM: Er moet weer een volgende zaak gedraaid worden, maar de vorige moet ook nog afgewerkt. We hebben denk ik ook wel vaak de neiging van: ‘Prima, want we hebben ook niet zoveel zin in die administratieve afhandeling.’ Een nieuwe zaak is wellicht leuker om aan te beginnen.” – Directeur opsporing

“Het aanleveren van restinformatie gebeurt mondjesmaat omdat de capaciteit meestal in nieuw onderzoek wordt gestopt. Dat wordt door het OM door de vingers gezien. (...) Het belangrijkste is dat wij onze onderzoeken draaien. Daar worden we voornamelijk op beoordeeld.” – Directeur opsporing

Verder wordt verschillend gedacht over de betrokkenheid van het OM bij het thema informatiedeling.

“Als we geen informatie delen en we draaien wel heel veel zaken, dan zal het ze worst wezen denk ik.” – Directeur opsporing

“Deze aanpak [waarbij gerichte informatie leidt tot eerder beschikbaar stellen van capaciteit voor een onderzoek] leidt tot een verbetering die door het OM wordt gewaardeerd.” – Directeur opsporing

7.3.2 Relatie korpsen - Ministerie van BZK

Het delen van informatie is onderdeel van de prestatieafspraken met het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK). Echter de sturingsrelatie tussen het ministerie en de korpsen op het onderwerp van informatiedeling, wordt door de andere informanten getypeerd als een indirecte relatie. Er is een beleidsmatige interesse voor het onderwerp maar de korpsen worden uiteindelijk op resultaten op andere terreinen afgerekend, vinden de informanten.

“Het OM zit bovenop onze onderzoeken en kan zien of wij informatie delen. De dwingende ogen komen van het OM maar dat richt zich niet in eerste instantie op het landelijk delen van informatie. BZK doet dat minder frequent via monitoring door de Inspectie Openbare Orde en Veiligheid op de korpsen af te sturen. (...) Ik merk dat de aantallen aanhoudingen en bijvoorbeeld diversiteit, dat daar hard op gestuurd wordt en zeker in dit korps. Ik merk dat op de samenwerkingsafspraken veel minder gestuurd wordt.” – Directeur opsporing

“De beleidsmatige interesse is dat we een goede informatiehuishouding hebben en dat we daar een bijdrage aan leveren, maar het gaat hun in the end ook om de resultaten. (...) Naarmate wij meer informatie hebben van andere korpsen, kunnen wij beter voldoen aan onze doelstellingen. We zijn er wel onderdeel van, maar we hebben te maken met de informatieorganisatie van anderen.” – Directeur opsporing

“Daar is een indirect verband [met de resultaten]. (...) Mijn stelling is dat vroegtijdig informatie delen leidt tot betere resultaten, dan ga je dat altijd merken in de tevredenheid van BZK. (...) Er is ook een rechtstreeks verband: bij de resultaatgesprekken wordt expliciet gevraagd naar de informatie-uitwisseling.” – Directeur opsporing

Drie van de vier informanten geven aan dat binnen hun korpsen een afweging wordt gemaakt tussen de capaciteit die wordt besteed aan het landelijk delen van opsporingsinformatie en andere doelstellingen van hun korps.

"Ja [wij maken een afweging tussen de capaciteit die wordt besteed aan het landelijk delen van informatie en andere doelstellingen van ons korps]. Het is vaak het stiefkindje. Je bent bezig met opsporingsonderzoek en dan moet je ook je rest- en zijtakinformatie nog verwerken. Dat is altijd lastig. We hebben daar aandacht aan besteed, maar de vacatures zitten nog in de data-entry." – Directeur opsporing

"Ja [wij maken een afweging tussen de capaciteit die wordt besteed aan het landelijk delen van informatie en andere doelstellingen van ons korps]. Wij hebben capaciteit binnen het proces opsporing. Dat wordt verdeeld naar bijvoorbeeld tactische onderzoeken, maar ook wat er kan worden besteed aan het informatieproces, restinformatie wegzetten. Zoals ik daarnet al zei: eigenlijk is de opdracht om na ieder onderzoek een rest-PV te maken en dan wordt toch gekozen om een volgend onderzoek te beginnen omdat dat belangrijk is om een volgend crimineel samenwerkingsverband op te rollen. De voornemens zijn goed maar het managementteam kiest dan om de capaciteit in te zetten op de opsporing." – Directeur opsporing

Eén van de directeuren opsporing stelt dat het zoeken van een balans binnen zijn korps op veel verschillende fronten aan de orde is.

Op diverse manieren wordt het werk van politiekorpsen gestuurd. Om een systeem van landelijk gedeelde opsporingsinformatie te realiseren (zoals met de samenwerkingsafspraken 2008 beoogd), wordt van de korpsen gevraagd tijd te reserveren voor onder meer het invoeren van opsporingsinformatie in BVO. Als het ware wordt daarbij aangenomen dat deze forse extra inspanning de opsporing effectiever zal maken, waardoor de tijd die in het invoeren van de informatie werd gestoken een goede investering zou zijn. Deze verbetering ten opzichte van de oude situatie, waarbij ook wel landelijke matching van opsporingsonderzoeken plaatsvond, tekent zich pas duidelijk af na verloop van jaren. Eerder in deze rapportage kwam al naar voren dat informanten in het algemeen overtuigd zijn van het nut van informatiedeling tussen korpsen. Geconcludeerd kan worden dat zolang niet vaststaat dat de opsporing effectiever is geworden door de extra inspanningen die korpsen doen, deze grote inzet een waagstuk is en ook zo wordt ervaren. Immers, de effecten op de resultaten zijn niet precies duidelijk en op deze laatste worden de korpsen primair afgerekend. Voor de veranderingsgezindheid van de korpsen is dat niet bevorderlijk.

7.4 Tussenconclusie

Conclusies m.b.t. de onderwerpen die in dit hoofdstuk zijn behandeld, worden betrokken bij de tussenconclusie aan het einde van het volgende hoofdstuk. Daarin wordt deelvraag V kort van een antwoord voorzien en wordt het bijbehorende deel uit het verklaringsschema geëvalueerd.

8. Politiewerk is en blijft spannend

In het vorige hoofdstuk werd de basis gelegd voor de beantwoording van de vijfde deelvraag uit de inleiding. Hierbij werd ingegaan op specifieke sturingskenmerken van de politieorganisatie en haar omgeving, door de politie te beschouwen als een *Human Service Organisation*. In dit hoofdstuk is in de eerste plaats de aard van het politiewerk gekozen als invalshoek om de invloed van organisatorische omstandigheden op informatiedeling tussen politiekorpsen te beschrijven. In de eerste paragraaf wordt onder meer werk van Peter K. Manning geïntroduceerd die ICT in de politieorganisatie ook met deze invalshoek benadert: wat betekent de aard van het politiewerk voor de inzet van ICT en vice versa?²² Hij legt daarbij eveneens nadruk op sturingsproblemen, waardoor de beschrijving in hoofdstuk 8 naadloos aansluit op paragraaf 7.2.

In paragraaf 8.2 wordt in het bijzonder ingegaan op het belang van vertrouwelijkheid voor het politiewerk. In paragraaf 8.3 wordt beschreven welke rol dit thema speelt in de onderzochte korpsen.

8.1 De aard van het politiewerk

Volgens Manning is de politie primair gericht op het hier en nu. Hij stelt dat de focus van de politieorganisatie ligt op responsiviteit en beheer van de vraag; historisch het mandaat waarop de politie is gebaseerd. Echter, het is ook deze focus die volgens Manning de succesvolle introductie van complexe criminaliteitsanalyse (d.m.v. het gebruik van ICT-systemen) onwaarschijnlijk maakt.²³

Dat de werkelijkheid voor de politie niet eenvoudig is, is een gegeven dat van belang is om haar sturingsproblemen te kunnen begrijpen. “De politie moet werken in een omgeving die door een grote mate van diversiteit en onvoorspelbaarheid wordt gekenmerkt. (...) De politie is nauwelijks in staat om hier sturing aan te geven. Integendeel, het politiewerk wordt in hoge mate gestuurd door meldingen, klachten en aangiften van het publiek. De reactief ingestelde politie is – anders gezegd – de gevangene van een grillige omgeving.”²⁴ De focus op responsiviteit en als gevolg daarvan, de moeilijkheden bij het sturen van de organisatie, zou ook voor het probleem van de beperkte informatiedeling

²² Manning, Peter K. (2005), *Environment, Technology, and Organizational Change*, in: Pattavina, A. (ed.), *Information technology and the criminal justice system*

²³ *Idem*, p. 236

²⁴ Aalberts M.M.J., H.G. van de Bunt (1994), p. 383

van betekenis kunnen zijn. De aard van het politiewerk biedt een aanknopingspunt om te kijken naar de in de inleiding vermelde terughoudendheid bij Nederlandse politiemensen om opsporingsinformatie te delen. In het bijzonder wordt in dit hoofdstuk ingegaan op de vertrouwelijkheid van de gegevens waarmee de politie werkt.

