Gegevensuitwisseling door Toezichthouders

Onderzoek uitgevoerd in opdracht van het WODC

Prof. dr. A.J.C. de Moor-van Vugt
Prof. dr. T.M. van Engers
Dr. F.T. Groenewegen
Mr. W.F. van Haaften
Dr. A.P. Klap
Dr. A.J. Nieuwenhuis
Mw. L.M. Schouten (onderzoeksassistentie)
Mr. drs. M.W. Wessel (onderzoeksassistentie)

Universiteit van Amsterdam

Faculteit der Rechtsgeleerdheid
Amsterdam, juni 2012

Gegevensuitwisseling door Toezichthouders

Onderzoek uitgevoerd in opdracht van het WODC

UNIVERSITEIT VAN AMSTERDAM

Inhoudsopgave

Inhoudsopgave 1

Lijst van afkortingen 7

Samenvatting 9

Betrokken belangen en juridische erkenning ervan 9

Waardering van belangen 10

Organisatiebelang en transparante afwegingsprocessen 11

(G)een algemene regeling 13

Aanbevelingen 14

1. Inleiding en probleemstelling 15

1.1 Aanleiding voor het onderzoek 15

1.1.1 Probleemstelling en onderzoeksvragen 17

1.2 Uitwerking en aanpak van de onderzoeksvragen 17

1.2.1 Vraag I: Betrokken belangen 18

1.2.2 Vraag II: Algemene regeling 21

1.3 Methoden van onderzoek 22

1.4 Beperkingen 23

1.5 Onderzoeksteam en begeleidingscommissie 24

1.6 Opbouw van het rapport 24

2. Het juridisch kader bij gegevensuitwisseling 25

2.1 Inleiding 25

2.2 Toezichtgegevens 25

2.3 Persoonsgegevens 26
2.3.1 Grondrechtelijke achtergrond 26
2.3.2 Het EU-kader voor gegevensbescherming 27
2.3.3 Overlap en onderscheid 29
2.3.4 De term persoonsgegeven in de Wbp 29
2.3.5 Persoonsgegevens – bedrijfsgegevens 30
2.3.6 Bijzondere persoonsgegevens 31
2.3.7 Persoonsnummers 32
2.3.8 Verhouding Wbp, Wpg en Wjsg 32
2.4 Doelbinding 33
2.4.1 Gerechtvaardigde verwerkingen 34
2.4.2 Het uitgangspunt van doelbinding 34
2.4.3 Voldoende verwantschap: dubbele doelbinding 35
2.4.4 Jurisprudentie doelbinding 36
2.4.5 Doelbinding in de Wpg 36
2.5 Uitwisseling van persoonsgegevens 36
2.5.1 Koppelen en de Wbp 37
2.5.2 Risico-profielen 38
2.5.3 Verstrekkingen op grond van de Wpg en de Wjsg 38
2.5.4 Samenwerkingsverbanden 41
2.5.5 Convenanten 43
2.6 Geheimhoudingsplichten 45
2.6.1 Geheimhoudingsplicht Belastingdienst 46
2.6.2 Geheimhoudingsplicht financieel toezicht 47
2.7 Juridische vragen bij gegevensuitwisseling 49

3. Inventarisatie en weging van belangen 51
3.1 Methoden van onderzoek 51
3.1.1 Casus 51
3.1.2 Enquête 52
3.1.2.1 Uitvoering enquête 52
3.1.2.2 Vragen 53
3.1.3 Expertmeeting 54
3.2 Casusbeschrijving en uitkomsten 54
3.2.1 Casus Taxivervoer 54
3.2.1.1 Juridisch kader inzake de gegevensuitwisseling 55
3.2.1.2 Samenwerking met gegevensverstrekkers en -ontvangers Taxiconvenant G4 55
Taxi-database 55
Samenwerkingspartners 56
3.2.1.3 Soorten gegevens 56
3.2.1.4 Ervaringen en knelpunten 56
3.2.1.5 Behoefte aan een wettelijke regeling? 57
3.2.2 Casus Gegevensuitwisseling samenwerkend toezicht belastingheffing 57
3.2.2.1 Juridisch kader inzake gegevensuitwisseling 57
3.2.2.2 Samenwerking gegevensverstrekkers en -ontvangers 57
3.2.2.3 Soorten gegevens 58

1912170 01165

3.2.2.4 Doelbinding ... 58
3.2.2.5 Geheimhouding en verstrekking aan derden ... 59
3.2.2.6 Ervaringen en knelpunten ... 59
3.2.2.7 Behoefte aan een wettelijke regeling? ... 60
3.2.3 Casus Vuurwerk ... 61
3.2.3.1 Juridisch kader inzake de gegevensuitwisseling ... 61
3.2.3.2 Samenwerking met gegevensverstrekkers en –ontvangers ... 61
3.2.3.3 Soort gegevens ... 61
3.2.3.4 Bijzondere persoonsgegevens ... 61
3.2.3.5 Doelbinding ... 61
3.2.3.6 Geheimhouding en verstrekking aan derden ... 62
3.2.3.7 Ervaringen en knelpunten ... 62
3.2.3.8 Behoefte aan een wettelijke regeling? ... 63
3.3 Expertmeeting en uitkomsten ... 64
3.3.1 Organisatie specifieke punten ... 64
3.3.2 Onduidelijkheid bij verstrekking ... 65
3.3.3 Onduidelijk zicht van verstrekker op gebruik ... 65
3.3.4 Kleuring van gegevens en betrouwbaarheid voor hergebruik ... 65
3.3.5 Organisatorische aspecten van gegevensuitwisseling ... 66
3.3.6 Technische ontwikkelingen ... 66
3.3.7 Algemene regeling? ... 66
3.4 Enquêteresultaten en MCA ... 67
3.5 Resultaten ... 68
3.5.1 Juridisch kader ... 69
3.5.2 Samenwerking en basis voor uitwisseling ... 69
3.5.2.1 Soorten gegevens ... 70
3.5.3 Ervaringen en knelpunten/Betrokken belangen en weging ... 70
3.5.3.1 Gefragmenteerde regelgeving ... 70
3.5.3.2 Ontbreken verplichting tot informatieverstrekking ... 70
3.5.3.3 Praktische problemen ... 70
3.5.3.4 Onduidelijkheid bij verstrekking ... 71
3.5.3.5 Geen zicht op doeleinden gebruik bij doorverstrekking ... 71
3.5.3.6 Kleuring van gegevens en betrouwbaarheid voor hergebruik ... 71
3.5.4 Enquête ... 72
3.5.4.1 Behoefte aan een wettelijke regeling ... 72
4. Naar een algemene regeling? ... 73
4.1 Inleiding ... 73
4.2 Regeling in de Awb? ... 74
4.3 Regeling in een kaderwet? ... 74
4.4 Een nieuwe kaderwet of een omgebouwde Wbp? ... 74
4.5 De rol van convenanten ... 75
4.6 Problemen met betrekking tot de eis van doelbinding ... 75
4.6.1 Verwantschap tussen doelen ... 76
4.6.2 Een concreet, direct toepasbaar criterium ... 76
4.6.3 Het vervallen van het element van verwantschap ... 77
4.6.5 Specifieke opsomming van gevallen waarin verdere verwerking is toegestaan ... 78

4.7 Andere problemen **79**
4.7.1 Een wettelijke verplichting tot gegevensverstrekking? 79
4.7.2 De kwaliteit van de te verstrekken of verstrekte gegevens 80
4.7.3 De interpretatie van de verstrekte gegevens 80

5. Conclusies en aanbevelingen **81**
5.1 Inleiding **81**
5.2 Deelvragen 1 en 2: de bij de uitwisseling van toezichtgegevens betrokken belangen en belanghebbenden **82**
5.2.1 Uitgangspunten inventarisatie 82
5.2.2 Resultaat inventarisatie 83
5.2.3 Samenvatting belangen 84
5.3 Deelvragen 4 en 5: juridische erkenning van de gevonden belangen **85**
5.3.1 Deelvraag 4: juridisch gelabelde belangen 85
5.3.1.1 De bescherming van persoonsgegevens 85
5.3.1.2 De bescherming van bedrijfs- en fabricagegegevens 86
5.3.1.3 Geheimhoudingsplichten 86
5.3.1.4 Eigen verantwoordelijkheid voor doorverstrekking 86
5.3.2 Deelvraag 5: niet juridisch erkende belangen 87
5.3.2.1 Samenwerkende overheden 87
5.3.2.2 Efficiency en effectiviteit 88
5.3.2.3 Kwaliteit van gegevens 88
5.4 Deelvragen 3 en 6: onderlinge verhouding van betrokken belangen **89**
5.4.1 Samenvatting van de enquêteresultaten en MCA 89
5.4.2 Het organisatiebelang als overkoepelend belang 90
5.4.3 Het strategische belang van de geheimhoudingsplicht 91
5.4.4 Convenanten zijn geen panacee 91
5.4.5 Ruimte voor afweging? 92
5.5 Deelvragen 7 en 8: naar een algemene regeling? **93**
5.5.1 Geen grote behoefte aan een algemene regeling 93
5.5.2 Opties voor een regeling 94
5.6 Aanbevelingen **96**

6. Geraadpleegde bronnen **97**
6.1 Convenanten **97**
6.2 Literatuur **98**
Boeken, dissertaties, oraties 98
Artikelen 98
Rapporten en adviezen 99
6.3 Regelgeving en beleidstukken **101**
EU 101
Duitsland 101
Nederland 101
Kamerstukken 101
Beleid lagere overheden 102
6.4 Jurisprudentie **103**

1912170 01165

Europees Hof voor de Rechten van de Mens 103
Hof van Justitie van de Europese Gemeenschappen / Europese Unie 103
Nederland 103
Hoge Raad 103
Afdeling Bestuursrechtspraak Raad van State 104
Centrale Raad van Beroep 104
Gerechtshoven 104
Gerechtshof Amsterdam 104
Gerechtshof Arnhem 104
Gerechtshof 's-Gravenhage 104
Rechtbanken 104
Rechtbank Amsterdam 104
Rechtbank Arnhem 104
Rechtbank 's-Gravenhage 104
Rechtbank 's-Hertogenbosch 104
Rechtbank Haarlem 104
Rechtbank Leeuwarden 104
Rechtbank Middelburg 105
Rechtbank Roermond 105
Rechtbank Rotterdam 105
Rechtbank Utrecht 105
Rechtbank Zwolle 105
College Bescherming Persoonsgegevens 105

7. Bijlagen 107
7.1 CV Onderzoekers 107
7.2 Vragen enquête en resultaten 109
7.2.1 Resultaten 109
7.2.2. Enquêtevragen 125
MCA Enquête 1 125
MCA Enquête 2 134
MCA Enquête 3 139
7.3 Lijst deelnemers Expertmeeting 29 februari 2012 145
Experts 145
Begeleidingscommissie 145
Onderzoeksteam 145

Lijst van afkortingen

AFM	Autoriteit Financiële Markten
AMvB	Algemene Maatregel van Bestuur
Awb	Algemene wet bestuursrecht
Awr	Algemene wet inzake rijksbelastingen
B&W	Burgemeester en wethouders
BSN	Burgerservicenummer
BZK	Binnenlandse Zaken
CBP	College bescherming persoonsgegevens
CBR	Centraal Bureau Rijvaardigheidsbewijzen
CCV	Centrum voor Criminaliteitspreventie en Veiligheid
CIE	Criminele Inlichtingen Eenheid
CRvB	Centrale Raad van Beroep
DNB	De Nederlandsche Bank
DPG	Dienst Persoons- en Geo-informatie
EHRM	Europees Hof voor de Rechten van de Mens
EMM	Expertisecentrum Mensenhandel en Mensensmokkel
EU	Europese Unie
EVRM	Europees Verdrag tot bescherming van de Rechten van de Mens
FIOD-ECD	Fiscale Inlichtingen- en Opsporingsdienst - Economische Controledienst
GBA	Gemeentelijke Basisadministratie Persoonsgegevens
HR	Hoge Raad
HvJ	Hof van Justitie (EU)
IVG	Inspectie Volksgezondheid
KLPD/DNR	Korps landelijke politiediensten / Dienst nationale recherche
KvK	Kamer van Koophandel
LNV	Landbouw, Natuur en Voedsel

1912170 01165

LSI	Landelijke Stuurgroep Interventieteams
MCA	Multicriteria-analyse
MKZ	Mond-en klauwzeer
MvT	Memorie van Toelichting
NMa	Nederlandse Mededingingsautoriteit
NVWA	Nederlandse Voedsel- en Warenautoriteit
NZa	Nederlandse Zorgautoriteit
OM	Openbaar Ministerie
Opta	Onafhankelijke Post en Telecommunicatie Autoriteit
PbEG	Publicatieblad van de Europese Gemeenschappen
PbEU	Publicatieblad van de Europese Unie
Pw	Pensioenwet
Rb	Rechtbank
RCF	Regionale Coördinatiepunten Fraudebestrijding
RDW	Rijksdienst voor het wegverkeer
RIEC	Regionale Informatie- en Expertise Centra
RUG	Rijksuniversiteit Groningen
RvK	Raad van Kerken
SIOD	Sociale Inlichtingen- en Opsporingsdienst
Stcrt	Staatscourant
Sv	Wetboek van Strafvordering
SZW	Sociale Zaken en Werkgelegenheid
TNO	Nederlandse organisatie voor toegepast-natuurwetenschappelijk onderzoek
TTO	Toegelaten taxi organisatie
UvA	Universiteit van Amsterdam
UWV	Uitvoeringsinstituut Werknemers Verzekeringen
VIC	Vastgoed Intelligence Center
VNG	Vereniging van Nederlandse Gemeenten
VOG	Verklaring omtrent gedrag
VROM	Volkshuisvesting, Ruimtelijke Ordening en Milieubeheer
VROM-IOD	Inlichtingen- en opsporingsdienst van het Ministerie van Volkshuisvesting, Ruimtelijke Ordening en Milieubeheer
VU	Vrije Universiteit
VWEU	Verdrag betreffende de werking van de Europese Unie
Wbp	Wet bescherming persoonsgegevens
Wet Bibob	Wet bevordering integriteitsbeoordelingen door het openbaar bestuur
Wft	Wet op het financieel toezicht
Wjsg	Wet justitiële en strafvorderlijke gegevens
Wob	Wet openbaarheid van bestuur
WODC	Wetenschappelijk Onderzoek- en Documentatiecentrum
Wpg	Wet politiegegevens
WRR	Wetenschappelijke Raad voor het Regeringsbeleid
Wta	Wet toezicht accountantsorganisaties
Wvb	Wet verplichte beroepspensioenregeling
WVW	Wegenverkeerswet
Wwb	Wet werk en bijstand

Samenvatting

Dit onderzoek is gericht op het beantwoorden van de vraag met welke belangen rekening moet worden gehouden bij de verstrekking van toezichtgegevens tussen toezichthouders onderling en tussen toezichthouders enerzijds en het Openbaar Ministerie, de politie en de buitengewoon opsporingsambtenaren anderzijds. Daarnaast wordt de vraag onderzocht in hoeverre het gewenst en juridisch mogelijk is om voor het verstrekken van toezichtgegevens tussen genoemde partijen een algemene regeling in de Algemene wet bestuursrecht en/of eventuele andere wetten op te nemen.