8.1.1 Vertrouwelijkheid

Kijkend naar de aard van het politiewerk is de vertrouwelijkheid van gegevens waarmee wordt gewerkt kenmerkend. Hoewel binnen een team over het algemeen alle betrokkenen over alle informatie mogen beschikken, geldt dit niet noodzakelijkerwijs voor de rest van het korps – ook niet voor ondersteunende diensten.²⁵ “Het is niet altijd duidelijk wat geheim moet blijven en wat in een bredere kring kan worden gedeeld. Daarbij wordt – soms te veel – vertrouwd op de ervaring en het oordeel van de betrokken rechercheurs. Er is veelal geen procedure op grond waarvan uitspraken kunnen worden gedaan over welke informatie vertrouwelijk is en welke niet, of er is geen aangewezen functionaris die daarover beslist. In enkele gevallen leidt dat er ook toe dat informatie openbaar wordt die niet openbaar had mogen worden.”²⁶ Hierbij moet worden opgemerkt dat de aangehaalde studie werd uitgevoerd in de periode tussen 1998 en 2001. Deze beschrijving is daarom wellicht niet actueel, maar ze geeft wel aan dat toegang tot en het interpreteren van gegevens door medewerkers buiten het eigen team – en zoals met de ICT-basisvoorzieningen mogelijk is, door andere korpsen – tot enkele jaren geleden tamelijk ongewoon was. Met andere woorden, ook het belang van vertrouwelijkheid is een aspect van politiewerk dat de informatiedeling kan frustreren.

Het werken met informatiesystemen voegt volgens Manning complexiteit toe aan het politiewerk en leidt daarmee tot extra risico's. Hij stelt vervolgens dat het gebruik van ICT het creëren van nieuwe informatie, vanwege het belang van een stabiele organisatie in de weg staat.²⁷ Een vuistregel in de politiewereld lijkt hierbij van toepassing: naarmate de communicatie verder van een politiefunctionaris afstaat, vertrouwt hij deze minder. Onpersoonlijke informatiedeling via een geautomatiseerd systeem is daarom bij voorbaat verdacht.²⁸ Uit de literatuur blijkt verder dat via diverse overlegvormen informatie wordt overgedragen; door middel van direct contact. Daarnaast

²⁵ Poot, C. de et al (2004), pp. 348-351

²⁶ *Idem*, p. 351

²⁷ Manning (2005), p. 223

²⁸ Manning, P.K. (2001). *Technology's ways: Information technology, crime analysis, and the rationalizing of policing*. Criminal Justice, 1, p. 99

worden diverse schriftelijke vormen van informatieverbreiding toegepast, met als doel de leden van teams alle op eenzelfde niveau van informatie te krijgen. Maar het gaat daarbij om informatiedeling binnen teams. “Veel informatie blijkt te worden gedeeld op informele momenten waarop rechercheurs bij elkaar komen (koffie, pauzes, eten). Hoewel dit veelal niet erg gestructureerd gebeurt, is het voor veel rechercheurs een belangrijke informatiebron.”²⁹

²⁹ Poot, C. de et al (2004), p. 349

8.2 Politiemensen beleven risico's bij informatiedeling

Aan informanten op operationeel en op tactisch niveau is gevraagd welke risico's zij zien op het gebied van vertrouwelijkheid, als informatie via BVO en BlueView wordt gedeeld met geautoriseerden. Daarnaast is gevraagd hoe de beleving van deze risico's beslissingen beïnvloedt over het invoeren en delen van informatie.

Welke risico's worden ervaren?

Informanten van zowel operationeel als tactisch niveau stellen zich op het standpunt dat naarmate opsporingsinformatie meer met andere teams wordt gedeeld via BVO en BlueView, het risico toeneemt dat het oorspronkelijke onderzoek beschadigd raakt. Ook wordt als risico genoemd dat de informatie onterecht als startinformatie gebruikt kan worden. Die mogelijkheid kan volgens informanten worden tegengegaan door bij de geboden informatie duidelijk te zijn over de bron en over de betrouwbaarheid van de bron. Hoewel deze risico's worden ervaren, zijn ze niet altijd van invloed op beslissingen over het invoeren of delen van opsporingsinformatie.

“Als ik niets invoer, dan heeft niemand iets aan mijn informatie. (...) Zeker mensen die in grote onderzoeken zitten, zien het belang van landelijke informatiedeling. Een heel groot deel van ons werk bestaat uit het verzamelen van informatie. We zitten heel veel achter de computer om naar informatie te zoeken en te verzamelen. Als dat dan niet lukt is dat vervelend en dan bedenkt je ook dat je zelf ook genoeg moet blijven invoeren. We zijn ook enorm afhankelijk van de informatie die verzameld wordt op straat. We hebben gezien dat de informatiestroom in BVH terugloopt. Er wordt enorm gemopperd: het werkt niet altijd even makkelijk en prettig en het gevolg is dat mensen minder invoeren. De informatiestroom naar ons wordt dan ook minder. (...) Over twee jaar gaan we wel zien dat er veel minder informatie beschikbaar is. Dat is funest.” – Tactisch coördinator regiorecherche (afdeling ZwaCri)

“Uiteraard zijn er risico's. Maar ik ga uit van het standpunt dat iedereen bij de politie is gescreend en geautoriseerd. Ik ga uit van de kracht van het delen en dat moet je niet de beren zien dat het door de verkeerden wordt opgevraagd. Dat vind ik een beperkende gedachte.(...) In elk onderzoek dat wij draaien komen collega's voor. Dan zou je kunnen zeggen, van dat gaan we afschermen en dat doe ik dus niet. ” – Teamleider regiorecherche

Sommige teams nemen (systematisch) maatregelen om reden van de ervaren risico's omtrent vertrouwelijkheid. Uit de antwoorden van informanten kan worden opgemaakt waaruit de genoemde risico's precies bestaan: (1) Rechercheactiviteiten raken (opzettelijk) bekend bij onderzoekssubjecten, en (2) onderzoek kan ongewild via de pers openbaar worden.

"Standaard wordt [informatie] misschien te hoog weggezet om te voorkomen dat er een keer te gevoelige informatie naar buiten komt. Er zijn ook best dingen bij, verklaringen bijvoorbeeld, die kunnen wel op een lager niveau weggezet worden. Maar we nemen het risico gewoon niet. Ik kom niet toe aan die afweging. De reden is dat in lopend onderzoek het niet altijd handig is dat iedereen bepaalde gegevens kan raadplegen. (...) Ongewild kunnen dingen bij een subject terecht komen. Iemand die bij de informatie is geweest kan dat ergens laten vallen. Ik noem het voorbeeld van de wijkagent.(...) Agenten worden goedbedoeld actiever, maar worden misschien gezien en dan worden de subjecten van het onderzoek wakker." – Senior tactisch coördinator districtsrecherche

"Naarmate je meer informatie met meer mensen deelt, loopt de vertrouwelijkheid steeds meer gevaar. Uit ervaring is dat gebleken. Hoe meer je informatie gaat delen, hoe verder het verdeeld is binnen de teams. Dan komt het voor dat blauwe teams in hun enthousiasme mensen gaan controleren die in jouw onderzoek voorkomen. Dat had je eigenlijk liever niet gehad. (...) Je onderzoek kan ook via de pers, of wat ook gebeurt bij de mensen zelf, op straat komen te liggen. (...) Informatie moet je wel delen. Maar wij houden bepaalde informatie ook achter. Binnen TGO's houdt de teamleiding, soms tijdelijk, bepaalde informatie achter. Dat gebeurt gewoon want dat is voor het onderzoek beter." – Tactisch coördinator districtsrecherche

Een informant gaat expliciet in op de inrichting van de basissystemen, in relatie tot de vertrouwelijkheid van de informatie.

"Als BlueView in beeld komt. (...) Voor het rechteproces vind ik het heel gevaarlijk. Ze zien de inhoud van de mutaties. Als ik een belangrijk tapgesprek in BVO neerzet en daar wordt over een liquidatie gesproken. Daar heeft iemand anders helemaal niets mee te maken. Als wij onze onderzoeken aanleveren in BlueView, dan zien ze de inhoud van alle mutaties tot op niveau 5. (...) Kijk maar hoeveel mensen binnen het KLPD een BlueView autorisatie hebben. Ik heb hier

kritisch naar gekeken. Het mag niet zo zijn dat we straks tapgesprekken op niveau 6 of 7 weg moeten gaan zetten. Dat lukt in een lopend onderzoek niet. Ze zien gewoon alles. BlueView is in mijn ogen bedoeld om naar art. 8 informatie te kunnen kijken. Als je onderzoek stukloopt middels lekken, dan kun je dat nooit meer traceren. Dan moet je alle BlueView registraties aflopen, landelijk. Daar komt je nooit meer uit. In een team kun je lekken wel tegengaan. Als je een BlueView registratie hebt en je kent een verdachte goed. Hij kan zijn naam door BlueView heen halen en hij ziet dat er twee actieve onderzoeken op hem lopen. Hij kan precies zien welke nummers we tappen. Hij kan alles zien, dat is toch bezopen?" – Analist/kwaliteitscoach recherche

Binnen het werk van de CIE is het verstrekken van informatie aan een CIE van een ander korps, zoals eerder aangeven, strak geregeld. De vertrouwelijkheid van de informatie beheerst de aard van het CIE werk volledig. Het principe van werken met de basissystemen levert echter geen bijzondere risico's met de vertrouwelijkheid op volgens informanten. Wel is de veiligheid van de ICT waarmee de CIE werkt een probleem in relatie tot vertrouwelijkheid. Met name de CIE bruto omgeving van BVO vormt een knelpunt. Hier wordt niet verder op in gegaan omdat dit probleem niet zozeer met de aard van het CIE werk te maken heeft, als wel met de toegepaste ICT en dat onderwerp is eerder in deze rapportage behandeld.

8.3 Politiewerk: mensenwerk?

Vertrouwelijkheid speelt een belangrijke rol bij het werk van politiemensen. Het gebruik van ICT maakt dat politiemensen opnieuw kritisch naar hun werkomgeving kijken. Informanten is gevraagd of de risico's uit voorgaande subsectie in mindere mate worden ervaren worden wanneer informatie wordt overgedragen in menselijk contact.

Wat is het belang van persoonlijk contact?

Gelukkig zijn de landelijke informatiesystemen nog niet zo compleet dat persoonlijk contact daardoor overbodig wordt, verzucht een informant. Zoals eerder aangegeven worden contacten tussen rechercheurs van verschillende teams meestal gelegd n.a.v. informatie die in systemen is vastgelegd. Echter de rol van menselijk contact is bij de huidige stand van zaken nog niet uitgespeeld. In sommige gevallen wordt informatie sneller gedeeld buiten systemen om. Voorbeelden daarvan zijn eerder in deze rapportage aan de orde geweest.

“Er zijn wel collega’s die je om wat voor reden dan ook goed kent. Bijvoorbeeld uit andere onderzoeken. Als ik naar Apeldoorn moet bellen, dan bel ik een bepaalde collega op. Ik zoek informatie en heb het idee dat er meer informatie is dan dat ik via de officiële kanalen krijg. Dan vraag ik: weet jij nog iemand die ik kan benaderen? En dan zegt hij: dan moet je hem hebben.” – Tactisch coördinator regiorecherche (afdeling ZwaCri)

De vraag of er minder risico's zijn als informatie wordt gedeeld via menselijk contact wordt echter eensgezind beantwoord. Het zou niet uitmaken of informatie in rechtstreeks contact of via een systeem wordt verspreid: niet iedereen kan zijn mond houden. In sommige gevallen is het beter informatie niet te delen, op welke manier dan ook.

“Ik denk niet dat menselijk contact voordeel geeft. Ik vind het een goede zaak dat we systemen open hebben staan en tot het tegendeel bewezen wordt, moet dat vooral zo blijven.” – Teamleider regiorecherche, politiekorps IJsselland

“Je kan zeggen: mondje dicht, het moet gewoon een normale situatie blijven. En toch zal hij er tijdens de nachtdienst langsrijden.” – Senior tactisch coördinator districtsrecherche

Eén informant was van mening dat bij menselijk contact er meer zicht is op de vertrouwelijkheid.

“Ik heb bij meerdere grote onderzoeken meegemaakt dat verdachten ontdekten dat ze geobserveerd werden, dat ze getapt werden etc.. Het is niet zozeer dat ik mijn collega's niet vertrouw. Maar je moet er wel rekening mee houden dat er altijd mensen zijn die misbruik maken. Wat niet weet, wat niet deert. Via menselijk contact heb je wel een betere focus.” – Analist/kwaliteitscoach recherche

Tot slot zijn informanten van mening dat de vertrouwelijkheid van informatie bij rechemedewerkers duidelijk minder gevaar loopt dan bij blauwe politiemensen.

8.3.1 Bronbescherming

Wanneer vertrouwelijkheid van informatie gewenst is, kan sprake zijn van meer specifieke belangen of risico's. Informanten op tactisch niveau is gevraagd naar een aantal specifieke belangen in relatie tot vertrouwelijkheid. De eerste is het belang van bronbescherming bij beslissingen over het delen van opsporingsinformatie.

Is bronbescherming van invloed?

In hun antwoord betrekken informanten drie typen bronnen: informanten, getuigen en camera's. De bescherming van informanten heeft de hoogste prioriteit bij de CIE, als het gaat om de beslissing informatie te delen.

“Als het belang groot is, als de staat in gevaar komt of de Koningin, dan gaan we in overleg met de Officier op zoek naar manieren waardoor we toch de informatie kunnen delen zonder dat het afbreukrisico bestaat. Soms moet je het wegzetten in een andere dienst en daar iets op gang brengen, zodat niet duidelijk is dat de informatie van onze bron komt. Dat komt voor.” – CIE Teamleider

Wel wordt er door de CIE aan gewerkt informatie die zodanig wordt gekwalificeerd dat deze niet operationeel gebruikt kan worden (00), op de duur wel door te spelen naar de opsporingsteams. Dan is het operationeel te gebruiken (01).

Teamleiders bij de recherche kennen CIE informanten in de praktijk niet en kunnen ze onmogelijk prijsgeven via informatiedeling. Over het afschermen van

getuigen denken de twee geïnterviewde teamleiders recherche verschillend. De één beschermt ze niet, de ander zegt dat hij een aantal keren heeft meegemaakt dat dit noodzakelijk was waardoor de betrokken informatie niet gedeeld kon worden. Tot slot worden genoemd de mensen die een ruimte beschikbaar stellen voor het opstellen van een camera. Hun gegevens worden niet gedeeld.

“Dat is ook een bron om uit de papieren te houden; uit tactisch oogpunt. Dat gaat om veiligheid. Je wilt dat soort mensen niet in gevaar brengen.” – Teamleider regiorecherche

“Ik deel niet als getuigen gevaar lopen. Dat is een paar keer voorgekomen. (...) We hebben geen regelingen om getuigen te beschermen. Maar het is zeker van belang.” – Onderzoeksleider TGO

“Over BlueView. Toen wij met X begonnen waren, toen hadden we daarvan proces verbaal opgemaakt en dan staat zijn naam er in en die gaat naar een team toe en wat hij wil. Bij ons gaat het naar een team dat werkt in een besloten ruimte. In [korps y] draaide onderzoek op een liquidatie en die hadden zijn verklaringen daarover in X-pol gedaan, maar via BlueView te benaderen. Dus heel Nederland kon dat lezen en wist meteen dat X verklaringen had afgelegd. Dat geeft al een gevaar voor zijn familie etc.. Zij denken daar niet bij na. (...) Eerst was hij informant bij ons. Hij wilde in de getuigenbescherming, dus hij wilde alles tactisch verklaren. Bij ons dan is het geen bewijs. Wordt het tactisch dan kan je het als bewijs gebruiken, maar dan moet wel zijn naam erin. Dan gaat hij in de getuigenbescherming en gaan ze hem nooit meer vinden, bij wijze van spreken. Maar hij heeft hier wel familie wonen. Dus het is helemaal niet van belang om al in een vroeg stadium aan te geven: we zijn met dat onderzoek bezig. Als de tegenpartij dat weet, gaat die al getuigen beïnvloeden. Zodat ze bij jou komen: jij gaat niks vertellen. Terwijl dat een lopend onderzoek is. Doordat het door BlueView door heel Nederland verspreid wordt, is dat een nadeel. Dat is een reden voor mijn korps geweest om dat niet in X-pol te doen zodat het niet door BlueView wordt opgezogen. Als je een onderzoek op Willem Holleeder doet, is dat niet handig om dat via BlueView benaderbaar te maken omdat iedereen hem kent. Leest een collega dat, op een verjaardagsfeestje is het interessant om daar over te vertellen. Zo werkt dat gewoon. Dat wordt veel te breed, terwijl het onderzoek nog in volle gang is. Als het onderzoek is afgesloten, dan mag het in BlueView en mag iedereen het weten. Je kan naar de rechtbank gaan en dan weet je het ook. Als een onderzoek

nog loopt, dan is dat vaak niet wenselijk. Ze hebben dat besef niet altijd. In [korps y] gooiden ze het er gewoon in.” – Coach bij de CIE

8.3.2 Bescherming van lopend onderzoek

Tevens is gevraagd welke rol de bescherming van lopend onderzoek speelt bij beslissingen over het delen van opsporingsinformatie.

Is bescherming van lopend onderzoek van invloed?

Eén van de informanten kan zich niet zoveel voorstellen bij het belang van de bescherming van lopend onderzoek. De andere geïnterviewde teamleiders geven aan dat de bescherming van lopend onderzoek erg van belang is.

“Ik kan me niet heugen dat wij hier een onderzoek draaien dat is afgeschermd. Dat doen we bijna niet. Ik heb ook nog nooit van onregelmatigheden gehoord. We gebruiken BlueView als sturing en anders vragen we de informatie op. Je wilt dan ook een originele verklaring. Anders kan de rechter er niets mee.” – Teamleider regiorecherche

“Als ik op voorhand kan inschatten dat bepaalde informatie kan leiden tot gebruik in het land, wat schade oplevert in mijn onderzoek dan zet ik het op een andere omgeving weg. Eventueel tijdelijk, tot het risico niet meer bestaat. (...) Als ik het met een collega niet eens word over het gebruik van informatie, dan laat ik mijn officier contact opnemen met zijn officier. Die moeten dat dan uitvechten. Ik leg het mijn officier dan wel uit. (...) Een voorbeeld. Regio X doet onderzoek naar een woninginbraak op verdachte Jansen. Maar ik doe onderzoek op het maatje van Jansen, naar een verdovende middelenhandel en ik ben daar al een jaar mee bezig. Zij willen Jansen aanhouden en die blijkt in de woning van mijn verdachte te zitten. Dan ga ik dat niet delen. Want dan vallen zij naar binnen en treffen daar ook mijn verdachte aan, die gewaarschuwd is en veel voorzichtiger gaat zijn en misschien vlucht. (...) Als er grotere belangen zijn dan deel ik informatie wel. Als ik zelf op een woninginbraak zit en ik krijg een VROS-melding dat we onderzoek doen op dezelfde persoon, dan deel ik alles want dan nemen ze mijn woninginbraak wel mee. Of niet, maar dat is niet erg als hij een zware gevangenisstraf krijgt voor het delict dat zij onderzoeken. (...) Soms is er samenspraak. Als vandaag jouw observatieteam op een verdachte rijdt, zou je ze dan ook attent willen maken op... Als ze dat zien, kunnen wij dan die informatie krijgen.” – Onderzoeksleider TGO

8.3.3 Bescherming van toegepaste werkwijzen

Tot slot is informanten gevraagd naar het belang van het beschermen van toegepaste werkwijzen, bij beslissingen over het delen van opsporingsinformatie.