Betrokken belangen en juridische erkenning ervan

Om de belangen die spelen rond gegevensuitwisseling tussen toezichthouders en de weging ervan te inventariseren is gekozen voor een aanpak door middel van bestudering van de relevante stukken, een quickscan, casus, gesprekken met ervaringsdeskundigen, een expert-meeting en een internetenquête onder ervaringsdeskundigen op de werkvloer ten behoeve van een Multicriteria-analyse. In paragraaf 1.3 en 3.1 zijn de onderzoeksmethoden nader toegelicht.

Uit het onderzoek blijkt dat gaat het om een uiteenlopend palet van belangen. In de eerste plaats zijn dat de belangen van de in deelvraag 1 genoemde inspectie- en opsporingsdiensten, de toezichthoudende functionarissen en opsporingsambtenaren. In de tweede plaats zijn dat de belangen van de in deelvraag 2 bedoelde andere belanghebbenden, te weten onder toezicht gestelde burgers en bedrijven en hun vertegenwoordigers. Deze belanghebbenden hebben ieder vanuit hun eigen positie belang bij de uitwisseling van gegevens. In paragraaf 3.2, 3.3 en 3.4, alsmede in bijlage 7.2 zijn de gedetailleerde resultaten te vinden van de

1912170 01165

inventarisatie van belangen. Het antwoord op de vraag welke belangen een rol spelen hangt af van de soort gegevens die zullen worden uitgewisseld. Zoals in hoofdstuk 2 is uiteengezet, kunnen toezichtgegevens worden onderverdeeld in persoonsgegevens, bedrijfs- of fabricagegegevens en overige gegevens. Voor laatstgenoemde categorie bestaan geen belemmeringen voor de uitwisseling: veelal wordt aangenomen dat uitwisseling bijdraagt aan de efficiency en de effectiviteit van het overheidsoptreden, terwijl er geen belangen zijn die pleiten tegen uitwisseling.

Voor de eerste twee categorieën geldt dat het belang bij privacy c.q. bescherming van bedrijfsgegevens wettelijk wordt gewaarborgd. De aard van de uit te wisselen gegevens en het gewicht van de betrokken belangen hangen aldus sterk samen.

Private belangen die hierbij een rol kunnen spelen zijn de vertrouwelijke behandeling van gegevens (geheimhouding), de bescherming van bedrijfs- en fabricagegegevens en de bescherming van persoonsgegevens (ook van derden), de transparantie ten aanzien van de uitwisseling van gegevens, de mogelijke baten doordat administratieve lasten verminderen, en het belang bij zorgvuldige gegevensverzameling en verwerking met het oog op beroepsaansprakelijkheid.

Overheidsbelangen zijn de efficiency en de effectiviteit van het overheidsoptreden, het openhouden van de informatiestroom (geheimhouding en organisatiebelang), de betrouwbaarheid van de overheid bij het beschermen van privacy en andere vertrouwelijke gegevens (privacy, imago en organisatiebelang), het zicht op gegevens bij doorverstrekking in verband met de eigen verantwoordelijkheid en het vertrouwen van de burger (doelbinding), de resultaten die met de verkregen gegevens kunnen worden gerealiseerd (eigen baten), de nadelen voor de eigen informatiepositie bij verstrekking van de gegevens, het belang van de juistheid/goede kwaliteit van de gegevens en het risico van het niet of niet correct ontvangen van de toezichtgegevens.

Een aantal van deze belangen is juridisch te labelen onder de categorieën bescherming van persoonsgegevens, bescherming van bedrijfs- en fabricagegegevens en geheimhoudingsplichten. De niet juridisch erkende belangen zijn terug te voeren op organisatorische, praktische, en ICT-gerelateerde omstandigheden.

Waardering van belangen

Uit de MCA en de expertmeeting blijkt dat juist bij de uitwisseling van toezichtgegevens het belang van de bescherming van persoonsgegevens, de eis van doelbinding en de geheimhouding van grote waarde worden geacht. De stuwende en procesmatige beginselen in de sfeer van baten voor de organisatie en kosten van de gegevensuitwisseling scoren lager. Kosten scoren zelfs uitgesproken laag. Hieruit zou kunnen worden afgeleid dat de zogenoemde verankerende beginselen ook werkelijk goed verankerd zijn in onze handhavingsorganisaties. Een aandachtspunt is dat de procesmatige beginselen zoals transparantie en accountability niet expliciet lijken te leven. Denkbaar is dat deze principes intrinsiek

1912170 01165

worden meegewogen bij de besluitvorming over het al of niet vragen of verstrekken van gegevens, maar de uitkomsten van ons onderzoek geven daarvoor geen basis. Eerder moet worden geconcludeerd dat deze beginselen geen rol spelen.

Als een rangorde van de hoogst gewaardeerde belangen moet worden aangegeven dan valt op dat doelbinding de hoogste score haalt, daarna volgen geheimhouding en privacy, en bij de overheid baten voor de ontvangende of leverende organisatie. De reden voor deze eenduidige keuze zou kunnen worden gezocht in de diepe worteling van de grondrechten in de overheidsorganisatie. Deze beginselen bieden immers tegenwicht aan de voortdurende roep om veiligheid, effectief optreden en efficiency van de overheidsdiensten.

Deze observatie behoeft echter nuancering. Bescherming van de privacy en doelbinding zijn weliswaar verankerende beginselen, maar voor de overheidsinstanties dienen zij het verder gelegen doel van het waarborgen van de betrouwbaarheid van de overheid en daarmee de effectiviteit en de efficiency van het overheidsoptreden. De bescherming van de belangen van de burger wordt daarbij ook als het belang van de eigen organisatie gezien, omdat daarmee de informatiestroom open wordt gehouden. Zoals uit de MCA blijkt, hechten de vertegenwoordigers van burgers en bedrijven zeer aan de bescherming van de positie van hun cliënt. Bescherming van de privacy, doelbinding en geheimhouding zijn hier de sleutelbegrippen ter omschrijving van deze belangen. Overheidsorganisaties zullen dus om hun informatiepositie te behouden en om hun imago als betrouwbare overheid te beschermen noodzakelijkerwijs een goede bescherming van deze belangen moeten bieden. Dit blijkt ook uit de positie van de ontvangers van gegevens. Daar ontbreekt de directe relatie tot het subject en leven de noties geheimhouding, bescherming van de privacy en doelbinding minder sterk bij de verwerking van gegevens. Voor de ontvanger nemen juist de resultaten die met de verkregen gegevens kunnen worden gerealiseerd een prominente plaats in.

Organisatiebelang en transparante afwegingsprocessen

Convenanten zijn bedoeld om een structureel samenwerkingsverband tot stand te brengen, waarbinnen op grond van de Wbp of de Wpg gegevens mogen worden uitgewisseld. Bij het onderzoek naar de inhoud van convenanten viel op dat deze convenanten over het algemeen meer intentieverklaringen zijn en weinig verheldering bieden over de verschillende posities en bevoegdheden. Zij dienen vooral ter legitimatie van de gegevensuitwisseling. Een convenant kan echter geen bevoegdheidsgrondslag bieden: deze moet worden ontleend aan de wet. Een convenant is wel de plaats om vast te leggen hoe deze bevoegdheden in procedurele zin zullen worden uitgeoefend. Zo zou een convenant moeten bepalen voor welke doeleinden de samenwerking dient, welke gegevens of gegevenssets daarvoor zullen worden aangemaakt of aangeleverd, wie bewaakt dat wordt voldaan aan de Wbp (melding aan het CBP), via welke media zal worden uitgewisseld (databank, cloud) en hoe de veiligheid van deze media wordt bewaakt.

In het onderzoek is veel aandacht uitgegaan naar de bescherming van persoonsgegevens. Dat is een kernpunt bij de afweging of tot uitwisseling kan worden overgegaan. In paragraaf 2.3.2

wordt het EU kader voor privacybescherming besproken, dat is uitgewerkt in artikel 7, 8 en 9 Wbp (paragraaf 2.4). Dit kader biedt ruime mogelijkheden om gegevens uit te wisselen, als maar is voldaan aan de randvoorwaarde dat duidelijk vaststaat waarvoor gegevens worden verzameld en verwerkt. Wanneer bestuurlijke toezichthouders en uitvoeringsorganisaties onderling willen uitwisselen, kan dat ook op grond van de Wbp. Het Europese recht, noch de Wbp staan daaraan in de weg. De problematiek van de doelbinding, die in het onderzoek in paragraaf 2.4.3 en 4.6 werd besproken, is niet onoverkomelijk.

Op de strafrechtelijke persoonsgegevens is de Wbp niet van toepassing. De Wpg en de Wjsg geven hier een kader voor de uitwisseling met benoemde partijen c.q. in een samenwerkingsverband. Beide wetten kennen daarnaast de bevoegdheid om in incidentele gevallen gegevens te verstrekken aan niet benoemde partijen, als dat een zwaarwegend belang dient (artikel 19 Wpg en 39f Wjsg). De wet biedt aldus ruimte voor afweging, zij het dat de normconditie 'zwaarwegend belang' tot terughoudendheid noopt. Uit ons onderzoek blijkt dat vragende partijen de politie en het OM soms te terughoudend vinden bij het maken van die afweging (zie paragraaf 3.2.1.4 en 3.2.3.7). Het eigen belang van de organisatie, het krijgen en behouden van de eigen informatiepositie, weegt daarbij volgens de vragende partijen regelmatig zwaarder dan het belang van de goede werking van de overheid in den brede. Bij concrete afwegingen zouden OM en de opsporingsinstanties daarom meer aandacht moeten besteden aan de belangen van andere overheidsorganisaties. Niet zelden wordt bovendien de doelbinding, die ook in de Wpg en de Wjsg beperkingen stelt, als argument naar voren gebracht om verstrekking te weigeren.

Ook het belang bij geheimhouding heeft in het onderzoek nadere aandacht gekregen. Geheimhoudingsplichten strekken zich niet alleen uit over de hiervoor besproken vertrouwelijke gegevens (persoonsgegevens en bedrijfs- en fabricagegegevens) maar over alle soorten toezichtgegevens. Zoals in paragraaf 2.6 is aangegeven heeft de wetgever geheimhoudingsplichten in het leven geroepen ter bevordering van de goede werking van het openbaar bestuur, daaronder begrepen de belangen bij toezicht, controle en opsporing. Geheimhouding, zeker zoals het op de werkvloer wordt geïnterpreteerd, is daarmee vooral ook een organisatiebelang: het openhouden van de inkomende informatiestroom en het niet weggeven van de informatiepositie in een onderzoek. In paragraaf 5.3.1.3 is ingegaan op het strategische belang van de geheimhoudingsplicht. De geheimhoudingsplicht biedt de mogelijkheid om zich in gevallen van twijfel over de wenselijkheid of toelaatbaarheid van de gegevensverstrekking daarachter te verschuilen.

Om de acceptatie van de uitkomst bij vragende instanties te vergroten, verdient het aanbeveling de afwegingsprocessen beter inzichtelijk en toetsbaar te maken. Dit kan voorkomen dat overheidsinstanties uitgaan van tegengestelde belangen en daarmee hun eigen organisatiebelang als belangrijkste ijkpunt zien. Het kan ook voorkomen dat overregulering ontstaat, waarbij de lijst van instanties waaraan bepaalde gegevens moeten worden verstrekt steeds langer wordt. Een andere oplossing kan zijn dat een verplichting tot het verstrekken van gegevens wordt opgenomen (bij twijfel wel inhalen) met de mogelijkheid tot het maken van een uitzondering, waarvoor dan wel een zware motiveringsplicht geldt. Deze laatste optie

1912170 01165

is door respondenten in het onderzoek als wenselijk naar voren gebracht (zie paragraaf 3.2.3.7 en hierna ook paragraaf 5.5.2).

(G)een algemene regeling

De behoefte aan een algemene regeling is gepeild via de oriënterende gesprekken over de drie casus en de expertmeeting. Uit deze gesprekken is geen eenduidig beeld gekomen. Op de werkvloer, waar daadwerkelijk beslissingen over doorverstrekking c.q. verzoeken om gegevens worden genomen, bestaat wel behoefte aan een algemene regeling, met name in de verwachting dat meer duidelijkheid zou ontstaan over de juridische basis bij het uitwisselen van gegevens. Op managementniveau blijkt die behoefte echter niet.

Omdat hieruit geen eenduidige conclusies zijn te trekken, hebben de onderzoekers zich gebogen over de vraag hoe een wettelijke regeling, zo die er moest komen, eruit zou kunnen zien. In de eerste plaats is onderzocht of een regeling voor uitwisseling van toezichtgegevens een plaats zou kunnen krijgen in de Awb. De Awb is om verschillende redenen die in paragraaf 4.2 uiteen zijn gezet een minder geschikte plek. Vervolgens is onderzocht of een kaderwet een geschikt medium zou kunnen zijn. Een kaderwet heeft het voordeel dat daarin de zaken geregeld kunnen worden die momenteel als belemmerend worden gezien voor de gegevensuitwisseling in het algemeen, zoals een duidelijke regeling inzake de bevoegdheid om gegevens uit te wisselen en verduidelijking van de wijze waarop verschillende verstrekkingsregimes met elkaar te verenigen zijn. Tegelijkertijd laat een kaderwet ruimte om onderwerpen die specifiek voor een bepaald beleidsterrein gelden, in bijzondere wetgeving en daarop gebaseerde (lagere) regelingen te regelen. Een kaderwet heeft als nadeel dat het naast elkaar bestaan van een kaderwet en de Wbp weer nieuwe vragen kan oproepen. De Wbp kan echter als uitgangspunt dienen en worden omgebouwd tot een brede wet inzake de gegevensverstrekking. Daarbij moet dan ook de verhouding tot de Wpg en de Wjsg worden geregeld. Denkbaar is dat ook de uitwisseling van strafrechtelijke persoonsgegevens in een brede kaderwet wordt geregeld.