Is bescherming van toegepaste werkwijzen van invloed?

Informanten zijn eensgezind over het beschermen van toegepaste werkwijzen. Daarvan is sprake. Waarbij in het eerste citaat alleen de werkwijze zelf wordt afgeschermd en in het voorbeeld van het tweede, ook de informatie die het team heeft verzameld niet wordt gedeeld.

“Wat je doet en hoe je dat doet. Dat wordt ook wel op niveau 5 weggezet soms. Dat is niet interessant. Als je een infiltratietraject hebt en er wordt een cover bedacht en uitgevoerd, dan hoef je dat niet te rapporteren. Je hoeft je methodiek niet prijs te geven, maar je moet wel aangeven welk opsporingsmiddel je hebt gebruikt. Je geeft wel aan dat het om camerabeelden gaat, maar niet waar die hing.” – Teamleider regiorecherche

“We hebben een safehouse vol met apparatuur die wij daar hebben aangebracht. Een ander korps is ook op zoek naar onze verdachte maar kent dat safehouse nog niet. In dat geval, ga ik niet delen. Want dan ligt het op straat. Als ze bepaalde informatie in hun onderzoek betrekken, dan zullen ze hem aanhouden en dan weet heel Nederland dat ik onderzoek doe en loopt dat afbreuk op.” – Onderzoeksleider TGO

Het afschermen van werkwijzen ligt gevoelig binnen de CIE, stelt één van geïnterviewde CIE teamleiders.

“Binnen de CIE gebeurt niks meer stiekem. De BOB geldt ook beperkt voor ons. Een inkijk, een observatie kan geen probleem zijn. Dat moeten we wel benutten. Maar het moet wel op papier. Dat is afgeschermd, maar wij kunnen het verantwoorden.” – CIE teamleider

8.4 Tussenconclusie: taaie problemen op organisatorisch vlak

In hoofdstukken 7 en 8 werden de onderzoeksgegevens gepresenteerd, betreffende deelvraag V van dit onderzoek: *In hoeverre beperken organisatorische omstandigheden de uitwisseling van opsporingsinformatie tussen Nederlandse politiekorpsen?*

De beantwoording van deze deelvraag vormt het sluitstuk van het verklaringsschema uit hoofdstuk 2, dat steeds in deze rapportage is gevolgd. Om deze vraag te beantwoorden werden twee verschillende thema's onderzocht. In relatie tot sturingskenmerken van de politie (hoofdstuk 7) kunnen op basis van de interviews de volgende conclusies worden getrokken:

-Sturingskenmerken van de *human service organization* blijken van toepassing op het probleem van de beperkte informatiedeling tussen korpsen. Enerzijds hebben korpsen te maken met sturingsproblemen die voortkomen uit de grote zelfstandigheid van rechercheurs en teamchefs. Anderzijds hebben korpsen te maken met tegenstrijdige doelstellingen vanuit een invloedrijke omgeving: onder meer Openbaar Ministerie en het ministerie van BZK. Onderstaande conclusies zijn ondersteunend aan deze algemene conclusie.

-Sturing op de invoer blijkt voor teamleiders op grootschalige onderzoeken gemakkelijker te realiseren dan voor hun collega's op de districtsrecherche, die diverse kleine onderzoeken tegelijkertijd moeten aansturen. De zelfstandigheid van districtsrechercheurs wordt daardoor groter. Daarnaast doen districtsrechercheurs minder vaak en minder diepgaand ervaring op met BVO omdat zij vaak in BVH kunnen blijven werken of zelfs kans zien om een dossier op te maken zonder gebruik te maken van de landelijke systemen. Hun kennis van BVO is daardoor beperkt en hun bereidheid om ermee te werken laag. Het is kortom lastiger om hen aan te sturen, dan de collega's die in een TGO werken. Bij gebrek aan meer uitgebreide geautomatiseerde managementtools, is de sturing op de invoer vanaf de korpsleiding in de eerste plaats gericht op het aanmelden van de MRO.

-Beslissingen over het invoeren en delen van informatie worden binnen korpsen bewust aan de teams overgelaten: in de praktijk bestaan er binnen korpsen geen hiërarchische lijnen op dit punt. De teamleider heeft een grote beslissingsruimte ten opzichte van zijn leidinggevende en de Officier van Justitie. Hij kan bij het

opstarten van een onderzoek het autorisatieniveau bepalen en aangeven of informatie kan worden doorgezet naar BlueView. Ook mutaties kan hij een hoger autorisatieniveau geven dan een gewone rechercheur. Binnen de CIE is actieve sturing op het delen van informatie noodzakelijk, maar wel veel eenvoudiger te realiseren dan binnen de recherche. De lijnen zijn korter en daarbij is het verstrekken van informatie de primaire taak van een CIE.

-Hoewel korpsen enigszins verschillende accenten leggen, zien alle geïnterviewde directeuren opsporing een duidelijk verband tussen de belangrijkste prioriteiten van hun korps en het belang van landelijk gedeelde opsporingsinformatie. Interne doelstellingen van de korpsen zijn dus goed verenigbaar met informatiedeling. In de prestatieafspraken van korpsen met het OM enerzijds en het Ministerie van BZK anderzijds, komt echter het belang van landelijk gedeelde opsporingsinformatie nauwelijks aan de orde stellen informanten.

-De omgeving van korpsen zorgt voor druk op de organisatie. Het aanbod van zaken die om een oplossing vragen is groter dan de organisatie aan kan. Daardoor ontstaat druk op de tijd die overblijft om aandacht te besteden aan informatiedeling. Net zoals in de relatie met het OM, worden korpsen ook door het ministerie van BZK uiteindelijk vooral op resultaten op andere terreinen afgerekend. De sturingsrelatie tussen het ministerie en de korpsen op het onderwerp van informatiedeling, wordt door informanten getypeerd als een indirecte relatie. Korpsen maken een afweging tussen de capaciteit die wordt besteed aan het landelijk delen van opsporingsinformatie en andere doelstellingen. Informatiedeling wordt daarbij een stiefkindje genoemd; gekozen wordt om de capaciteit op de opsporing in te zetten. Het verwerken van restinformatie is een verantwoordelijkheid van de korpsen die door het OM onder druk wordt gezet: nieuwe zaken krijgen voorrang. Echter drie van de vier geïnterviewde directeuren opsporing ervaren geen direct conflict tussen de aandacht die nodig is voor informatiedeling en voor het draaien van voldoende zaken.

In relatie tot de aard van het politiewerk (hoofdstuk 8) kunnen op basis van de interviews de volgende conclusies worden getrokken:

-Het blijkt dat de aard van het politiewerk in de praktijk wringt met de openheid die van teams wordt gevraagd bij het landelijk delen van opsporingsinformatie

binnen de huidige opzet, waarbij vaak de inhoud van onderzoeken raadpleegbaar is voor andere korpsen. Onderstaande conclusies zijn ondersteunend aan deze algemene conclusie.

-Informanten vinden dat naarmate opsporingsinformatie meer met andere teams wordt gedeeld via BVO en BlueView, het risico toeneemt dat het oorspronkelijke onderzoek beschadigd raakt. Ook wordt als risico genoemd dat de informatie onterecht als startinformatie gebruikt kan worden. Uit de antwoorden van informanten kunnen twee oorzaken worden onderscheiden voor het ontstaan van deze risico's: (1) Rechercheactiviteiten worden (opzettelijk) bekend (gemaakt) bij onderzoekssubjecten, en (2) onderzoek kan ongewild via de pers openbaar worden. Daarnaast vormde de CIE bruto omgeving van BVO in de afgelopen periode een knelpunt: niet aan alle veiligheidseisen werd voldaan waardoor informatie in bepaalde gevallen niet werd ingevoerd. Kortom, het belang van vertrouwelijkheid van informatie dat centraal staat bij het opsporingswerk, vormt op verschillende manieren een knelpunt voor informatiedeling tussen korpsen.

-Er is weinig reden voor menselijk contact bij informatiedeling. Het maakt volgens informanten niet uit of informatie in rechtstreeks contact of via een systeem wordt verspreid: niet iedereen kan zijn mond houden. In sommige gevallen is het beter informatie niet te delen, vinden ze. Informanten vinden dat de vertrouwelijkheid van informatie bij rechemedewerkers minder gevaar loopt dan bij blauwe politiemensen.

-De bescherming van informanten heeft de hoogste prioriteit bij de CIE, bij beslissingen over het delen van informatie. Over het afschermen van getuigen denken twee geïnterviewde teamleiders recheme verschillend. De één beschermt ze niet, de ander zegt dat hij een aantal keren heeft meegemaakt dat dit noodzakelijk was waardoor de betrokken informatie niet gedeeld kon worden.

-De bescherming van lopend onderzoek is zeer van belang bij beslissingen over het delen van opsporingsinformatie. Ook wordt het beschermen van toegepaste werkwijzen door informanten van invloed geacht op beslissingen over het delen van informatie.

De keten van juridische, technologische en organisatorische omstandigheden volgend, waarop het verklaringsschema in hoofdstuk 2 is gebaseerd, laat op ieder van deze onderdelen knelpunten zien. Deze theoretische benadering geeft een goed overzicht over de verklaringen die een rol spelen. De keten begint bij ervaren tekortkomingen van de toegepaste computertechniek, gebrek aan kennis en tijd. Bij juridische en technologische knelpunten is de vraag dus of informatiedeling wel kan, met name in dit laatste organisatorische hoofdstuk was de vraag, of een politiekorps en in het bijzonder een opsporingsteam ook onder alle omstandigheden informatiedeling wil.

Hasenfeld's *human service organization* blijkt goed toepasbaar op de politie en op het soort sturingsproblemen die de politie kenmerken en die voor een deel het achterblijven van informatie-uitwisseling kunnen verklaren. Volgens Hasenfeld behoren de beschreven sturingsproblemen tot de wezenskenmerken van de politieorganisatie. Tijdens de interviews in dit onderzoek werd zoals eerder aangegeven, de typische zelfstandigheid van de *street level bureaucrats* aangetroffen: rechercheurs en teamchefs zoeken vanuit hun eigen professionele opvattingen zelfstandig een uitweg in dilemma's waarvoor zij zich in de praktijk gesteld voelen. Gesteld voelen, want uit de interviews blijkt evenzo dat niet iedereen dagelijks met dilemma's te maken heeft. Met andere woorden, een substantieel deel van de opsporing is waarschijnlijk wél in staat mee te werken in de huidige aanzet naar een systeem van landelijk gedeelde opsporingsinformatie en de cultuur van openheid en vertrouwen die daarvoor nodig is. Tegelijkertijd zal ook in de toekomst sprake blijven van in de HSO ingebakken sturingsproblemen, die niet gemakkelijk overwonnen kunnen worden, ook niet als de uitvoering aan de ingezette veranderingen gewend is geraakt.

Verder blijkt de aard van het politiewerk op verschillende punten te wringen met de openheid die van teams wordt gevraagd bij het landelijk delen van opsporingsinformatie binnen de huidige opzet, waarmee ook de theoretische invalshoek van Manning ook van grote waarde blijkt voor het verklaren van de beperkte informatiedeling tussen Nederlandse korpsen. Met 'huidige opzet' wordt bedoeld dat op dit moment de inhoud van lopende onderzoeken (op enkele uitzonderingen na) raadpleegbaar moet zijn voor andere korpsen. Deze opzet staat intern discussie. Op deze discussie wordt nader ingegaan in de conclusie.

Politiewerk is en blijft spannend, ook in ons kleine Nederland. In hoofdstuk 8 is beschreven welke risico's opsporingsmensen ervaren bij hun

werk, wanneer zij beslissingen nemen over het delen van informatie. De terughoudendheid om informatie landelijk raadpleegbaar te maken en ter beschikking te stellen wordt veroorzaakt door het gevoel dat daarmee de regie over die informatie uit handen wordt gegeven. Het idee bij rechercheurs en teamleiders is dat daardoor onderzoeken bekend kunnen worden bij subjecten en dat de kans toeneemt op een lek naar de pers. Belangen van getuigen en andere betrokkenen bij het onderzoek zijn eveneens van invloed op de terughoudendheid om informatie raadpleegbaar te maken en te delen met een ander team.

Manning volgend zullen verbeterde computersystemen, meer kennis van de techniek en zelfs een verbeterde sturing van de organisatie (vgl. hoofdstuk 7) slechts ten dele de afwegingen van de individuele rechercheur of teamchef kunnen veranderen. De professionals, uitvoerders – zij die uiteindelijk in de onzekere en risicovolle praktijk van het politiewerk moeten handelen, verantwoordelijkheid nemen en beslissen – zullen hun eigen blik op de werkelijkheid behouden en eigen professionele afwegingen blijven maken. De aard van hun werk en de risico's die daarbij ervaren worden, veranderen niet door ander beleid.

In eerdere hoofdstukken kwam naar voren dat op dit moment het kunnen delen (technisch gezien) van informatie duidelijke knelpunten oplevert. Deze knelpunten, het verbeteren van de techniek en het bijscholen van politiemensen, vragen een grote inspanning van de politie, maar de genoemde organisatorische barrières zijn dus van meer structurele aard. De aard van het politiewerk en de aard van de organisatie werpen beide evenzeer (structurele) barrières op voor een optimale informatiedeling. Tegelijkertijd moet hierbij worden vermeld dat bij ruim de helft van de geïnterviewden de wens leeft om bij te dragen aan een werkend systeem van landelijk gedeelde opsporingsinformatie. Deze korte samenvatting geeft aan dat het in deze rapportage gehanteerde theoretisch kader een brede analyse van het probleem van beperkte informatiedeling bij de politie heeft opgeleverd, waaruit diverse verklaringen naar voren zijn gekomen. De resultaten van dit onderzoek worden nog verder beschouwd in de conclusie.

9. Conclusie

In voorgaande hoofdstukken werden tussenconclusies geformuleerd. Aangezien in dit onderzoek een aantal verschillende invalshoeken zijn gekozen om beslissingen betreffende het delen van opsporingsinformatie te kunnen verklaren, is het goed om aan te geven hoe sterk de diverse factoren van invloed zijn. In dit slothoofdstuk worden de tussenconclusies in samenhang gebracht. Hiermee wordt de centrale vraagstelling van dit onderzoek van een antwoord voorzien: ***In hoeverre en onder welke omstandigheden wordt opsporingsinformatie niet (optimaal) uitgewisseld tussen Nederlandse politiekorpsen?***

Ten aanzien van de het algemeen beschrijvende deel uit de centrale vraagstelling kunnen de bevindingen uit dit onderzoek als volgt worden samengevat:

In hoeverre informatie niet of niet optimaal wordt gedeeld kan niet exact worden bepaald. De hoeveelheid informatie die wel wordt gedeeld is niet precies bekend en de totale hoeveelheid beschikbare informatie is geheel niet vast te stellen. Over het algemeen zien informanten het nut van de uitwisseling van opsporingsinformatie voor de opsporing als geheel. Echter in verschillende opzichten wordt afgeweken van het *Beleid Uitwisseling Opsporingsgegevens* waarmee eveneens van wettelijke en technische mogelijkheden om opsporingsinformatie te delen wordt afgeweken.

Geen van de informanten blijkt bereid om altijd informatie in BVO in te voeren wanneer dit zou moeten. Het blijkt dat de invoer in BVO met name een knelpunt vormt binnen teams van de districtsrecherche en dat de leiders van deze teams hier vaak niet sturend op reageren. Twee rekercheteams uit verschillende korpsen werkten vrijwel helemaal in schaduwsystemen.

Een groot deel van de informanten zijn terughoudend bij het raadpleegbaar maken van informatie via BVO en BlueView. Deze terughoudendheid speelt zowel op operationeel als op tactisch niveau een rol. De geïnterviewde teamleiders zijn soms terughoudend bij het ter beschikking stellen van informatie aan een ander team.

Ten aanzien van het verklarende deel uit de centrale vraagstelling kunnen de volgende conclusies worden getrokken:

Kijkend naar de tussenconclusies die eerder in deze rapportage werden gegeven betreffende de diverse deelvragen, blijkt dat informatiedeling niet of nauwelijks door wettelijke regels en voorgeschreven procedures in de weg wordt gestaan. De nieuwe Wet politiegegevens was nog niet bij alle informanten goed bekend maar levert tegelijkertijd geen onbeheersbare problemen op waardoor van informatiedeling af moet worden gezien. Wel is sprake van een juridisch knelpunt ten aanzien van Art. 9 lid 3 Wpg. Eén van de onderzochte korpsen heeft er bezwaar tegen als onderzoeken geraadpleegd kunnen worden zonder dat deze formeel ter beschikking zijn gesteld. Deze kritiek komt aan de kern van de wijze waarop op dit moment opsporingsinformatie via geautomatiseerde systemen plaatsvindt bij de politie. Het landelijk vastgestelde *Beleid Uitwisseling Opsporingsgegevens* schrijft voor dat gegevens raadpleegbaar zijn voor een beperkt aantal infodesk-medewerkers van andere korpsen. Op deze wijze kan het vragende korps het zoekwerk voor zijn rekening nemen. Slechts in een beperkt aantal gevallen kan hierop een uitzondering worden gemaakt.¹

Technologische omstandigheden verklaren de beperkte informatie-uitwisseling beter dan de juridische omstandigheden, die eigenlijk vooral een positieve invloed hebben. Factoren die de acceptatie van de nieuwe ICT in de weg staan zijn van toepassing met name op de knelpunten bij de invoer van informatie. De informanten in dit onderzoek zijn de gebruikers van deze systemen en zij zijn vaak zeer ontevreden. De kwaliteit van BVO en BVH en van de organisatorische implementatie van de basisvoorzieningen (opleiding, inpassing in de werkprocessen) heeft nonchalance gewekt. Problemen met het gebruiksgemak en het faciliteren van gebruikers vormen de belangrijkste knelpunten. Het gebruiksgemak van BVO vormt een drempel voor voldoende invoer van informatie, met name bij de recherche. De CIE kent ook wel problemen met het gebruiksgemak van BVO, echter heeft zij veel minder mogelijkheden om het gebruik ervan te omzeilen. De werkprocessen bij de CIE, zoals ook vereist door de CIE-Regeling, zijn veel meer gericht op het invoeren van informatie in BVO, terwijl de reguliere opsporing de mogelijkheid heeft dossiers op te maken in schaduwsystemen. De belangrijkste klachten zijn:

- BVO is lastig om in te leren werken.
- BVO zit niet logisch in elkaar: er is veel kennis van de “truckjes” nodig.
- Er zijn veel (naar de stand van de computertechniek overbodige) handelingen nodig.