De eis van doelbinding zorgt voor veel vragen. Dit leidt er toe dat veel partijen die over persoonsgegevens beschikken bij twijfel over de toelaatbaarheid van uitwisseling er dan maar van afzien. In Hoofdstuk 4 zijn drie oplossingen voor dit probleem aangedragen. De eerste mogelijkheid zou zijn het criterium van artikel 9 Wbp (voldoende verwantschap) helderder en concreter te formuleren, zodat een maatstaf bestaat die voor de praktijk beter hanteerbaar is. De tweede mogelijkheid is het laten vallen van de eis van de dubbele doelbinding zoals die nu in de wet geformuleerd is. De derde mogelijkheid is in een nadere regeling specifiek voor een bepaald beleidsterrein op te sommen welke gegevens aan welke toezichthouders verstrekt mogen worden.

Al met al concluderen wij dat een algemene wettelijke regeling weliswaar mogelijk is, maar slechts voor een beperkt aantal van de in dit rapport gesignaleerde problemen een oplossing biedt.

1912170 01165

Aanbevelingen

1. Het verdient aanbeveling de bepalingen uit de Wbp over de voor gegevensverwerking vereiste doelbinding - die nu een belemmering vormen bij de gegevensuitwisseling - te verduidelijken in een kaderwet, eventueel met nadere uitwerking in sectorale wetgeving. Deze bepalingen zouden samen met de bepalingen die thans in de Wbp zijn opgenomen, tot een brede kaderwet omgevormd kunnen worden.

2. Met betrekking tot de eis van doelbinding bij doorverstrekking is het aan te bevelen het criterium van voldoende verwantschap te schrappen. De vraag of twee doelen onverenigbaar zijn, is in de meeste gevallen makkelijker te beantwoorden dan de vraag of er tussen twee doelen voldoende verwantschap bestaat. Als het in artikel 9, tweede lid, Wbp genoemde element van verwantschap van doelen voor toezichthouders zou komen te vervallen, zou dat de eisen die de Wbp op dit punt stelt, voor de praktijk beter hanteerbaar maken.

3. Convenanten zouden niet opgesteld moeten worden met als primair doel te regelen welke gegevens uitgewisseld kunnen worden en tussen welke partijen dat kan. Het centrale probleem bij de gegevensuitwisseling is dat de wettelijke normen die momenteel vaak onduidelijkheid veroorzaken, eerst verduidelijkt moeten worden. Als het al mogelijk zou zijn deze normen in convenanten zodanig te concretiseren dat ermee gewerkt kan worden, is nog niet duidelijk of ze in overeenstemming zijn met de wettelijke normen. Wel kunnen convenanten worden afgesloten ter nadere uitvoering van de wettelijke normen uit een kaderwet of sectorale wetgeving, die al wel concreet genoeg zijn. Het verdient aanbeveling om in een convenant louter praktische en procedurele afspraken te maken tussen de gegevensverstrekker en ontvanger.

4. In het geval dat onwil een factor is bij het uitwisselen van gegevens, zou een wettelijke verplichting tot gegevensuitwisseling overwogen kunnen worden. Een algemene verplichting in een kaderwet lijkt echter niet doelmatig en schiet wellicht over het doel heen. Voldoende is dat in een kaderwet wordt opgenomen dat 'bij of krachtens de wet' een verplichting in het leven kan worden geroepen. Deze verplichting zou uitzondering moeten kunnen lijden om zwaarwegende redenen, die worden geëxpliciteerd in de motivering van de weigeringsbeslissing.

5. In die gevallen waarin niet wordt gekozen voor het invoeren van een wettelijke verplichting tot gegevensverstrekking als in Aanbeveling 4 genoemd, verdient het aanbeveling de afwegingsprocessen die leiden tot weigering van gegevensverstrekking beter inzichtelijk en toetsbaar te maken. Dit kan voorkomen dat overheidsinstanties uitgaan van tegengestelde belangen en daarmee hun eigen organisatiebelang als belangrijkste ijkpunt zien. Verder kan het leiden tot een betere acceptatie van een weigering bij de vragende partij.

6. Aanpassing van wettelijke regels kan helpen bij het oplossen van de hier besproken problemen. Los daarvan verdient het aanbeveling om voor degenen die moeten beslissen over gegevensverstrekking praktische handvatten te ontwikkelen op basis waarvan zij verantwoorde en transparante beslissingen kunnen nemen.

1912170 01165

1. Inleiding en probleemstelling

1.1 Aanleiding voor het onderzoek

Een van de speerpunten van het Programma Andere Overheid[1] is het verminderen van de regeldruk. Burgers en bedrijven moeten in die zin zo min mogelijk geconfronteerd worden met regels. Een exponent hiervan is de zogeheten 'één-loket-gedachte', die inhoudt dat een burger niet meerdere keren wordt geconfronteerd met een gegevensuitvraag indien dit niet noodzakelijk is. Als de gegevens zich lenen voor hergebruik, dan dient dit ook zoveel mogelijk te gebeuren. Deze gedachte is in het kader van het Programma Vernieuwing Rijksdienst verder uitgewerkt. [2]

Rijksinspectiediensten werken zoveel mogelijk samen op basis van een geïntegreerd inspectieprogramma. Gegevens die de verschillende inspecties vergaren in het kader van hun toezichtstaak worden zo mogelijk gedeeld met andere inspecties. De technische mogelijkheden daartoe worden steeds geavanceerder, maar het delen en koppelen van gegevens bergt ook gevaren in zich, zoals het gevaar dat het doel waarvoor de bevoegdheid tot gegevensuitvraag is verleend uit het oog wordt verloren (door de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) 'function creep' genoemd).[3]

Binnen de interdepartementale werkgroep Herijking toezichtregelgeving is vervolgens onderzocht wat de mogelijke juridische belemmeringen zijn voor de voortzetting en intensivering van de samenwerking tussen de rijksinspecties en welke mogelijkheden er zijn deze belemmeringen te slechten.[4] De werkgroep Herijking en ook de minister in zijn aanbiedingsbrief wijzen erop dat een algemene regeling van informatie-uitwisseling tussen toezichthouders problematisch kan zijn, omdat steeds in de context van de toepasselijke toezichtswetgeving moet worden bezien welke belangen een rol spelen bij de gegevens

1 Zie de toezichtvisie *Minder last, meer effect. Zes principes van goed toezicht, Kamerstukken II* 2005/06, 27 831, nr. 15 (bijlage) Voortgezet als *Programma Eenduidig toezicht.*

2 Zie *Programma Vernieuwing toezicht, Kamerstukken II* 2007/08, 31 201, nr. 25, en de *Nota Vernieuwing Rijksdienst,* aangeboden bij Kamerbrief van 24 september 2007, *Kamerstukken II* 2007/08, 31 201, nr. 3, onder punt 80-86 (Inspecties). Zie voorts de documentatie op de websites <www.vernieuwingrijksdienst.nl> en <www.inspecteloket.nl>.

3 WRR-rapport, *iOverheid*, Amsterdam: Amsterdam University Press 2011, p. 16, 79, 101, 146, 176, 201, 215, 230.

4 *Rapport van de werkgroep herijking toezichtregelgeving* (rapport van 20 augustus 2008), *Kamerstukken II* 2008/09, 31 700 VI, nr. 70.

1912170 01165

uitwisseling. Per beleidssector of zelfs per wet kunnen die belangen verschillen, en zal steeds een andere afweging moeten worden gemaakt tussen de belangen die baat hebben bij gegevensuitwisseling en de belangen die daarmee worden geschaad, zo is de gedachte. Het toenmalige kabinet heeft het merendeel van de in het rapport van de werkgroep opgenomen conclusies en aanbevelingen overgenomen. Het kabinetsstandpunt hield het volgende in:

> "1. Noch een Algemene wet op het toezicht noch een Algemene wet op gegevensuitwisseling bij toezicht is wenselijk.
> 2. In de bijzondere wetgeving is – wettelijk – maatwerk gewenst indien de samenwerking bij toezicht in een keten of op een domein vaste vorm aanneemt en sprake is van structurele gegevensuitwisseling.
> 3. Aan de Werkgroep Aanwijzingen voor de regelgeving zal worden gesuggereerd een in het rapport opgenomen modelbepaling (in enkele varianten) voor een wettelijke bepaling over de verwerking van gegevens, in de Aanwijzingen voor de regelgeving op te nemen. Overigens zal, in samenhang met het nog te verschijnen advies van de Adviescommissie veiligheid en persoonlijke levenssfeer (commissie Brouwer-Korf), nog worden bezien of deze modelbepaling zou kunnen en moeten worden verbreed tot opsporingsambtenaren en/of -diensten en het openbaar ministerie.
> 4. Vanwege de verwarring die in brede kring, ook buiten die van de toezichthouders, blijkt te bestaan over de verhouding tussen de diverse wetgevingscomplexen die aan de orde zijn bij samenwerking op het terrein van toezicht en de verhouding tussen die complexen, wordt de in het rapport opgenomen achtergrondstudie via de website van het Kenniscentrum Wetgeving en daarnaast in schriftelijke vorm in ruime kring verspreid, eventueel als zelfstandig geschrift.
> 5. Er wordt een leidraad ontwikkeld over de verhouding tussen de Wet bescherming persoonsgegevens en andere wetgeving omtrent de verzameling en verwerking van (persoons-) gegevens."[5]

De aanbeveling om een bepaling in de Algemene wet bestuursrecht (Awb) op te nemen, inhoudende dat als toezichthoudende organen structureel samenwerken zij nadere afspraken moeten maken over een aantal specifiek genoemde onderwerpen, werd door het kabinet niet overgenomen. Het kabinet was van oordeel dat samenwerkingsafspraken tussen toezichthoudende instanties, die binnen de wettelijke grenzen vallen, ook zonder wettelijke grondslag mogelijk zijn en in de praktijk ook reeds gemaakt worden; daarom zou een dergelijke bepaling slechts symbolische waarde hebben.

Bij behandeling van de evaluatie van de Wet bescherming persoonsgegevens (Wbp), is echter, mede naar aanleiding van een aantal rapporten[6], op aandringen van de Tweede Kamer toegezegd de mogelijkheid van een dergelijke algemene regeling toch te bezien.[7] De achtergrond daarvan was dat de bestaande wetgeving structurele afspraken over gegevensuitwisseling mogelijk maakt onder bepaalde voorwaarden, maar dat geen wettelijke regeling met bijbehorende waarborgen voor de gegevensbescherming bestaat voor de gevallen waarin de wet niet voorziet in structurele samenwerking en er wel behoefte is aan gegevensuitwisseling. In de Awb zou een vangnetbepaling kunnen worden opgenomen, die verplicht tot

5 *Kamerstukken II* 2008/09, 31 700 VI, nr. 70 (bijlage bij brief van de minister van 29 oktober 2008).
6 *Kamerstukken II* 2007/08, 31 051, nr. 2 (verslag van een algemeen overleg over het onderzoeksrapport *Eerste fase evaluatie Wet bescherming persoonsgegevens. Literatuuronderzoek en knelpuntenanalyse*). Zie ook: *Kamerstukken II* 2008/09, 31 051, bijlage bij nr. 4 (*Wat niet weet, wat niet deert. Evaluatieonderzoek werking Wbp*); *Kamerstukken II* 2009/10, 31 051, nr. 5 (kabinetsstandpunt ten aanzien van het rapport *Gewoon doen, beschermen van veiligheid en persoonlijke levenssfeer* van de Adviescommissie Veiligheid en persoonlijke levenssfeer (commissie Brouwer-Korf) en de evaluatierapporten van de Wet bescherming persoonsgegevens).
7 *Kamerstukken II* 2009/10, 31 051, nr. 7, p. 19 (Evaluatie Wet bescherming persoonsgegevens).

1912170 01165

het bekend maken van structurele samenwerking op het punt van gegevensuitwisseling tussen toezichthouders, in die gevallen waarin geen specifiek wettelijke regeling bestaat. Deze regeling zou moeten waarborgen dat burgers en bedrijven weten dat een samenwerkingsverband bestaat met het oog op de vereisten van transparantie, kenbaarheid van de gegevensuitwisseling en doelbinding.[8]

1.1.1 Probleemstelling en onderzoeksvragen

Tegen de achtergrond van het voorgaande heeft de opdrachtgever de volgende probleemstelling voorgelegd:

I. Met welke belangen moet rekening worden gehouden bij de verstrekking van toezichtgegevens tussen toezichthouders onderling en tussen toezichthouders enerzijds en het Openbaar Ministerie, de politie en de buitengewoon opsporingsambtenaren anderzijds?

II. Is het, in het licht van de vorige vraag, gewenst en juridisch mogelijk om voor het verstrekken van toezichtgegevens tussen toezichthouders onderling en tussen toezichthouders enerzijds en het Openbaar Ministerie, de politie en de buitengewoon opsporingsambtenaren anderzijds, een algemene regeling in de Algemene wet bestuursrecht en/of eventuele andere wetten op te nemen?

Het belangenperspectief staat bij de eerste onderzoeksvraag voorop. De uitkomsten van het onderzoek zouden, naar de onderzoekers bij aanvang van het onderzoek verwachtten, een spectrum van belangen opleveren, waardoor zowel voor- als nadelen van een verstrekking van toezichtgegevens tussen inspectiediensten onderling en tussen inspectie- en opsporingsdiensten in beeld zouden kunnen komen. Op basis daarvan zou vervolgens kunnen worden gekeken naar de noodzaak voor en de juridische haalbaarheid van een algemene regeling in de Algemene wet bestuursrecht en/of eventuele andere wetten (de tweede onderzoeksvraag).

1.2 Uitwerking en aanpak van de onderzoeksvragen

De opdrachtgever heeft een aantal onderzoeksvragen voorgelegd, die zijn ingegeven door de ratio achter bestaande juridische beperkingen bij gegevensuitwisseling tussen toezichthouders onderling c.q. toezichthouders en OM/opsporing.

De juridische beperkingen komen voort uit het streven belangen die door de gegevensverstrekking worden geraakt te beschermen. Deze belangen kunnen zijn verankerd in fundamentele rechten, zoals het recht op privacy, het recht op een eerlijk proces en de onschuldpresumptie. Ze kunnen in aansluiting daarop voortkomen uit vrees voor oneigenlijk gebruik (*function creep*) of misbruik, zoals de eis van doelgebondenheid van gegevensverzameling en -verwerking. De bevoegdheden tot verstrekking komen op hun beurt voort uit het streven de belangen die met de gegevensverzameling en -verstrekking zijn gediend te beschermen, zoals de veiligheid, het belang bij naleving en het opsporingsbelang. Bij deze mix van belangen hebben zich inmiddels ook gevoegd het belang gevrijwaard te zijn van onevenredige administratieve lasten, het belang van efficiënte inzet van mensen en middelen bij het toezicht, en het belang bij effectief toezicht. Tot nu toe worden de belangen per wet, instantie of bevoegdheid benoemd en afgewogen. De vraag is echter of een algemeen afwegingskader kan worden ontworpen dat zicht geeft

8 *Kamerstukken II* 2008/09, 31 700 VI, nr. 118, p. 9.