¹ Zie hoofdstuk 3

-De ontbrekende koppeling tussen BVH en BVO. Hierdoor moet veel informatie dubbel worden ingevoerd.

Kennisachterstand en problemen met de koppeling van BVO aan andere systemen die de opsporing gebruikt, zoals BVH en de Gemeentelijke Basisadministratie zijn knelpunten bij de wijze waarop gebruikers worden gefaciliteerd.

Een grote meerderheid van de informanten vindt de toepassing van de systemen wel effectief: ze kunnen meer informatie vinden, al zijn zoekresultaten niet betrouwbaar. Veel informatie is niet in BVO opgenomen.

De inrichting van de basisvoorziening BVO of die van zijn opvolger vraagt veel aandacht in de toekomst. Het is algemeen bekend dat politiemensen in toenemende mate klagen over administratieve lastendruk, waardoor zij minder tijd zouden overhouden voor het 'echte' werk. In die situatie is het extra belangrijk om het gebruik van een nieuw systeem met voldoende kennis en opleiding te ondersteunen en te zorgen dat systemen efficiënt werken en in combinatie met andere systemen die van belang zijn.

De laatste stap in het verklaringsschema om de beperkte informatie-uitwisseling te verklaren, wordt gevormd door de organisatorische omstandigheden. Bij de beschrijving van de organisatorische omstandigheden werd in dit onderzoek gebruik gemaakt van Hasenfeld's begrip van de *Human Service Organization*.

De sturingsproblemen die voortkomen uit de grote zelfstandigheid van zowel rechercheurs als teamchefs, zijn kenmerkend voor een HSO. Verder heeft een korps, als een typische HSO, te maken met tegenstrijdige doelstellingen vanuit een invloedrijke omgeving: onder meer OM en het ministerie van BZK.

De aard van het politiewerk heeft fundamentele gevolgen voor hoe de organisatie in elkaar zit en voor de organisatie van de informatiehuishouding in het bijzonder, stelt Manning. Bij de onderzochte korpsen blijkt dat het belang van vertrouwelijkheid van informatie – een centraal staand thema binnen het opsporingswerk – op verschillende manieren een knelpunt vormt voor informatiedeling tussen korpsen. De invloed van een technisch medium, blijkt daarbij niet zozeer van belang. De terughoudendheid om informatie landelijk raadpleegbaar te maken en ter beschikking te stellen wordt vooral veroorzaakt door het gevoel dat daarmee de regie over die informatie uit handen wordt gegeven. Ook wanneer informatie met slechts één ander team wordt gedeeld, kan dit leiden tot het angstige gevoel dat daardoor onvoorspelbare moeilijkheden kunnen ontstaan, zoals een lek naar de pers. Recherchemensen

maken zich vooral zorgen dat hun onderzoeksactiviteiten bij subjecten bekend worden. Verder zijn uiteraard beroepseer ('we do all the work, they get all the glory'), maar vooral belangen van getuigen en andere betrokkenen bij het onderzoek van invloed op de terughoudendheid om informatie raadpleegbaar te maken en te delen met een ander team.

Nu de uitkomsten van dit onderzoek op een rijtje zijn gezet, is het tijd om een aantal algemene opmerkingen voor de toekomst te maken en enkele aanbevelingen te doen.

9.1 Slotoverweging

Uit de discussie over art. 9 lid 3 Wpg, zoals door één van de onderzochte korpsen wordt aangezwengeld, blijkt hoe wezenlijk verschillend binnen de politie wordt gedacht over het raadpleegbaar maken van informatie uit lopende onderzoeken. Eensgezindheid over landelijke afspraken is cruciaal voor een uniform en krachtig systeem van landelijke uitwisseling van opsporingsinformatie. Om de discussie rondom de samenwerking en het delen van informatie binnen de politie vlot te trekken, is het van belang dit juridische discussiepunt veel aandacht te geven en alle Nederlandse korpsen op één lijn te krijgen waar het gaat om de uitwerking in het *Beleid Uitwisseling Opsporingsgegevens* op dit punt.

De vraag die een buitenstaander bij deze kritiek stelt is: Wat kan het voor kwaad wanneer uw collega's van een ander korps informatie zien, waarvan de vertrouwelijkheid gewaarborgd is en waarvan uw collega's geen gebruik mogen maken zonder uw toestemming? De vraag is eigenlijk: Waarom bent u zo terughoudend informatie met andere korpsen te delen? Het antwoord is dat informatiedeling binnen de politie niet alleen in een positief perspectief wordt gezien. Dat is ook niet voor niets, want informatiedeling kan behalve positieve ook negatieve gevolgen hebben. Hoe klein de kans op negatieve gevolgen ook mogen zijn: het zijn altijd professionals die de betrokken informatie onder ogen krijgen.

Politiemensen kunnen vaak niet alle gevolgen van hun beslissingen overzien. Dat is een vuistregel. Het beheersen van de informatie die teams genereren vergt veel organisatie.² Immers aan eenvoudige zaken wordt gewerkt door één of twee rechercheurs en in gecompliceerde zaken wordt vaak een groot aantal politiemensen ingezet. Beide voorgaande vuistregels versterken elkaar wanneer informatie op landelijke schaal wordt gedeeld. De grilligheid en complexiteit die zo eigen zijn aan het politiewerk, maken dat de gevolgen van

² Poot, C.J. de et al (2004), p. 11

informatiedeling niet altijd overzien kunnen worden. Het is ook om deze reden dat politiemensen geneigd zijn het belang van hun eigen onderzoeken boven dat van een meer abstract belang van een meer effectieve opsporing te stellen. Soms is dat terecht, vaak niet.

Politiewerk is typisch het werk van professionals die snelle beslissingen moet kunnen nemen in onzekere situaties. Een vraag die opkomt is hoe professionele afwegingen ten aanzien van informatiedeling worden gemaakt. Tijdens dit onderzoek zijn slechts enkele voorbeelden genoemd waarbij door toedoen van een ander korps een onderzoek werd beschadigd. De meeste informanten hebben niet direct met zo'n beschadigde zaak te maken gehad. Incidenten die plaatsvinden hebben sommige geïnterviewden erg bezorgd gemaakt en na enige tijd ebden hun zorgen weer weg. Waarschijnlijk zal de bereidheid om informatie te delen toenemen naarmate politiemensen beter gewend raken aan de samenwerking met andere korpsen, incidenten uitblijven en meer vertrouwen ontstaat dat de vertrouwelijkheid van informatie is gewaarborgd.

Informatiedeling via een strak protocol is lastig verenigbaar met de snelle, onzekere afwegingen die individuele teams en politiemensen dagelijks moeten maken. Met voldoende begrip voor de onzekere positie waarin rechteerteams zich bevinden, kunnen teams bekend worden gemaakt met procesbeschrijvingen bedoeld om op een snelle, efficiënte wijze goede afweging te maken tussen de verschillende belangen die een rol spelen bij het delen van informatie: genoemde belangen die bij een opsporingsonderzoek een rol kunnen spelen enerzijds, en het belang van een krachtige informatiehuishouding anderzijds. Op dit moment zijn de uitzonderingen die door de Wet politiegegevens en het *Beleid Uitwisseling Opsporingsgegevens* worden toegestaan nog maar weinig ingeburgerd. De ruim geformuleerde uitgangspunten van het *Beleid Uitwisseling Opsporingsgegevens* leiden tot nu toe niet tot eenduidige besluitvormingsprocessen binnen korpsen en binnen teams. De onderlinge verschillen tussen korpsen en tussen teams zijn groot en die moeten worden weggewerkt.

Op diverse manieren wordt het werk van politiekorpsen gestuurd. Om een systeem van landelijk gedeelde opsporingsinformatie te realiseren (zoals met de samenwerkingsafspraken 2008 beoogd), wordt van de korpsen gevraagd tijd te reserveren voor onder meer het invoeren van opsporingsinformatie in BVO. Als het ware wordt daarbij aangenomen dat de informatie die vervolgens via BlueView landelijk beschikbaar komt in de korpsen de opsporing effectiever zal maken, waardoor de tijd die in het invoeren van de informatie vanzelf wordt

teruggewonnen. Dit effect is echter pas aannemelijk na verloop van jaren en de invloed van een individueel korps op dit effect zal beperkt blijven. In de huidige situatie waarin korpsen worden afgerekend op resultaten van het opsporingswerk, betekent dat concreet een stimulans voor het individuele korps om maximaal in te zetten op opsporingsactiviteiten en dus minder op informatiedeling. Dat zou er in theorie toe kunnen leiden dat een individueel korps als het ware profiteert van de informatie van andere korpsen zonder daarbij een wezenlijke bijdrage te leveren aan de uitwisseling met andere korpsen. Deze inzet van prestatieafspraken leidt ertoe dat het behalen van de doelstellingen op het terrein van de informatiehuishouding wordt tegengewerkt. Het zou daarom goed zijn als er meer aandacht komt voor het belang van informatiedeling in de prestatierelaties met de korpsen.

Deze overwegingen en denkrichtingen voor de toekomst, leiden tot onderstaande aanbevelingen.

9.2 Aanbevelingen

1. De Nederlandse korpsen dienen op één lijn te komen waar het gaat om de landelijke raadpleegbaarheid van informatie uit lopende onderzoeken. Concreet dient art. 9 lid 3 Wpg in het *Beleid Uitwisseling Opsporingsgegevens* te worden uitgewerkt. In de discussie daarover behoren de aard van het politiewerk en sturingskenmerken van de politieorganisatie voldoende gewicht te krijgen.
2. Op dit moment vormt de benodigde tijd voor het werken met de basisvoorzieningen een knelpunt. Een behoorlijk niveau van gebruiksgemak van individuele opsporingssystemen, de koppeling tussen opsporingssystemen onderling en waar nodig tussen handhavings- en opsporingssystemen zijn noodzakelijke voorwaarden om de tijdsinvestering voor medewerkers te verminderen en daarmee voor een succesvolle uitwisseling van informatie binnen de politie.
3. Opleiding en sturing op de gewenste werkprocessen binnen teams dienen hand in hand te gaan en kunnen zorgen voor een betere invoer van informatie.

4. Het uitwisselen van informatie is niet in de eerste plaats afhankelijk van de techniek die wordt ingezet. Een succesvolle uitwisseling kan worden gestimuleerd door te werken aan het vertrouwen tussen teams en korpsen onderling.
5. Top-down sturing binnen de korpsen zal gegeven de aard van de politieorganisatie niet tot succes kunnen leiden. Gelet op de complexiteit en daaruit voortvloeiende onvoorspelbare risico's van het politiewerk, dient de professionaliteit van politiemensen bij het maken van individuele beslissingen gerespecteerd te blijven.
6. Uitgangspunten vanuit het *Beleid Uitwisseling Opsporingsinformatie* zijn zeer algemeen gesteld. Meer uitgebreide procesbeschrijvingen over welke stappen gevolgd moeten worden bij beslissingen over het raadpleegbaar maken en delen van informatie, kunnen hierop een aanvulling zijn. Deze processen bieden vervolgens een goed aanknopingspunt voor sturing binnen de korpsen.
7. De formele positie van informatiedeling in de prestatierelaties van OM en het ministerie van BZK met de korpsen kan worden versterkt, waardoor doelstellingen op dit terrein minder spanning vertonen met andere afspraken waar de korpsen aan worden gehouden.

Lijst van veelgebruikte afkortingen

Bpg	Besluit politiegegevens
BPS	BasisProcessenSysteem
BVH	Basisvoorziening Handhaving
BVCM	Basisvoorziening Capaciteitsmanagement
BVO	Basisvoorziening Opsporing
BZK	Binnenlandse Zaken en Koninkrijksrelaties
CBP	College Bescherming Persoonsgegevens
CIE	Criminele Inlichtingen Eenheid
HKS	HerkenningsSysteem
HSO	Human service organization
ICT	Informatie- en communicatietechnologie
IOOV	Inspectie OOV Inspectie Openbare Orde en Veiligheid
KBB	Korpsbeheerdersberaad
KLPD	Korps landelijke politiediensten
ME	Mobiele eenheid
MRO	Melding Recherche Onderzoek
RBS	Recherche Basis Systeem
RHC	Raad van Hoofdcommissarissen
TGO	Team Grootschalige Opsporing
VG's	Verzorgingsgebieden
VROS	Verwijsindex rechercheonderzoeken en subjecten
vtspN	Voorziening tot samenwerking Politie Nederland
Wpolr	Wet politieregisters
Wpg	Wet politiegegevens
ZwaCri	Zware criminaliteit

Literatuurlijst

- Aalberts M.M.J., H.G. van de Bunt (1994), *Politieële waarheden*. Tijdschrift voor de Criminologie, 36
- Babbie, E. (2004) The practice of social research,
- Bel, D. van der (2007), Informatie en Opsporing, Studiecentrum rechtspleging, Zeist
- Bekkers, V., M. Thaens, G. van Straten en P. Siep (2009), *Informatiemanagement binnen de politie. Van praktijk naar normatief kader*. Politiekunde 23, Politie & Wetenschap, Apeldoorn
- Dijkstra et al (2006), Towards a Multi-agent system for regulated information exchange in crime investigations. Artificial Intelligence and Law, nr. 13
- Geurts, P. (1999), Van probleem naar onderzoek, Coutinho, Bussum
- Hasenfeld, Y. (1983) *Human service organizations*, Prentice Hall, Englewood Cliffs
- Huberts, L.W.J.C. (2007), *Politiebestel in de praktijk: sturing en invloed*, in: Fijnaut, C.J.C.F., Muller, E.R. & Rosenthal, U (red.), Politie: Studies over haar werking en organisatie, Deventer: Kluwer
- Hutjes, J.M., Buuren, J.A. van (1992), De gevalsstudie: strategie van kwalitatief onderzoek, Boom, Meppel
- Manning, P.K. (2001). 'Technology's ways: Information technology, crime analysis, and the rationalizing of policing. Criminal Justice, 1
- Manning, Peter K. (2005), *Environment, Technology, and Organizational Change*, in: Pattavina, A. (ed.), Information technology and the criminal justice system, Sage
- Meyer, J. en B. Rowan (1977). "Institutionalized Organizations: Formal Structure as Myth and Ceremony," *American Journal of Sociology* 83
- Pattavina, A (2005), The future of information technology in the criminal justice system, in: Pattavina, A. (ed.), Information technology and the criminal justice system, Sage
- Poot, C.J. de et al (2004), *Rechercheportret, over de dilemma's in de opsporing*, Kluwer, Alphen aan den Rijn
- Stol, W.Ph. (2007) 'Informatie voor politiewerk: basisprincipes', in: Fijnaut, C.J.C.F., Muller, E.R. & Rosenthal, U (red.), Politie: Studies over haar werking en organisatie, Deventer: Kluwer
- Venkatesh et al (2003), *User Acceptance of Information Technology: Toward a Unified View*, MIS Quarterly, Vol. 27, No. 3, pp. 425-478

Wilensky, H. (1975), *The welfare state and Equality*. Berkeley: University of California Press

Zuurmond, A. en Meesters, M.J. (2007). *ICT en de moderne politieorganisatie*, in: *Politie, studies over haar werking en organisatie*

Geraadpleegde bronnen

ABRIO (2005), *Informatie-gestuurde politie, sturen op resultaat*

Autorisatiemodel BVO, 30 mei 2007

Beleid Uitwisseling Opsporingsinformatie

BlueView Gegevensbeveiliging, 15 oktober 2007

BZK (1999). Brief aan de Tweede Kamer over de stand van zaken politieke informatiehuishouding (U76403). Den Haag

CBP (2008), *Politie Infodesk; onderzoek naar de inrichting van de politie infodesk en de waarborgen voor de bescherming van persoonsgegevens*, Den Haag

CBP (2009), *Politie Infodesk II, onderzoek naar de waarborgen voor de bescherming van persoonsgegevens bij de Infodesk: rapportage van definitieve bevindingen*, Den Haag

Coalitieakkoord *Samen werken, samen leven*. Kamerstukken II, 2006-2007, 30891, nr. 4

Evaluatie Wet bijzondere politieregisters, uitgevoerd door de Erasmus Universiteit en Net2legal Consultant & Mazars, in opdracht van het Ministerie van Justitie en BZK, onder begeleiding van het WODC

Inspectie OOV (2008), *Samenwerkingsafspraken 2008*, Den Haag

Inspectie OOV (2008a), *Informatiegestuurde politie*, Den Haag

Memorie van toelichting Wet politiegegevens: Kamerstukken II 2005-2006, 30327, nr. 3

Parlementaire Enquêtecommissie Opsporingsmethoden (1996) *Inzake opsporing*, SDU, Den Haag

Raad van Hoofdcommissarissen (2005), *Politie in Ontwikkeling*, NPI, Den Haag

Raad van Hoofdcommissarissen (2006), *Wenkend Perspectief*, Politie Nederland, Driebergen

Raad van Hoofdcommissarissen (2008), *Programmaplan Intelligence 2008: Sturing, Informatieorganisatie, Verbetering en Innovatie*

Samenwerkingsafspraken politie 2008. Kamerstukken II, 2007-2008, 30880, nr. 6

Tweede Kamer (2000). *Brief van de minister van Binnenlandse Zaken en Koninkrijksrelaties, Beleidsplan Nederlandse Politie*. 26345, nr. 11