1912170 01165

op de aard en zwaarte van de betrokken belangen en daarmee op de aard van eventueel noodzakelijke beperkingen op het verstrekkingenregime.

Hierna wordt per vraag die door de opdrachtgever is opgeworpen aangegeven hoe deze is onderzocht.

1.2.1 Vraag I: Betrokken belangen

Bij de *eerste onderzoeksvraag*, met welke belangen moet rekening worden gehouden bij het verstrekken van toezichtgegevens tussen toezichthouders onderling en tussen toezichthouders enerzijds en Openbaar Ministerie (OM), de politie en de buitengewoon opsporingsambtenaren anderzijds, is het volgende onderzocht:

1. *Welke belangen spelen een rol bij de afweging of al dan niet sprake kan zijn van het uitwisselen van gegevens?*

   Daarbij gaat het om een uiteenlopend palet van belangen. In de eerste plaats zijn dat belangen van de inspectie- en opsporingsdiensten, de toezichthoudende functionarissen en opsporingsambtenaren en de onder toezicht gestelde burgers en bedrijven (soms tevens verdachte). Daarnaast spelen algemene belangen een rol en de meer democratisch georiënteerde belangen van de verantwoordelijke bewindslieden.

   Ten aanzien van deze vraag was een nadere inventarisatie nodig van de belangen die hier in het geding kunnen zijn. De werkgroep Herijking heeft in 2008 een overzicht gemaakt van samenwerkende partijen en van regelgeving waarin gegevensuitwisseling is geregeld.[9] We hebben een quickscan uitgevoerd op een enkele van de door de werkgroep Herijking genoemde vormen van samenwerking en zijn nagegaan welke belangen een rol (kunnen) spelen bij de wettelijk geregelde gegevensuitwisseling. Op basis van deze quickscan is een lijst van mogelijke belangen samengesteld die, door middel van open vragen aan betrokkenen, is aangevuld ten behoeve van de te houden kwalitatieve enquête.

2. *Is er mogelijk sprake van nog andere belanghebbenden dan de onder vraag 1 genoemden bij het verstrekken van toezichtgegevens?*

   Naast betrokken uitvoeringsorganisaties en de onder toezicht staande partijen spelen intermediaire partijen een rol van toenemend belang bij het verzamelen en doorgeven van data ten behoeve van de administratieve processen van de overheid, zoals bijvoorbeeld advocaten, fiscale intermediairs, administratiekantoren, en hulpverleners. Welke specifieke partijen op dit moment een dergelijke rol vervullen en derhalve als mogelijk belanghebbende door de verstrekking van toezichtgegevens geraakt kunnen worden, is met behulp van de quickscan nader in beeld gebracht. Het betreft hierbij veelal instanties die vertrouwelijke informatie overdragen onder restrictie van het gebruik. Op basis daarvan zijn vervolgens enkele gesprekken gevoerd om te komen tot een meer onderbouwde inventarisatie.

3. *Onder welke condities kunnen de vastgestelde belangen met elkaar in botsing komen?*

   Bij de beantwoording van deze vraag is de aanpak tweeledig. Enerzijds is onderzocht hoe degenen wier belangen bij de gegevensuitwisseling zijn betrokken zelf aankijken tegen de

9 Zie *supra*, noot 4.

1912170 01165

verschillende betrokken belangen. Welke punten vinden zij belangrijk en welke spelen in hun ogen juist geen of slechts een kleine rol? Dit is onderzocht in de reeds genoemde gesprekken met betrokkenen en door middel van een vragenlijst die is uitgezet binnen de gekozen domeinen en deels daarbuiten. Anderzijds zijn de verschillende (soorten) van belangen beoordeeld, waarbij in eerste instantie is uitgegaan van de juridische context waarbinnen de verstrekking van toezichtgegevens plaatsvindt. Deze context bepaalt met name de belemmeringen die de verstrekking van toezichtgegevens in de weg staan, zoals doelbinding, geheimhoudingsplicht, restrictieve bevoegdheidstoedeling en moeilijk verenigbare sanctiestelsels. Deze belemmeringen zijn niet willekeurig gekozen maar zijn ieder voor zich de resultante van een, in het verleden gemaakte, belangenafweging of van inrichtingskeuzes met een minder fundamenteel karakter. Voor een deel heeft het nagaan van de betrokken belangen bij het verstrekken van toezichtgegevens dan ook betekend dat de oorspronkelijke belangenafweging in het kader van de gegroeide mogelijkheden door digitalisering opnieuw tegen het licht werd gehouden. Hadden we de belangen hetzelfde gewogen als we over de huidige technologische mogelijkheden hadden beschikt? En zo nee, wat zouden we anders doen?

Deze fase vraagt om een rangschikking, completering en vervolgens analyse van het verkregen materiaal ten behoeve van de volgende fase, gevolgd door een beoordeling van de bevindingen aan de hand van het juridisch kader.

4. *Hoe worden de (potentieel botsende) belangen juridisch gelabeld?*

Bij deze vraag is onderzocht of en, zo ja, hoe de verschillende belangen die uit de inventarisatie naar voren zijn gekomen juridisch gekwalificeerd zijn. Het kan daarbij bijvoorbeeld gaan, in de terminologie van de WRR, om een – mogelijke – botsing tussen 'stuwende' en 'verankerende' beginselen, zoals zorg voor veiligheid en het recht op privacy.[10] 'Verankerend' zijn ook plichten die worden opgelegd om bepaalde belangen te beschermen (zoals geheimhoudingsplichten). Ook kan strijd ontstaan met 'procesmatige beginselen', dat wil zeggen beginselen die aandacht moeten verzekeren voor aspecten zoals zorgvuldige vaststelling van gegevens en transparantie. De toepasselijke wettelijke regelingen worden onderzocht, evenals nationale en internationale jurisprudentie (Hof van Justitie EU en EHRM). De belangen die niet wettelijk zijn verankerd zijn nader geanalyseerd aan de hand van de – deels wettelijk vastgelegde – beginselen van behoorlijk bestuur, van behoorlijke rechtspleging en van goed toezicht.[11]

5. *Zijn er belangen bij die juridisch (nog) niet erkend zijn?*

Uit de analyse bij vraag 4 moet blijken in hoeverre bepaalde belangen juridisch wel of niet zijn gekwalificeerd. Bepaalde, meer operationele belangen, zoals het belang bij een efficiënte inzet van mensen en middelen, het belang bij een goede ontsluiting van een databank, of het belang bij wederkerigheid, zullen in de regel geen juridische verankering hebben, hoewel deze in praktisch opzicht wel bepalend kunnen zijn. Het belang bij beperking van administratieve lasten is ook een voorbeeld van een meer praktisch belang dat recent naar voren is gekomen. Het heeft geen

10 Het WRR-rapport *iOverheid* geeft vele voorbeelden, onder andere het gevaar van 'détournement d'information' bij ingebruikname van het digitale Midoffice door lagere overheden (p. 126-127) en onwettig gebruik van gegevens die geregistreerd worden door On Board Diagnostics in auto's (p. 133). Het rapport constateert onder meer dat in het nastreven van 'stuwende' beginselen als veiligheid en efficiëntie 'aanmerkelijk minder' gebouwd wordt aan de verankerende en procesmatige beginselen: 'er is enige schroom om die beginselen zich te laten bewijzen' (p. 136).

11 Het gaat dan bijvoorbeeld om zorgvuldige voorbereiding, materiële zorgvuldigheid, het evenredigheidsbeginsel, het vertrouwensbeginsel, de beginselen van een *fair trial*, de onschuldpresumptie en het beginsel van *nemo tenetur*.

1912170 01165

juridische verankering,[12] maar wordt gereflecteerd in het evenredigheidsbeginsel en het materiële zorgvuldigheidsbeginsel, ook wel het 'beginsel van de minste pijn' genoemd. Daarin valt een begin van juridische erkenning waar te nemen. Daarbij gaat het overigens niet alleen om belangen, maar in toenemende mate ook om – reële dan wel gepercipieerde – met het dienen van deze belangen verbonden risico's.

6. *Welke van de vastgestelde juridisch erkende belangen (rechten) hebben voorrang op andere vastgestelde rechten en waarom?*

Een juridische erkenning van belangen kan de vorm aannemen van de erkenning van rechten. Het grootste gewicht komt daarbij juridisch gezien toe aan fundamentele rechten, zoals erkend in de Grondwet, het EVRM, en het EU-recht. Daarnaast kan die erkenning in de vorm van plichten of procedurebepalingen worden gegoten. Ook daaruit kan immers blijken dat een bepaald gewicht toekomt aan belangen of dat bepaalde belangen voorrang hebben.

Bij de beantwoording van deze vraag is betrokken hoe de onderlinge verstrekking van gegevens tussen toezichthouders en OM/opsporing juridisch op elkaar is afgestemd. Voor OM en opsporingsambtenaren gelden wettelijke beperkingen ten aanzien van het uitwisselen van gegevens (Wet politiegegevens (Wpg), Wet justitiële en strafvorderlijke gegevens (Wjsg)), terwijl de Wbp met name voor toezichthouders in de bestuursrechtelijke keten van belang is. Bijzondere wetten kennen bepalingen over uitwisseling tussen toezichthouders.[13] Verschillende toezichthouders maken gebruik van samenwerkingsprotocollen, waarin afspraken over uitwisseling zijn neergelegd, en waarin de juridische verantwoordelijkheid van de partners is benoemd.[14] Bij het beantwoorden van deze vraag worden deze afspraken zo mogelijk volledig in kaart gebracht.

Uit het onderzoek op dit onderdeel zal blijken in hoeverre er sprake is van een asymmetrische verhouding tussen de informatieposities van bestuursorganen en toezichthouders enerzijds en politie en OM anderzijds. Laatstgenoemde instanties kunnen bijvoorbeeld bij de uitoefening van de algemene politietaak en bij de opsporing zeer veel informatie vergaren, mede op grond van wettelijke dwangmiddelen. Zij kunnen deze informatie echter niet zo maar doorgeven aan het bestuur. Anderzijds zullen bestuurlijke toezichthouders niet zonder meer genegen zijn toezichtsinformatie aan politie of OM door te geven wanneer niet zeker is of deze in een strafvorderlijk traject zal mogen worden gebruikt.

Ook zal uit het onderzoek blijken welk gewicht aan de verschillende rechtsposities van de betrokkenen wordt toegekend, welke posities dan vervolgens prevaleren en welke de redenen daarvoor zijn.

12 Dit praktische belang wordt geadresseerd in de toezichtvisie uit 2005 van het toenmalige kabinet (*Minder last, meer effect. Zes principes van goed toezicht*, bijlage bij *Kamerstukken II* 2005/06, 27 831, nr. 15). Aan de in 2001 geformuleerde principes van goed toezicht - 'onafhankelijk', 'transparant', en 'professioneel' - worden drie principes toegevoegd die met name zien op beperking van administratieve lasten: 'selectief', 'slagvaardig' en 'samenwerkend'. Zie over 'selectief' toezicht (prioritering, beleidsvrijheid binnen een algemene beginselplicht tot handhaven): A.A. van Rossum, 'Civielrechtelijke aansprakelijkheid voor overheidstoezicht', in: A.A. van Rossum, L.F.M. Verhey & N. Verheij, *Toezicht* (Preadviezen. Handelingen Nederlandse Juristenvereniging 2005-1, Jaargang 135), Deventer: Kluwer 2005, p. 37 e.v.

13 Vgl. de lijst opgesteld door de werkgroep Herijking (zie *supra*, noot 4) maar ook bijvoorbeeld de artikelen 18.19 en 18.20 Telecommunicatiewet.

14 Vgl. Kwink groep, TNO, Berenschot, *Evaluatie OPTA*, 31 augustus 2009, en *Informatie-uitwisselingsprotocol OPTA – KLPD/DNR*, 30 augustus 2007. Andere samenwerkingsprotocollen tussen toezichthouders zijn onder meer: Opta en NMa (2004), Inspectie Volksgezondheid (IVG) en OM (2009), de Nederlandse Zorgautoriteit (NZa) en DNB (2007).
Een specifiek voorbeeld van een toezichtnetwerk betreft de Consumentenautoriteit die als een spin in het web, en steeds in het kader van een bepaalde taak, protocollen heeft getekend met een groot aantal toezichthouders. Zie: <www.consumentenautoriteit.nl/over-ons/missie-en-kerntaken/samenwerking>.

1912170 01165

1.2.2 Vraag II: Algemene regeling

Bij de *tweede onderzoeksvraag*, te weten of het, in het licht van de vorige vraag, juridisch mogelijk is om voor het verstrekken van toezichtgegevens tussen toezichthouders onderling en tussen toezichthouders enerzijds en het Openbaar Ministerie, de politie en de buitengewoon opsporingsambtenaren anderzijds een algemene regeling in de Algemene wet bestuursrecht en/of eventuele andere wetten, op te nemen, is het volgende onderzocht:

7. *Is een algemene voorziening in de Awb of in andere wetten gewenst en juridisch mogelijk?*

   De werkgroep Herijking heeft reeds een modelbepaling ontworpen met betrekking tot gegevensuitwisseling en de bescherming van persoonsgegevens die in bijzondere wetgeving kan worden opgenomen. Een algemene regeling achtte de werkgroep niet goed doenlijk vanwege de uiteenlopende bevoegdheden, taken en gegevens in toezichtsregelgeving. De hiervoor opgenomen onderzoeksvraag gaat verder dan de vraag die de werkgroep zich heeft gesteld en zoekt naar een algemeen afwegingskader, met behulp waarvan de betrokken belangen kunnen worden benoemd en gewogen. Op grond van zo'n kader zal moeten kunnen worden bepaald wanneer gegevensuitwisseling ontoelaatbaar is, wanneer wel toelaatbaar maar onder voorwaarden, en wanneer volledig toelaatbaar.

   Voor de beantwoording van deze vraag zal worden onderzocht in hoeverre de resultaten van het onderzoek naar de belangen (en hun juridische status en gewicht) steun geven aan het treffen van een algemene regeling voor de uitwisseling van gegevens, hetzij bij wege van een voorziening in de Algemene wet bestuursrecht, hetzij in eventuele andere wetten.[15] Daarbij zal worden betrokken de vraag welke ruimte de internationale en Europeesrechtelijke kaders inzake gegevensbescherming overlaten voor een dergelijke algemene voorziening. Deze gaan immers uit van een stelsel waarbij doorbreking van de doelgebondenheid van informatieverzameling slechts toegestaan is in individuele gevallen, waarbij steeds een belangenafweging in concreto nodig is.[16]

   Overigens moet worden bedacht dat in de Awb wel een en ander geregeld kan worden voor toezichthouders (nalevingstoezicht) maar, gelet op artikel 1:6 Awb, niet voor OM/opsporingsambtenaren bij de uitvoering van hun opsporingstaken.