Abstract

Door onder meer de opkomst van complexere vormen en door 'ontgrenzing' van criminaliteit in de afgelopen jaren, is het belang van een goede informatiehuishouding voor de effectiviteit van de opsporing verder toegenomen. Tegen deze achtergrond stelt de vooruitgang van de computertechniek de politie voor de vraag, hoe zij daarvan optimaal kan profiteren. Grote inspanningen op het terrein van de informatiehuishouding, hebben tot op heden niet tot het gewenste resultaat van een goed werkend systeem van landelijk gedeelde politie-informatie geleid. Zo blijkt uit publicaties van de Inspectie Openbare Orde en Veiligheid en ook uit dit onderzoek. In hoeverre informatie niet of niet optimaal wordt gedeeld kan niet exact worden bepaald. De hoeveelheid informatie die wel wordt gedeeld is niet precies bekend en de totale hoeveelheid beschikbare informatie is geheel niet vast te stellen. Over het algemeen zien geïnterviewden het nut van de uitwisseling van opsporingsinformatie voor de opsporing als geheel. Echter in verschillende opzichten wordt afgeweken van het *Beleid Uitwisseling Opsporingsgegevens* waarmee eveneens van wettelijke en technische mogelijkheden om opsporingsinformatie te delen wordt afgeweken. Onderzocht is in hoeverre juridische, technische en organisatorische knelpunten de beperkte informatiedeling tussen Nederlandse politiekorpsen kunnen verklaren. Voor dit onderzoek is literatuurstudie verricht, zijn documenten bestudeerd en hebben interviews plaatsgevonden met politiemedewerkers op operationeel, tactisch en strategisch niveau in vijf verschillende korpsen. Gebleken is dat informatiedeling niet of nauwelijks door wettelijke regels en voorgeschreven procedures in de weg wordt gestaan. Technologische omstandigheden verklaren de beperkte informatie-uitwisseling beter dan de juridische omstandigheden, die eigenlijk vooral een positieve invloed hebben. Factoren die de acceptatie van de nieuwe ICT in de weg staan zijn van toepassing met name op de knelpunten bij de invoer van informatie. De informanten in dit onderzoek zijn de gebruikers van deze systemen en zij zijn vaak zeer ontevreden. Problemen met het gebruiksgemak en het faciliteren van gebruikers vormen de belangrijkste knelpunten. Kennisachterstand en problemen met de koppeling tussen diverse systemen die de opsporing gebruikt zijn knelpunten bij de wijze waarop gebruikers worden gefaciliteerd. Een grote meerderheid van de informanten vindt de toepassing van de systemen wel effectief: ze kunnen meer informatie vinden, al zijn zoekresultaten niet betrouwbaar. Veel informatie is nog niet opgenomen. Op organisatorisch vlak zijn de voor de politie kenmerkende sturingsproblemen voortkomend uit de grote zelfstandigheid van zowel rechercheurs als teamchefs,

ook van toepassing op het probleem van de beperkte informatiedeling. Daarnaast hebben korpsen te maken met tegenstrijdige doelstellingen vanuit een invloedrijke omgeving: onder meer OM en het ministerie van BZK. Tot slot heeft de aard van het politiewerk fundamentele gevolgen voor hoe de organisatie in elkaar zit en voor de organisatie van de informatiehuishouding in het bijzonder. Bij de onderzochte korpsen blijkt dat het belang van vertrouwelijkheid van informatie – een centraal staand thema binnen het opsporingswerk – op verschillende manieren een knelpunt vormt voor informatiedeling tussen korpsen. Recherchemensen maken zich vooral zorgen dat hun onderzoeksactiviteiten bij subjecten bekend worden of lekken naar de pers. Verder zijn beroepseer ('we do all the work, they get all the glory'), maar vooral belangen van getuigen en andere betrokkenen bij het onderzoek van invloed op de terughoudendheid om informatie raadpleegbaar te maken en te delen met andere korpsen en opsporingsteams.

Summary

Information is crucial in policing. Information plays an important role in law enforcement and in assistance tasks as well. Information is at the heart of crime investigations, in which the collection and processing of information is crucial. This refers to the title of this report: *Open je hart*, or: open your heart. In some cases, information known to the police is of vital importance for citizens and for its own employees. Because of its investigative powers and its 24-hour presence in society, the police have specific responsibilities concerning signaling and advisory towards its partners.

People who are followed by the police appear in different police regions and move well across national borders. It is therefore obvious that forces independently collect information on the same people. It is usually very important that this information is put together. It is essential that useful and accurate information is shared between the various police forces and service units engaged in carrying out police duties. Striking is the importance of information exchange on the detection process, but it can also support strategic and tactical decisions.

Developments in the field of information and communication technologies (ICTs in recent decades, have opened new possibilities for information within the police.

However, adequate information management shows a complex task for Dutch police. Around the year 2000, the Minister of the Interior and Kingdom Relations stated that the police automation and computerization could no longer meet the demands of the modern age. He reported to the Dutch Parliament that several areas had a backlog. Information infrastructure was obsolete, the renewal of applications and systems insufficient, coordination between the forces inadequate and the conditions for a transparent management weren't optimal. One explanation for the delay according to the ministry, were internal affairs due to the police reorganization in 1993-1994. It followed that the police didn't spend enough effort in order to improve its information exchange.

In order to help achieving main objectives concerning cooperation and information exchange, the Ministers of the Interior and Justice made an agreement with the regional police force managers (korpsbeheerders), known as the 2008 police cooperation agreement (Samenwerkingsafspraken 2008). Part of the agreement was that the Dutch Public Order and Safety Inspectorate would examine the results police forces obtained from mid-2008.

Agreements concerning ICT systems designed to support law enforcement (Basisvoorziening Handhaving) respectively criminal investigations (Basisvoorziening Opsporing) were reviewed by the Inspectorate. BVH is a nationwide information system for all core processes of the police. It supports the registration of notifications from citizens, the processing of police reports and incident handling. BVO is a national and uniform information system that manages information from crime investigations and also supports information exchange. BlueView is a search engine linked to both information on law enforcement and investigation, and can be directly consulted by all Dutch police forces. BVH data and certain data from BVO are accessible, in addition to data from several other information systems that are to be replaced. For example the "Recherche Basis Systeem" (RBS) and "Octopus".

The research report of the inspection published November 2008, showed that three arrangements from the 2008 cooperation agreement were not fully met. It was concluded that the planned information sharing between police forces, not fully existed. The investigation revealed, inter alia, a certain reluctance by police employees in providing investigative information to each other.

The Inspectorate concluded in its report that police forces decide independently on the sharing of information. They decide whether or not to enter information in BVO or in other cases, information gets an excessive classification to prevent police employees to access the information other than by members of the Criminal Intelligence Unit (Criminele Inlichtingen Eenheid; CIE). In particular serious crime cases should be kept out of BlueView, according to a number of police employees interviewed by the inspectorate. The Inspectorate also found that cases were "shrunk". Cases less than 40 hours do not require to be introduced in BVO, with the result that they cannot be shared nationwide in Blue View. Because of these conclusions, the Inspectorate executed a follow-up study, published in May 2010. It also commissioned for this research.

The purpose of this research is twofold, namely a detailed description of the limitations in information exchange between police forces identified by the Inspectorate. Second, this study aims to find explanations for these limitations. This dual aim leads to the following central question:

To what extent and under what circumstances, investigative information is not (fully) exchanged between Dutch police forces?

On the basis of the following sub-questions, an answer to this central question will be provided:

1. What is the policy within the Dutch police regarding the exchange of investigative information between police forces?
2. What characteristics apply to information that is not (fully) shared, and which actors, do not (fully) share their information?
3. To what extent is the exchange of information between Dutch police forces limited by legal rules?
4. To what extent is the exchange of information between Dutch police forces limited by technological problems?
5. To what extent is the exchange of information between Dutch police forces limited by organizational characteristics of the police?

As stated earlier, it was because of the emergence of complex forms of crime and of international crime in recent years, that the importance of good information management for the effectiveness of the detective force increased. Against this background, advances in computer technology questioned the police: how can we benefit? However, great efforts in the field of information management have to date not achieved the desired result of an effective national system of information led police. This shows from for example publications of the Public Order and Safety Inspectorate and also this investigation. To what extent information is not shared cannot be precisely determined. The amount of information that is being shared is not precisely known and the total amount of available information is not completely fixed. In general, interviewees see the usefulness of the exchange of investigative information for the investigation as a whole. However, in many respects a deviation from the policy on information exchange can be observed. This study examined the extent to which legal, technical and organizational problems can explain the limited sharing of investigative information. For this study, literature and document study have taken place and interviews were held with police officers at the operational, tactical and strategic levels in five different police forces. It appeared that legal rules and procedures prescribed do not oppose to information exchange. It's

quite the opposite. Particularly technological conditions well explain the limited exchange of information. Factors affecting the acceptance of new ICTs apply in particular to bottlenecks at the entry of information. The informants in this study are the users of these systems and they are often very unhappy. Problems with the ease of use and facilitating users are the main bottlenecks. Lack of knowledge and problems in the linking of various systems used, can be observed. A large majority of the informants find the application of the new ICT systems effective, as they can find out more, although they say: search results are not reliable for much information is not yet included in the databases. The limited information sharing can be further explained by organizational problems. Yeheshel Hasenfels work on the Human Service Organisation helped describing specific police management problems arising from for example the large autonomy of both investigators and team principals. In addition, police forces have to deal with conflicting from for example the Ministry of the Interior and also the Public Prosecutor. Further, as follows from Peter Manning's work on the relation between police work and ICT, it appeared that the fundamental nature of police work also has implications for the information exchange within the police. Police work dictates how the organization works and the organization of information management in particular. Interviewees are particularly worried that their research activities might leak to their research subjects or to the press. In some cases, this prevents them from sharing their information. Furthermore interests of witnesses and others involved in the investigation affect this so called reluctance.