8. *Mogelijke neveneffecten van een algemene voorziening*

   De vraag naar mogelijke neveneffecten van een algemene voorziening is meegenomen in de vragenlijst ten behoeve van de inventarisatie van belangen en tijdens een expertmeeting. De verschillende belanghebbenden zullen worden bevraagd op hun inschatting van de risico's van

15 In enkele wetten is reeds een voorziening getroffen, bijvoorbeeld: Telecommunicatiewet, Arbowet, Arbeidstijdenwet, Wet structuur uitvoeringsorganisatie werk en inkomen (Wet SUWI).

16 Zie: *Rapport werkgroep herijking, supra* noot 4; Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (*PbEG* 1995, L 281/31); Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) (*PbEG* 2002, L 201/37); G.J. Zwenne, A.W. Duthler, M. Groothuis, H. Kielman, W. Koelewijn & L. Mommers, *Eerste fase evaluatie Wet bescherming persoonsgegevens. Literatuuronderzoek en knelpuntenanalyse*, WODC, Ministerie van Justitie, December 2007.

1912170 01165

een algemene bevoegdheid tot het uitwisselen van gegevens, zoals het risico van misbruik en oneigenlijk gebruik (*function creep*).

1.3 Methoden van onderzoek

Gelet op de voor het onderzoek beschikbare tijd en middelen heeft het onderzoeksteam een quickscan uitgevoerd op basis van de inventarisatie die de werkgroep Herijking heeft gemaakt van samenwerkende partijen en van regelgeving waarin gegevensuitwisseling is geregeld. Deze quickscan is in eerste instantie gericht op een aantal domeinen, te weten de vastgoedsector, de bestuurlijke aanpak van criminaliteit, het financiële toezicht, en de gegevensverstrekking in samenwerkingsverbanden met de Belastingdienst. Deze quickscan is besproken met enkele medewerkers binnen de betrokken organisaties[17] en met de begeleidingscommissie. In overleg met de begeleidingscommissie is besloten het onderzoek nader te richten op drie domeinen: de gegevensverstrekking in samenwerkingsverbanden met de Belastingdienst, de aanpak van criminaliteit in de vuurwerkketen en de aanpak van het toezicht op het taxibedrijf in Amsterdam. Daartoe is een aangepaste quickscan opgesteld.

Op basis van deze quickscan is een inventarisatie van belangen gemaakt door het voeren van oriënterende gesprekken met betrokkenen in de gekozen domeinen. Op basis daarvan is vervolgens een lijst met probleempunten en belangen samengesteld. Om inzicht te verkrijgen in de perceptie van de relevantie van deze factoren is aan degenen die als betrokkenen bij de betreffende gegevensuitwisseling zijn geïdentificeerd met behulp van een internetenquête (vragenlijsten) gevraagd welk gewicht zij aan de verschillende factoren hechten (ranking). Dit betrof niet alleen degenen die werkzaam zijn in het toezicht of de opsporing, maar nadrukkelijk ook de ondertoezichtgestelden en derden die als professional een belang hebben (zoals advocaten en accountants).

Met de resultaten van de enquête zijn de onderzoeksresultaten door middel van een Multicriteria-analyse in kaart gebracht. Multicriteria-analyse (MCA) is een wetenschappelijke evaluatiemethode met behulp waarvan een rationele keuze kan worden gemaakt tussen verschillende alternatieven op basis van meer dan één onderscheidingscriterium. De onderhavige MCA resulteerde een rangorde van het relatieve belang van relevante aspecten (factoren) met betrekking tot (her)gebruik van gegevens door toezichthouders en opsporingsinstanties. De weging van het relatieve belang dat aan deze factoren werd gehecht is richtinggevend geweest bij het zoeken naar de balans tussen de verschillende deelbelangen en daarmee medebepalend voor het draagvlak dat binnen de praktijkdeelnemers aan dit onderzoek bestaat voor mogelijke data(her)gebruik regulerende bepalingen. De resultaten zijn uitgesplitst naar de rol die de betreffende subjecten spelen in de gegevensverstrekking, administratieve verwerking, toezicht dan wel opsporing. Met de MCA is inzicht verkregen in de mate waarin homogeniteit bestaat qua opvattingen over de regulering van het uitwisselen van toezichtgegevens.

Om de gevonden belangen en de optie van een algemene regeling ook in een debat in interactie tussen de verschillende spelers te toetsen is een expertmeeting met betrokkenen uit het veld georganiseerd. De experts waren afkomstig uit verschillende domeinen, waaronder ook andere domeinen dan het drietal dat meer in het bijzonder is onderzocht. Op deze manier is getoetst in hoeverre aan de voorlopige onderzoeksresultaten een meer algemene betekenis kan worden toegekend. De aldus gevalideerde MCA heeft tevens als basis gediend voor de beantwoording van onderzoeksvraag II.

17 Gemeente Amsterdam, Openbaar Ministerie en de Belastingdienst.

1912170 01165

Onderzoeksvraag II is nader onderzocht met behulp van de klassieke juridische methoden van bestudering van literatuur, de wetsgeschiedenis van wetgeving waarin gegevensuitwisseling is geregeld (of juist daarvan af is gezien), jurisprudentie, Europese regelgeving en jurisprudentie van het Hof van Justitie en het EHRM.

1.4 Beperkingen

Het onderzoek is een studie naar problemen die zich voordoen of kunnen voordoen bij de uitwisseling van gegevens tussen overheidsinstanties op drie domeinen. Gegevensverzameling en -verstrekking zijn verbonden met bepaalde waarborgen die dienen ter bescherming van bepaalde belangen. De soorten gegevens die kunnen worden verzameld en verstrekt verschillen per domein en ook de ratio voor de waarborgen en beperkingen met betrekking tot de verzameling en verstrekking verschillen (deels) per domein. De toelaatbaarheid van de uitwisseling van toezichtgegevens is daarom naar de huidige stand van zaken maatwerk. Het bestek van dit onderzoek laat niet toe dat alle uitwisselingsrelaties in alle domeinen konden worden onderzocht. Om die reden moesten keuzes gemaakt worden en is in overleg met de begeleidingscommissie eerst een quickscan gedaan op vier domeinen, namelijk de vastgoedsector, de bestuurlijke aanpak van criminaliteit, het financiële toezicht, en de gegevensverstrekking in samenwerkingsverbanden met de Belastingdienst. Zoals hiervoor reeds opgemerkt, is vervolgens besloten het onderzoek toe te spitsen op drie (nader afgebakende) domeinen.

In enkele gesprekken met betrokkenen in het veld bleek, dat op bepaalde domeinen actuele ontwikkelingen gaande waren waar de dilemma's voor de betrokken partijen bij gegevensuitwisseling duidelijk naar voren kwamen. Dit waren de domeinen vuurwerk en taxibranche. Bij het nalevingstoezicht op de vuurwerkregelgeving zijn veel partijen betrokken, omdat het gaat om het toezicht op de invoer, het vervoer, de opslag, de verkoop en het gebruik. Om informatie tussen een aantal betrokken toezichthouders uit te wisselen is een pilot gestart, die nuttige informatie oplevert voor ons onderzoek. Bij een oriënterend gesprek over de gegevensuitwisseling bij de bestuurlijke aanpak van criminaliteit bleek dat vanwege de nieuwe regelgeving ten aanzien van de taxibranche nieuwe toezichtsarrangementen worden ontwikkeld, waarbij private partijen (de TTO's) een rol zullen gaan spelen bij de gegevensverstrekking en -uitwisseling. Bij het toezicht op de taxibranche zijn bovendien veel partijen op rijks- en gemeentelijk niveau betrokken, terwijl ook politie en justitie een belangrijke rol spelen. Deze case sloot daarom goed aan bij onze onderzoeksvragen. Omdat de Belastingdienst in vrijwel alle situaties waarbij gegevens-uitwisseling aan de orde is een rol speelt, is besloten de gegevensverstrekking in samenwerkingsverbanden met de Belastingdienst als casus op te nemen. Daarbij kan worden opgemerkt dat de Belastingdienst primair is belast met het heffen en innen van rijksbelastingen (Uitvoeringsregeling Belastingdienst) en daarnaast in specifieke gevallen is aangewezen als toezichthouder (zie bijvoorbeeld het Besluit aanwijzing toezichthouders Belastingdienst). Gegevens van de Belastingdienst zijn dus ook niet perse toezicht-gegevens, maar kunnen dit wel zijn.

De offerteaanvraag gaat uit van uitwisseling tussen rijksinspecties onderling en tussen rijksinspecties en opsporingsinstanties en OM. In twee van de in het onderzoek gekozen domeinen speelt ook de gemeentelijke overheid een rol. De inspecties zijn als zodanig niet expliciet onderzocht. Zij maakten deel uit van twee groepen convenantspartijen: de VROM-inspectie in het vuurwerkdossier en de Inspectie Verkeer en Waterstaat in de casus taxivervoer.

1912170 01165

1.5 Onderzoeksteam en begeleidingscommissie

Het onderzoeksteam bestond uit onderzoekers van de Faculteit der Rechtsgeleerdheid van de Universiteit van Amsterdam:

Prof. dr. A.J.C. de Moor-van Vugt
Prof. dr. T.M. van Engers
Dr. F.T. Groenewegen
Mr. W.F. van Haaften
Dr. A.P. Klap
Dr. A.J. Nieuwenhuis
Mw. L. M. Schouten en Mr. drs. M.W. Wessel (onderzoeksassistentie)

Een CV van de onderzoekers is opgenomen in de bijlage (paragraaf 7.1).

De begeleidingscommissie bestond uit:

Prof. mr. dr. H.E. Bröring (RUG), voorzitter
Drs. R. van den Hoven van Genderen (VU)
Mr. dr. J.P. de Jong (Ministerie van Veiligheid en Justitie)
Mw mr. F.A. de Lange (WODC)
Mw mr. T. Rijnten (Ministerie van Financiën)

De onderzoeksleiding is drie maal bijeen gekomen met de begeleidingscommissie om de te maken keuzes en de voortgang te bespreken. Het rapport werd afgerond op 1 juni 2012.

1.6 Opbouw van het rapport

In dit rapport wordt eerst het juridisch kader voor gegevensuitwisseling besproken. Daarbij wordt aandacht besteed aan de Wbp, de Wpg en de Wjsg. Verder komen de relevante bepalingen uit de EU regelgeving en het EVRM aan bod. Hoofdstuk 3 doet verslag van het onderzoek dat is gedaan om de bij gegevensuitwisseling betrokken belangen te inventariseren en om de rangorde die bij de uitwisseling in de praktijk door betrokken partijen wordt aangebracht te achterhalen. In hoofdstuk 4 wordt ingegaan op de vraag welke opties openstaan voor een algemene wettelijke regeling en in hoeverre deze tegemoet komen aan de in het onderzoek gesignaleerde behoeftes. In hoofdstuk 5 worden conclusies getrokken en enkele aanbevelingen gedaan.

1912170 01165

2. Het juridisch kader bij gegevensuitwisseling

2.1 Inleiding

Het juridisch kader bij gegevensuitwisseling wordt gedomineerd door de Wet bescherming persoonsgegevens. Juist omdat bescherming van de privacy en daarmee de persoonsgegevens als een belangrijke waarde wordt gezien, kunnen toezichthouders en opsporingsdiensten niet onbeperkt gegevens verwerken en uitwisselen. Hierna wordt daarom met name ingegaan op de Wbp, de Wpg en de Wjsg.

2.2 Toezichtgegevens

De Algemene wet bestuursrecht regelt de bevoegdheden waarmee toezichthouders gegevens kunnen verzamelen. Belangrijke bevoegdheden zijn die tot het vorderen van inlichtingen (artikel 5:16) en tot het vorderen van inzage in zakelijke gegevens en bescheiden en het maken van kopieën daarvan (artikel 5:17). Andere bevoegdheden zijn die tot het vorderen van inzage in het identiteitsbewijs (artikel 5:16a), het onderzoeken, opnemen en nemen van monsters van zaken, (artikel 5:18), en het onderzoeken van vervoermiddelen en hun lading (artikel 5:19). In bijzondere wetgeving kunnen de toezichtsbevoegdheden worden beperkt.

Los van het toezicht bevat artikel 4:2, tweede lid, Awb de bepaling dat een aanvrager van een beschikking gegevens en bescheiden moet verschaffen die voor de beslissing op de aanvraag nodig zijn. De aanvrager mag weigeren deze te overleggen, voor zover het belang daarvan voor de beslissing van het bestuursorgaan niet opweegt tegen het belang van de eerbiediging van de persoonlijke levenssfeer, waaronder de bescherming van medische en psychologische onderzoeksresultaten, of tegen het belang van de bescherming van bedrijfs- en fabricagegegevens (artikel 4:3). In bijzondere wetgeving wordt de verplichting tot verschaffing van bescheiden en gegevens aangevuld met en versterkt door informatie en meldingsplichten.

Toezichtgegevens zijn gegevens die worden gebruikt ten behoeve van het toezicht op de naleving van regelgeving. Zij kunnen expliciet zijn verzameld voor toezichtsdoeleinden, maar zij kunnen ook voortkomen uit gegevensverzameling ten behoeve van de primaire besluitvorming, zoals de heffing en inning van belastingen. Toezichtgegevens kunnen worden onderverdeeld in persoonsgegevens, bedrijfs- en fabricagegegevens en overige gegevens. De laatste categorie levert weinig problemen op als het gaat om het verwerken en uitwisselen ervan, omdat daarvoor geen wettelijke belemmeringen gelden. Het belangrijkste obstakel geldt voor gegevens die (mede) moeten worden aangemerkt als persoonsgegevens.

2.3 Persoonsgegevens

Deze paragraaf gaat in op het begrip 'persoonsgegeven'. Daartoe wordt eerst kort de grondrechtelijke achtergrond van de bescherming van persoonsgegevens geschetst. Daarna komt de betekenis van de term 'persoonsgegeven' in de Wbp aan bod. Onder meer wordt ingegaan op de vraag wanneer gegevens zodanig herleidbaar zijn tot een identificeerbare persoon dat zij als persoonsgegevens kunnen worden aangemerkt, op de categorie bijzondere persoonsgegevens en op de verhouding tussen persoonsgegevens en bedrijfsgegevens. De uiteenzetting besteedt ook aandacht aan de positie van persoonsgegevens onder de Wpg en de Wjsg.

2.3.1 Grondrechtelijke achtergrond

Artikel 8 EVRM legt het recht op respect voor het privéleven vast. Dat recht omvat onder meer het recht op respect voor het gezinsleven, de woning en de correspondentie. Meer in het algemeen ziet het op het afschermen van het eigen leven tegen ongewenste inmenging. Die inmenging kan zowel bestaan uit een vrijheidsbeperking ten aanzien van de vormgeving van het eigen leven, het aangaan van relaties met derden (relationele privacy) als uit het verzamelen, vastleggen en openbaren van informatie betreffende de persoon (informationele privacy). Artikel 10, eerste lid, Grondwet, dat het recht op bescherming van de persoonlijke levenssfeer vastlegt, kent een vergelijkbare reikwijdte. Hoewel het in artikel 8 EVRM vastgelegde recht ziet op het privéleven van de natuurlijke persoon, sluit dat niet uit dat het recht ook van toepassing is op het professionele leven.[18] In het verlengde daarvan kan het recht onder omstandigheden ook bescherming bieden tegen maatregelen als het doorzoeken van bedrijfsgebouwen.[19]

Een inmenging op het in artikel 8 EVRM vastgelegde recht dient op grond van het tweede lid bij wet te zijn voorzien en noodzakelijk in een democratische samenleving te zijn ten behoeve van de in het tweede lid genoemde doeleinden. De voorwaarde van noodzakelijkheid impliceert dat een inmenging moet voldoen aan de eisen van proportionaliteit en subsidiariteit. Bij de informationele privacy spelen onder meer de aard van de gegevens,[20] de reikwijdte van de maatregel,[21] de duur van de vastlegging,[22] de mogelijkheid voor de betrokkene om controle uit te oefenen,[23] en het bestaan van maatregelen tegen misbruik[24] een rol. Het verzamelen van gegevens door de overheid kan een inbreuk vormen op artikel 8 EVRM, evenals het bewaren ervan.[25]

18 EHRM 16 december 1992, nr. 13710/88 (*Niemietz/Duitsland*).
19 EHRM 16 april 2002, nr. 37971/97 (*Société Colas Est e.a./Frankrijk*).
20 EHRM 25 februari 1997, nr. 22009/93 (*Z./Finland*); EHRM 4 december 2008, nr. 30562/04 en 30566/04 (*Marper/Verenigd Koninkrijk*).
21 EHRM 4 december 2008 (*Marper/Verenigd Koninkrijk*).
22 EHRM 4 mei 2000, nr. 28341/95 (*Rotaru/Roemenië*).
23 EHRM 7 juli 1989, nr. 10454/83 (*Gaskin/Veremgd Koninkrijk*); EHRM 28 april 2009, nr. 32881/04 (*K.H. e.a./Slowakije*).
24 EHRM 17 juli 2008, nr. 20511/03 (*I/Finland*).
25 EHRM 6 september 1978, nr. 5029/71 (*Klass e.a./Duitsland*); EHRM 2 augustus 1984, nr. 8691/79 (*Malone/Verenigd Koninkrijk*). Zie met betrekking tot bewaren van gegevens: EHRM 16 februari 2000, nr. 27798/95 (*Amann/Zwitserland*).

1912170 01165

In het verlengde van het recht op respect voor het privéleven is een meer zelfstandig recht op bescherming van persoonsgegevens opgekomen. Daarbij speelden de toenemende technische mogelijkheden ten aanzien van de verwerking van persoonsgegevens een rol van betekenis. Er bestond met name vrees dat het koppelen van gegevens uit verschillende bestanden de privacy en de vrijheid van het individu ernstig onder druk zou kunnen zetten.

Het recht op bescherming van persoonsgegevens is niet expliciet vastgelegd in artikel 10 EVRM, maar wel in het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens, [26] dat tevens in het kader van de Raad van Europa tot stand is gekomen en waar het EHRM in zijn uitspraken naar verwijst.[27] De Nederlandse Grondwet ziet op persoonsgegevens in artikel 10, tweede en derde lid; beide bepalingen behelzen een opdracht aan de wetgever om de bescherming nader uit te werken.

Andere grondrechtencatalogi bevatten een zelfstandig en individueel recht op bescherming van de persoonsgegevens. Een goed voorbeeld vormt het Handvest van de Grondrechten van de EU (artikel 8), dat een ieder een recht geeft op bescherming van de persoonsgegevens (eerste lid) en waarin voorts onder meer is bepaald dat de verwerking plaats dient te vinden op een eerlijke wijze en voor bepaalde doeleinden (tweede lid). Persoonsgegevens zijn ingevolge de jurisprudentie van het Hof van Justitie gegevens die betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon.[28] De beperkingen die mogen worden gesteld aan het recht op bescherming van de persoonsgegevens, komen overeen met die welke worden toegelaten in het kader van artikel 8 EVRM, zo oordeelde het Hof van Justitie.[29] Overigens is de bescherming van persoonsgegevens ook in het VWEU zelf (artikel 16, eerste lid) vastgelegd.

2.3.2 Het EU-kader voor gegevensbescherming

De binnen de EU vastgesteld Privacyrichtlijn[30] geeft de nationale overheden opdracht tot bescherming van persoonsgegevens. Het is deze Privacyrichtlijn die ten grondslag heeft gelegen aan de Wbp (eerder: Wet persoonsregistraties), waarmee de wetgever tegelijkertijd voldoet aan zijn grondwettelijke opdracht. De toepassing van de wet beperkt zich dan ook niet tot de reikwijdte van het EU-recht. In veel gevallen zou het bovendien ook moeilijk zijn hier een grens te trekken.

De Privacyrichtlijn bevat bepalingen met betrekking tot de kwaliteit van persoonsgegevens. Lidstaten dienen te bepalen dat persoonsgegevens eerlijk en rechtmatig moeten worden verwerkt. Het vereiste van doelbinding komt voort uit artikel 6 van de richtlijn, dat bepaalt dat gegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden moeten worden verkregen. Ze mogen vervolgens niet worden verwerkt op een wijze die onverenigbaar is met die doeleinden. Daarnaast zijn de eisen van subsidiariteit en proportionaliteit vastgelegd. Verwerking van persoonsgegevens moet ter zake dienend en niet bovenmatig zijn, uitgaande van de doeleinden waarvoor zij worden verzameld of waarvoor zij vervolgens worden verwerkt (subsidiariteit). Voorts moet de verwerking noodzakelijk zijn om de doelstellingen van de verwerking te bereiken en mag deze niet verder gaan dan noodzakelijk (proportionaliteit). Verder bevat de richtlijn een bepaling met betrekking tot de juistheid en nauwkeurigheid van de gegevensverwerking. In artikel 7 is vervolgens aangegeven wanneer gegevens-

26 Straatsburg 28 januari 1981, *Trb.* 1988, 7.
27 Zie bijvoorbeeld: EHRM 4 mei 2000 (*Rotaru/Roemenië*).
28 HvJ EU 9 november 2010, nr. C-92/09 en C-93/09 (*Schecke en Eifert*).
29 HvJ EU 9 november 2010, nr. C-92/09 en C-93/09 (*Schecke en Eifert*)
30 Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (*PbEU* 1995, L 281/31).

1912170 01165

verwerking toelaatbaar is. Het Hof heeft geoordeeld dat dit artikel een uitputtende lijst bevat van gevallen waarin een verwerking van persoonsgegevens als rechtmatig kan worden aangemerkt. Lidstaten zijn niet bevoegd om aan artikel 7 nieuwe beginselen betreffende de toelaatbaarheid van de verwerking van persoonsgegevens toe te voegen, of bijkomende vereisten vast te stellen die de reikwijdte van een van de zes in dat artikel vervatte beginselen zouden wijzigen. Artikel 7 heeft voorts rechtstreekse werking.[31] Artikel 7 van de Privacyrichtlijn is uitgewerkt in artikel 8 Wbp (zie daar).

Van belang is op te merken dat het EU-recht in ontwikkeling is. De Commissie heeft twee voorstellen voor regelingen het licht doen zien, beide te baseren op artikel 16, eerste lid, VWEU. Het betreft in de eerste plaats een ontwerpverordening betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.[32] In de tweede plaats gaat het om een ontwerprichtlijn betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming van strafbare feiten, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens.[33] Deze regelingen moeten volgens de Commissie zorgen voor een Europees gegevensbeschermingskader voor de 21e eeuw en voor waarborging van de privacy in het online tijdperk. Voorts kunnen ook andere grondrechten zoals het recht op non-discriminatie in het geding zijn. De Commissie heeft verschillende opties overwogen en meent dat de gekozen oplossing een stevig en coherent kader biedt, dat voor alle beleidsterreinen geldt.[34] Daarmee komt de Commissie onder meer tegemoet aan de kritiek dat de huidige Privacyrichtlijn tot een te grote mate van fragmentering leidt.

Met de inwerkingtreding van de Privacyverordening zal de huidige Privacyrichtlijn vervallen. Een belangrijk verschil tussen beide regelingen is uiteraard dat de verordening geen implementatie behoeft, maar direct toepasbaar is in alle lidstaten. Daar staat tegenover dat de uitgangspunten en de inhoud van de Privacyrichtlijn en de voorgestelde verordening in belangrijke mate overeenkomen. Dat geldt ook voor het uitgangspunt dat er grondrechtelijke belangen in het geding zijn, maar dat het recht op bescherming van persoonsgegevens geen absolute gelding heeft.

Voor dit onderzoek is in het bijzonder artikel 44 van de voorgestelde verordening van belang. In dat artikel worden de uitzonderingsbepalingen voor gegevensdoorgifte uiteengezet en verklaard, gebaseerd op de bestaande bepalingen van artikel 26 van de Privacyrichtlijn. Dit artikel heeft in het bijzonder betrekking op doorgiften van gegevens die vereist en noodzakelijk zijn om gewichtige redenen van algemeen belang, zoals in geval van internationale doorgifte van gegevens tussen mededingingsautoriteiten, belasting- of douanediensten, of diensten met bevoegdheid op het gebied van de sociale zekerheid of visserijbeheer. Verder kan een gegevensdoorgifte onder beperkte voorwaarden gerechtvaardigd zijn in verband met de gerechtvaardigde belangen van de voor de verwerking verantwoordelijke of de verwerker, maar slechts nadat de omstandigheden van deze doorgifte zijn geëvalueerd en gedocumenteerd.

De voorgestelde richtlijn inzake politiegegevens en justitiële gegevens heeft een veel ruimer toepassingsgebied dan het bestaande Kaderbesluit 2008/977/JBZ, dat alleen van toepassing is op grensoverschrijdende gegevensverwerking en niet op verwerkingsactiviteiten van de politiële en justitiële autoriteiten op zuiver nationaal niveau. Dat beperkte toepassingsgebied leidde tot problemen bij de

31 HvJ EU 24 november 2011, gevoegde zaken C-468/10 en C-469/10 (*ASNEF en FECEMD*).
32 COM (2012) 11 final, Brussel 25 januari 2012.
33 COM (2012) 10 final, Brussel 25 januari 2012.
34 Mededeling van de Commissie aan het EP, de Raad, EESC en het Comité van de regio's, COM (2012) 9 final, Brussel 25 januari 2012.

1912170 01165

samenwerking. De voorgestelde richtlijn moet voor enige harmonisatie zorgen. Het toepassingsgebied is daarom niet beperkt tot grensoverschrijdende gegevensverwerking, maar bestrijkt alle verwerkingsactiviteiten die "bevoegde autoriteiten" (zoals gedefinieerd in artikel 3, punt 14) voor de toepassing van de richtlijn uitvoeren. Voor zover de voorgestelde regelingen relevante verschillen met het geldend recht bevatten, zal er in dit hoofdstuk te bestemder plaatse aandacht aan worden besteed.

2.3.3 Overlap en onderscheid

Het recht op bescherming van persoonsgegevens heeft zich mede ontwikkeld uit het recht op respect voor het privéleven. Het ligt dan ook voor de hand dat er een overlap bestaat wat de reikwijdte betreft.[35] Indien bijvoorbeeld bestanden met medische gegevens van bij naam genoemde individuen openbaar worden, zijn beide rechten in het geding. Een tweede overeenkomst is dat de beginselen van proportionaliteit en subsidiariteit op beide terreinen van groot belang zijn.

Deze overlap betekent niet dat sprake is van een samenval van beide rechten. Uit het bovenstaande komt reeds naar voren dat onder meer de vormgeving van het eigen leven onder artikel 8 EVRM valt, ook als er geen sprake is van de verwerking van persoonsgegevens. Omgekeerd hoeft niet iedere verwerking van een persoonsgegeven een inmenging in het recht op respect voor het privéleven te vormen. Dat hoeft niet het geval te zijn indien het bijvoorbeeld alleen om NAW-gegevens gaat. Ook wordt het bestaan van een dossier met louter gegevens omtrent het professionele handelen, waarvan de betrokkene op de hoogte was, door het EHRM niet als een inmenging op het recht op respect voor het privéleven aangemerkt.[36] Deze vastleggingen vallen uiteraard wel binnen de reikwijdte van het persoonsgegevensrecht.

2.3.4 De term persoonsgegeven in de Wbp

De Wbp ziet op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens en op de niet geautomatiseerde verwerking van gegevens die in een bestand zijn opgenomen of die bestemd zijn daarin opgenomen te worden (artikel 2). 'Verwerking' en 'persoonsgegeven' zijn daarmee twee van de centrale begrippen in de wet. Verwerking - van persoonsgegevens - is conform de richtlijn gedefinieerd als elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, al dan niet uitgevoerd met behulp van geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, bewaren, uitwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens (artikel 1, sub b, Wbp).

Artikel 1, sub a, Wbp omschrijft conform de Europese eisen een persoonsgegeven als elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Het gegeven dient dus informatie over een persoon te bevatten. Bij feitelijke of waarderende gegevens over eigenschappen, opvattingen of gedragingen zal dat uit de aard van de gegevens voortvloeien.[37] Een beperking tot rechtens relevante informatie is in elk geval onjuist. Daar staat tegenover dat niet elk technisch of toevallig verband tussen een gegeven en een persoon voldoende is om dat gegeven een persoonsgegeven te doen zijn.

In het algemeen kan worden gesteld dat als gegevens mede bepalend zijn voor de wijze waarop de betrokken persoon in het maatschappelijk verkeer wordt beoordeeld of behandeld, die gegevens als

35 H.R. Kranenborg & L.F.M. Verhey, *Wet bescherming persoonsgegevens in Europees perspectief*, Deventer: Kluwer 2011, p. 17 e.v.
36 EHRM 4 januari 2007, nr. 39658/05 (*Smith/Verenigd Koninkrijk*).
37 *Kamerstukken II* 1997/98, 25 892, nr. 3 (MvT), p. 46.

1912170 01165

persoonsgegevens moeten worden aangemerkt.[38] Daar dient aan toegevoegd te worden dat daarbij niet slechts bepalend is het doel waarvoor de gegevens worden verwerkt, maar ook waarvoor zij *kunnen* worden verwerkt. Zo zijn coderingen van CIE-mutaties in het register zware criminaliteit ook persoonsgegevens. [39]

De gegevens dienen niet alleen over een persoon te gaan, de persoon dient ook identificeerbaar te zijn. Daarbij kan een onderscheid worden gemaakt tussen direct en indirect identificerende gegevens. Direct identificerende gegevens zijn gegevens die betrekking hebben op een persoon waarvan de identiteit zonder veel omwegen eenduidig vast te stellen is (bijv. NAW-gegevens). Ook bijvoorbeeld een op naam gestelde aangifte is een persoonsgegeven.[40]

Indirect identificerende gegevens zijn gegevens die niet zonder nadere stappen in verband kunnen worden gebracht met een bepaalde persoon: kentekens,[41] GSM-nummers,[42] en eventueel ook IP-adressen, tenzij het met zekerheid om niet-identificeerbare gebruikers gaat.[43] Ook andere unieke gegevens kunnen als identificerend worden aangemerkt, zoals het burgerservicenummer (BSN) of unieke biometrische gegevens zoals stem, vingerafdruk of DNA-profiel. Het is mogelijk dat een persoonsgegeven na het schrappen van de bijbehorende NAW-gegevens nog steeds een persoonsgegeven blijft. Dat is het geval indien uit de verdere informatie afgeleid kan worden om wie het gaat. Dat geldt bijvoorbeeld ook voor de verklaring van een verhoorde of gehoorde persoon, voor zover uit de verklaring afgeleid kan worden wie de persoon is die deze heeft afgelegd.[44]

2.3.5 Persoonsgegevens – bedrijfsgegevens

In het kader van het toezicht en in het kader van de beoordeling van aanvragen (vergunningen, ontheffingen, subsidies) zijn bedrijven vaak verplicht gegevens over hun bedrijf aan te leveren. Het kan dan bijvoorbeeld gaan om gegevens met betrekking tot het product dat het bedrijf maakt, het productieproces, emissies van stoffen of de financiële gegevens. In het kader van de Wet openbaarheid van bestuur (Wob) heeft de Afdeling bestuursrechtspraak geoordeeld dat slechts sprake is van bedrijfs- en fabricagegegevens 'indien en voor zover uit die gegevens wetenswaardigheden kunnen worden gelezen of afgeleid met betrekking tot de technische bedrijfsvoering of het productieproces dan wel met betrekking tot de afzet van de producten of de kring van afnemers en leveranciers.' [45] Onder omstandigheden kunnen ook financiële gegevens worden beschouwd als bedrijfsgegevens, maar niet die financiële gegevens die rechtspersonen ingevolge Boek 2 van het Burgerlijk Wetboek moeten opmaken en openbaar maken, ook indien daaruit wetenschap zou kunnen worden verkregen over de hiervoor bedoelde onderwerpen, aldus de rechtbank Dordrecht.[46]

Gegevens die betrekking hebben op overledenen of rechtspersonen zijn op zichzelf geen persoonsgegevens. Hebben deze gegevens echter tegelijkertijd betrekking op nog levende, natuurlijke

38 Ibid. In dit verband is de vraag gerezen in hoeverre de minuut die wordt opgemaakt ter voorbereiding van de afwijzing van een aanvraag om een verblijfsvergunning persoonsgegevens bevat die recht geven op inzage. Zie: HR 29 juni 2007, *LJN* AZ4663, Afdeling bestuursrechtspraak 2 februari 2011, *LJN* BP2831 en de prejudiciële verwijzing van Rb. Middelburg, 15 maart 2012, *LJN* BV8942.
39 HR 9 juli 2010, *LJN* BM2311, *NJ* 2010, 416.
40 *Kamerstukken II* 1997/98, 25 892, nr. 3 (MvT), p. 47.
41 Zie met betrekking tot Automatic Numberplate Recognition (ANPR): Hof Arnhem 16 juni 2010, *LJN* BM8111; zo ook eerder al de uitspraak: Rb. Zwolle 2 juli 2009 *LJN* BJ2119, *NJFS* 2009, 225.
42 Rb. Dordrecht 31 augustus 2004, *NJ* 2004, 678. Tevens besproken in: T.E. van Dijk (red.), *Uitsprakenbundel Wet bescherming persoonsgegevens*, Den Haag: Sdu Uitgevers 2009.
43 G.J. Zwenne, 'Over persoonsgegevens en IP-adressen, en de toekomst van privacywetgeving', in: L. Mommers (red.), *Het binnenste buiten. Liber amicorum ter gelegenheid van het emeritaat van prof. dr. Aernout H.J. Schmidt, hoogleraar Recht en Informatica te Leiden*, Leiden: eLaw 2010, p. 321-342.
44 Vgl. Afdeling bestuursrechtspraak 25 januari 2007, *LJN* AZ6853. Zie ook: Afdeling bestuursrechtspraak 31 januari 2007, *LJN* AZ7410.
45 Afdeling bestuursrechtspraak 17 juli 2002, *LJN* AE5445.
46 Rb. Dordrecht 11 januari 2002, *LJN* AD9759.

1912170 01165

personen en kunnen zij mede bepalend zijn voor de wijze waarop deze in het maatschappelijk verkeer worden beoordeeld of behandeld, dan zijn het wel weer persoonsgegevens. Zo is het gegeven dat de bij name genoemde X deel uitmaakt van de directie van bedrijf Y onmiskenbaar een persoonsgegeven. Gegevens die betrekking hebben op een product of een productieproces kunnen soms tegelijkertijd over een bepaalde persoon informatie verschaffen, bijvoorbeeld wanneer daarmee de arbeidsproductiviteit van een werknemer gemakkelijk in kaart kan worden gebracht.[47] In dat geval zijn het tegelijkertijd persoonsgegevens.

Bij informatie over eenmanszaken en maatschappen zal er relatief vaak sprake zijn van bedrijfsgegevens die terzelfder tijd als persoonsgegevens kunnen worden aangemerkt. De jurisprudentie laat wel enige twijfel over het antwoord op de vraag op welk moment dat het geval is. Zo kwam de rechtbank Zwolle in 2004 tot de conclusie dat gegevens omtrent de MKZ besmetting van dieren van een veehouder geen persoonsgegevens in de zin van de Wbp zijn, mede omdat het 'bedrijfsgegevens' in de zin van de Wob waren.[48] Dat laatste argument is in zijn algemeenheid onjuist; een dergelijke scheidslijn bestaat niet. Het is dan ook veelbetekenend dat de rechtbank Zwolle twee jaar later uitdrukkelijk vaststelde dat de hoedanigheid van bedrijfsgegeven in de zin van de Wob niet uitsluit dat er sprake is van een persoonsgegevens in de zin van de Wbp. Gegevens ten aanzien van het bedrijf en de bedrijfsvoering kunnen in veel gevallen direct betrokken zijn op de natuurlijke persoon. De rechtbank stelt onder verwijzing naar de MvT van de Wbp vast dat ook dergelijke gegevens mede bepalend kunnen zijn voor de manier waarop de betrokkene wordt beoordeeld of behandeld.[49]

2.3.6 Bijzondere persoonsgegevens

In navolging van de Privacyrichtlijn definieert de Wbp bepaalde gegevens als bijzondere persoonsgegevens, waarvoor een apart regime geldt. Het zijn gegevens die intiem van karakter zijn of waarvan het gebruik het risico van discriminatie in zich draagt: persoonsgegevens betreffende iemands godsdienst of levensovertuiging, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakbond en strafrechtelijke gegevens (artikel 16). Onder strafrechtelijke persoonsgegevens vallen zowel gegevens ten aanzien van veroordelingen als ten aanzien van verdenkingen.

De verwerking van bijzondere gegevens is verboden, tenzij de wet een uitzondering schept. De Wbp kent specifieke uitzonderingen voor gegevens betreffende de godsdienst, bijvoorbeeld voor kerkgenootschappen (artikel 17, eerste lid, sub a) en voor medische gegevens, bijvoorbeeld voor instellingen voor gezondheidszorg (artikel 21 eerste lid, sub a). Daarbij komt dat medische gegevens op grond van artikel 21, tweede lid Wbp in beginsel alleen mogen worden verwerkt door personen met een geheimhoudingsplicht. Het verbod om strafrechtelijke gegevens te verwerken is niet van toepassing indien de verantwoordelijke de gegevens heeft verkregen krachtens de Wpg of de Wjsg (artikel 22 eerste lid Wbp) (zie ook hieronder).

Naast deze specifieke uitzonderingen kent de wet een aantal meer algemene uitzonderingen op het verbod om bijzondere gegevens te verwerken. Op grond van artikel 23 Wbp is de verwerking onder meer toegestaan wanneer deze noodzakelijk is met het oog op een zwaarwegend algemeen belang, er passende waarborgen zijn ter bescherming van de persoonlijke levenssfeer en de verwerking bij wet bepaald is of

47 *Kamerstukken II* 1997/98, 25 892, nr. 3 (MvT), p. 46.
48 Rb. Zwolle 22 maart 2004, *LJN* AO6018.
49 Rb. Zwolle 21 februari 2006, *LJN* AV3139.

1912170 01165

het CBP toestemming heeft gegeven. Het beleid van het CBP is om geen toestemming te geven voor structureel gebruik, behalve indien er wetgeving op komst is.[50]

De ontwerp Privacyverordening van de EU voegt aan de expliciet in de Privacyrichtlijn – en dus ook in de Wbp – genoemde bijzondere gegevens nog, overeenkomstig de jurisprudentie van het Europees Hof voor de rechten van de mens, genetische gegevens toe.[51] De ontwerpverordening legt het hogere beschermingsniveau van deze gegevens expliciet vast.

2.3.7 Persoonsnummers

Artikel 24 Wbp ziet op zogeheten persoonsnummers. Het bepaalt dat een nummer dat ter identificatie van een persoon bij wet is voorgeschreven, bij de verwerking van persoonsgegevens slechts wordt gebruikt ter uitvoering van de betreffende wet dan wel voor doeleinden bij de wet bepaald. Op grond van het tweede lid is het mogelijk andere dan in het eerste lid bedoelde gevallen aan te wijzen waarin een zodanig persoonsnummer kan worden gebruikt. Hoewel de wet een persoonsnummer niet onder de bijzondere gegevens schaart, is het gebruik dus wel specifiek genormeerd.

Uit de specifieke regeling ten aanzien van bijzondere gegevens en van persoonsnummers mag overigens niet geconcludeerd worden dat de verwerking van andere - gewone - gegevens steeds als een geringe inbreuk op het recht op bescherming van de persoonsgegevens kan worden beschouwd. De mate van inbreuk hangt mede van de context af, dus onder meer van de situatie waarin de gegevens worden verkregen en het doel waarvoor zij worden verwerkt.

2.3.8 Verhouding Wbp, Wpg en Wjsg

In artikel 2, tweede lid, Wbp heeft de wetgever bepaald dat de Wbp niet van toepassing is op de verwerking van persoonsgegevens door of ten behoeve van de inlichtingen- en veiligheidsdiensten (sub b), ten behoeve van de politietaak (sub c) of ten behoeve van de uitvoering van de Wjsg (sub e). Regelgeving omtrent de verwerking van persoonsgegevens in het kader van deze taken is opgenomen in respectievelijk de Wet op de Inlichtingen- en Veiligheidsdiensten, de Wpg en de Wjsg.

Op grond van artikel 16 Wbp is verwerking van strafrechtelijke persoonsgegevens in beginsel verboden. Ingevolge artikel 22, eerste lid, is dit verbod niet van toepassing indien de verwerking geschiedt door organen die krachtens de wet zijn belast met de toepassing van het strafrecht, of wanneer de verwerking geschiedt door verantwoordelijken die de gegevens hebben verkregen krachtens de Wpg of de Wjsg. De Wpg is een lex specialis die ziet op de verwerking van politiegegevens. In de wet zijn politiegegevens gedefinieerd als: 'elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon dat in het kader van de uitoefening van de politietaak wordt verwerkt' (artikel 1, sub a). Ook in de Wpg is de noodzakelijkheid van de verwerking een belangrijk criterium. Voorts kent ook de Wpg de categorie bijzondere gegevens (artikel 5); anders dan in de Wpg vallen daaronder niet de strafrechtelijke gegevens. Verwerkt de politie persoonsgegevens buiten de uitoefening van de politietaak, bijvoorbeeld als toezichthouder in de zin van de Awb, dan is niet de Wpg maar de Wbp van toepassing. Dat is in beginsel ook het geval indien door de politie verstrekte politiegegevens door andere organen verwerkt worden.

50 Zie de brief van het CBP aan onder meer de Minister voor Vreemdelingenzaken en Integratie van 11 december 2006, betreffende het Besluit inzake het ontheffingsverzoek Verwijsindex Antillianen en de gemeentelijke casusoverleggen Antillianen. Toegankelijk via de website van het CBP, <www.cbpweb.nl>.

51 EHRM 4 december 2008, nr. 30562/04 en 30566/04 (S. en Marper/Verenigd Koninkrijk).

1912170 01165

Blijkens de memorie van toelichting van de Wpg, achtte de wetgever het wenselijk om, met het oog op de bijzondere aspecten van de politietaak, een aparte regeling te treffen voor de verwerking van politiegegevens.[52] Dit in navolging van de daarvoor geldende Wet politieregisters. Onder deze bijzondere aspecten wordt onder meer het feit geschaard dat de verwerking van persoonsgegevens door de politie, bijvoorbeeld in het kader van opsporing, consequenties kan hebben die de betrokken persoon niet in het eigen belang acht.[53] Met de invoering van de Wbp beoogde de wetgever om 'met eerbiediging van de beginselen die de bescherming van de persoonlijke levenssfeer ten doel hebben, meer ruimte te bieden dan de huidige wetgeving voor het verwerken van gegevens ten behoeve van een optimale uitvoering van de politietaak'.[54]

De Wjsg ziet op de verwerking van gegevens in het kader van de strafrechtelijke taken van het OM. De wet omschrijft strafvorderlijke gegevens als gegevens over een natuurlijk persoon of rechtspersoon die zijn verkregen in het kader van een strafvorderlijk onderzoek en die het OM in een strafdossier of langs geautomatiseerde weg verwerkt (artikel 1, sub b). Justitiële gegevens zijn gedefinieerd als bij algemene maatregel van bestuur te omschrijven gegevens omtrent natuurlijke personen en rechtspersonen inzake de toepassing van het strafrecht of de strafvordering (artikel 1, sub a). Uit het Besluit justitiële gegevens blijkt dat het om bepaalde beslissingen van de rechter en het OM gaat ten aanzien van natuurlijke en rechtspersonen (artikelen 7 jo. 2, 3, 4, 6 en 9 Besluit justitiële gegevens). Ten overvloede zij gezegd dat, wanneer deze gegevens door anderen verwerkt worden, de Wbp van toepassing is, waarbij uiteraard de bepaling die ziet op de verwerking van strafrechtelijke gegevens van betekenis is (artikel 22 Wbp).

De ontwerp-richtlijn van de EU die ziet op de verwerking van politiegegevens en justitiële gegevens legt twee nieuwe relevante normen vast. In de eerste plaats zal er zo veel mogelijk onderscheid gemaakt moeten worden betreffende verschillende soorten betrokkenen (artikel 5). Daarbij onderscheidt de richtlijn verschillende categorieën: personen ten aanzien van wie gegronde vermoedens bestaan dat zij een strafbaar feit hebben gepleegd of zullen gaan plegen; b) personen die veroordeeld zijn voor een strafbaar feit; c) slachtoffers van een strafbaar feit, of personen ten aanzien van wie op basis van bepaalde feiten wordt vermoed dat zij slachtoffer zouden kunnen worden van een strafbaar feit; d) personen die als derden bij een strafbaar feit betrokken zijn, zoals personen die als getuige kunnen worden opgeroepen (…); en e) personen die onder geen van de bovengenoemde categorieën vallen. In de tweede plaats moet er – zoals hiervoor al werd opgemerkt - voor zover mogelijk worden onderscheiden naar de graad van juistheid en betrouwbaarheid van de gegevens en moeten de lidstaten erop toezien dat persoonsgegevens die op feiten zijn gebaseerd, voor zover mogelijk, worden onderscheiden van persoonsgegevens die op een persoonlijke oordeel zijn gebaseerd.[55]

2.4 Doelbinding

De Wbp legt in de artikelen 6 tot en met 11 een aantal materiële normen vast die in het algemeen van toepassing zijn op de verwerking van persoonsgegevens. Artikel 6 bepaalt dat de verwerking behoorlijk en zorgvuldig dient te zijn. Artikel 7 eist dat gegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld. Artikel 8 geeft een opsomming van gerechtvaardigde verwerkingen. Artikel 9 bepaalt dat persoonsgegevens niet verder verwerkt worden op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen. Artikel 10 stelt de eis dat gegevens niet langer bewaard worden dan noodzakelijk is voor de verwerkelijking van de doeleinden waarvoor zij

52 *Kamerstukken II* 2005/06, 30 327, nr. 3 (MvT), p. 2-3.
53 Ibid., p. 3.
54 Ibid., p. 1.
55 Vgl. HR 9 juli 2010, *LJN* BM2311, *NJ* 2010, 416, waarin sprake is van coderingen van CIE-mutaties in verband met de betrouwbaarheid van de gegevens.

1912170 01165

worden verzameld en artikel 11 Wbp bepaalt dat persoonsgegevens slechts verwerkt worden voor zover zij gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt ter zake dienend en niet bovenmatig zijn.

Het is niet moeilijk in een aantal van deze bepalingen de eisen van proportionaliteit en subsidiariteit te herkennen. Daarnaast speelt het beginsel van doelbinding een belangrijke rol. Dat zal verder in dit rapport dan ook uitdrukkelijk aan de orde worden gesteld. Alvorens dat te doen, krijgt eerst artikel 8 Wbp enige aandacht. Dat is van belang zowel omdat daarin specifieke normen zijn vastgelegd voor de verwerking van persoonsgegevens door bestuursorganen als omdat het vereiste van doelbinding van artikel 9 Wbp een eis is die voor alle in artikel 8 Wbp genoemde gerechtvaardigde verwerkingen kan gelden en bij uitstek ook relevant is bij de koppeling van gegevens.

2.4.1 Gerechtvaardigde verwerkingen

Artikel 8 Wbp bepaalt wanneer de verwerking van persoonsgegevens gerechtvaardigd is. Dat is het geval wanneer de betrokkene uitdrukkelijk toestemming heeft verleend (sub a) of wanneer de verwerking noodzakelijk is ter uitvoering van een overeenkomst (sub b), ter nakoming van een wettelijke verplichting (sub c), ter vrijwaring van een vitaal belang van de betrokkene (sub d), voor de goede vervulling van een publiekrechtelijke taak door een bestuursorgaan (sub e) of ter behartiging van het gerechtvaardigd belang van de verantwoordelijke, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert (sub f).[56]

In een aantal gevallen zal de gegevensverwerking door bestuursorganen kunnen worden gebaseerd op artikel 8 sub c Wbp. Dat is echter lang niet altijd het geval. Een gegevensverwerking ter vervulling van een publiekrechtelijke taak zal immers veelal geschieden zonder dat daaraan een wettelijke verplichting ten grondslag ligt. In dat geval zal de gegevensverwerking onder artikel 8 sub e Wbp moeten vallen. Die bepaling ziet, zo blijkt uit de tekst, op een tweetal verschillende situaties. Allereerst kan een verwerking noodzakelijk zijn met het oog op een publiekrechtelijke taak die het bestuursorgaan zelf verricht. Daarnaast laat de bepaling uitdrukkelijk ruimte voor verwerking van gegevens ten behoeve van de publiekrechtelijke taak die door een ander bestuursorgaan wordt verricht, voor zover dat met het oog op die taak noodzakelijk is.

2.4.2 Het uitgangspunt van doelbinding

Een van de specifieke uitgangspunten van de Wbp is het beginsel van doelbinding. Dit beginsel komt met name tot uitdrukking in de artikelen 7, 9, 10 en 11 Wbp. Nu artikel 10 en 11 Wbp grotendeels voor zichzelf spreken, is de behandeling hier beperkt tot artikel 7 en 9 Wbp. De doelbinding dient reeds bij het verzamelen van gegevens aanwezig te zijn. Artikel 7 schrijft voor dat persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld. Er moet dus een duidelijke doelomschrijving zijn alvorens gegevens verzameld mogen worden. Deze dient welbepaald te zijn, dus niet zo vaag of ruim dat zij tijdens het verzamelproces geen kader kan bieden waaraan getoetst kan worden of de gegevens nodig zijn voor dat doel of niet.[57] Het is evenmin toegestaan om het doel pas te formuleren in de loop van het verzamelproces. Is er sprake van een meldingsplicht op grond van artikel 27 Wbp, dan dient het doel van de verwerking bij de melding uitdrukkelijk te zijn omschreven. In de

56 Het gebruik van de f-grond om in afwachting van wetgeving belastinggegevens door te geven aan de verhuurders ten behoeve van huurverhogingen om ' scheefwonen' te voorkomen, werd door de rechter onrechtmatig geacht. Zie: Rb. 's-Gravenhage 13 april 2012, *LJN* BW2236, *NTFR* 2012, 937, m. nt. Thomas.

57 *Kamerstukken II* 1997/98, 25 892, nr. 3 (MvT), p. 78-79.

1912170 01165

gevallen vrijgesteld van een melding op grond van artikel 29 Wbp, geldt het doel dat bij algemene maatregel van bestuur is omschreven op grond van artikel 29, tweede lid, Wbp.

Het beginsel van doelbinding is ook terug te vinden in artikel 9 Wbp, dat aan de reeks van gerechtvaardigde verwerkingen in artikel 8 Wbp een meer algemeen vereiste toevoegt. Mede daarom heeft deze bepaling een niet te onderschatten belang.[58]

Artikel 9, eerste lid, Wbp bepaalt dat persoonsgegevens niet verder worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen. Daarmee maakt de bepaling duidelijk dat deze verdere verwerking niet ongeoorloofd is, maar stelt zij daar tegelijkertijd een grens aan. Deze eis van verenigbaar gebruik geldt zowel binnen als buiten de organisatie van de verantwoordelijke.[59] Het tweede lid kent een niet-limitatieve opsomming van factoren die mede bepalend zijn voor het antwoord op de vraag of er sprake is van verenigbaar gebruik. Elk van de genoemde factoren dient – mogelijk in samenhang met andere factoren die in het concrete geval als relevant moeten worden beschouwd – in onderling verband te worden beoordeeld en gewogen ter beantwoording van de vraag of sprake is van verenigbaar gebruik.[60]

2.4.3 Voldoende verwantschap: dubbele doelbinding

Een belangrijke factor is de verwantschap tussen het doel waarvoor de verantwoordelijke de gegevens overweegt te gebruiken enerzijds en het doel waarvoor de gegevens zijn verkregen anderzijds (artikel 9, tweede lid, sub a, Wbp). Deze verwantschapsfactor kan bij uitstek als uitdrukking van het beginsel van doelbinding worden beschouwd.[61] Hoe nauwer de verwantschap, hoe eerder er sprake is van verenigbaar gebruik. Een tweede factor is de aard van de gegevens (artikel 9, tweede lid, sub b, Wbp). Te denken valt uiteraard aan de in artikel 16 Wbp genoemde bijzondere gegevens. Daarnaast wijst de MvT erop dat de context waarin gegevens worden gebruikt, deze tot gevoelige gegevens kunnen maken.[62] Zo kan een persoonsgegeven dat ziet op een betalingsachterstand, gevolgen hebben voor de kredietwaardigheid.[63] Daarbij geldt dat hoe gevoeliger het gegeven, hoe minder snel van het oorspronkelijke doel mag worden afgeweken. Een derde factor wordt gevormd door de gevolgen van de beoogde verwerking voor de betrokkene (artikel 9, tweede lid, sub c, Wbp). Daarbij is met name ook relevant of de gegevens worden gebruikt als basis voor mogelijke beslissingen jegens de betrokkene. De twee laatstgenoemde factoren zijn de wijze waarop de gegevens zijn verkregen (artikel 9, tweede lid, sub d, Wbp), bijvoorbeeld buiten betrokkene om of juist met diens instemming, en de mate waarin jegens betrokkenen wordt voorzien in passende waarborgen.[64] Genoemde factoren dienen in onderling verband te worden toegepast. Zo is het gebruik van de gegevens in de gemeentelijke basisadministratie, die weinig informatie bevatten, voor uiteenlopende doelen veel eerder in overeenstemming met artikel 9 Wbp dan het door een ziekenfonds aan een fabrikant verstrekken van gegevens van patiënten die een bepaalde operatie hebben ondergaan.

Tot slot zij er op gewezen dat indien er geen sprake is van verenigbaar gebruik, de verwerking in uitzonderlijke omstandigheden toch rechtmatig kan zijn uit hoofde van artikel 43 Wbp. Conform artikel 13 van de Privacyrichtlijn kan op grond van deze bepaling de eis van verenigbaar gebruik worden

58 Kranenborg & Verhey 2011, p. 93.
59 *Kamerstukken II* 1997/98, 25 892, nr. 3 (MvT), p. 89.
60 Ibid., p. 90.
61 Ibid.
62 Ibid.
63 Zo leidt de opname in het zogenoemde Incidentenregister tot uitsluiting van vrijwel alle vormen van leningen en kredietverstrekkingen indien sprake is van (zware) verdenking van hypotheekfraude. Zie: Rb. Amsterdam 9 februari 2012, *LJN* BW0269.
64 Eventueel bezwaar kunnen maken, eventueel van te voren informeren, CBP 19 jan 2006, 2006-0703.

1912170 01165

doorbroken voor zover dat noodzakelijk is in het belang van een van de aldaar opgesomde doeleinden. Het gaat hier evenwel om uitzonderingen: artikel 43 Wbp dient restrictief te worden geïnterpreteerd.[65]

2.4.4 Jurisprudentie doelbinding

De eerstgenoemde factor – verwantschap – heeft in de jurisprudentie ten aanzien van verstrekking van persoonsgegevens aan andere organen of instellingen het meeste aandacht gekregen. Zo achtte de Afdeling bestuursrechtspraak het doel van de kentekenregistratie – de goede uitvoering en handhaving van de WVW – te ver verwijderd van het doel om straatprostitutie tegen te gaan.[66] De gemeente Heerlen had bij de RDW gegevens opgevraagd om rijdende klanten van straatprostituees te kunnen identificeren. Het CBP kwam tot de conclusie dat het doeleinde waarvoor gegevens ten aanzien van het waterverbruik door huishoudens waren verzameld zo weinig verwantschap toonde met het doeleinde waarvoor de sociale dienst deze gegevens wenste te gebruiken, dat verstrekken geen vorm van verenigbaar gebruik opleverde.[67] De CRvB achtte daarentegen het op verzoek verstrekken van gegevens door het RDW aan de uitkeringsinstanties wel in overeenstemming met de Wbp nu de belanghebbende op grond van artikel 17 Wet werk en bijstand (Wwb) deze gegevens eigenlijk zelf aan genoemde instanties had moeten verstrekken. Daarbij lijkt de nadruk meer op de aard van de gegevens dan op de verwantschap van de doeleinden gelegd te zijn.[68]

2.4.5 Doelbinding in de Wpg

Een laatste opmerking is dat ook de Wpg het beginsel van doelbinding kent. Artikel 5 bepaalt in het eerste lid dat politiegegevens slechts verwerkt worden voor zover dit noodzakelijk is voor de bij of krachtens deze wet geformuleerde doeleinden. Het derde lid voegt daar aan toe dat politiegegevens uitsluitend voor een ander doel worden verwerkt dan waarvoor zij zijn verkregen voor zover deze wet daar uitdrukkelijk in voorziet.

2.5 Uitwisseling van persoonsgegevens

De Wbp laat de uitwisseling van persoonsgegevens onder bepaalde omstandigheden toe. Daartoe onderscheidt de wet tussen incidentele en structurele verstrekking van gegevens. Met betrekking tot de doorgifte is de term 'koppelen' van persoonsgegevens in het gewone spraakgebruik ingeburgerd. Het is echter geen juridische term die in de Wbp of in een andere wet omschreven wordt.

De wetgever heeft ervan afgezien een aparte bepaling over koppeling in de Wbp op te nemen, mede omdat het geen eenduidig begrip is en de algemene bepalingen ten aanzien van de verwerking van persoonsgegevens voldoende soelaas moeten bieden.[69] De memorie van toelichting wijst tevens op ontwikkelingen in de informatietechnologie die tot verruimde mogelijkheden tot koppeling leiden en van de maatschappelijke acceptatie ervan.[70] Ook mede daarom is er van afgezien om te dien aanzien strikte bepalingen in de wet op te nemen.

In zijn algemeenheid kan het koppelen van persoonsgegevens worden omschreven als het combineren van gegevens uit verschillende gegevensbestanden. Dit is een vrij ruime omschrijving waaronder zowel

65 T.F.M. Hooghiemstra, *Tekst en toelichting Wet bescherming persoonsgegevens*, Den Haag: Sdu Uitgevers 2007, p. 80.
66 Afdeling bestuursrechtspraak 12 mei 2004, *LJN* AO9207, *JB* 2004, 251, m. nt. G. Overkleeft-Verburg.
67 CBP 12 juli 2006, nr. 2005-1447.
68 CRvB 24 juni 2008, *LJN* BD5289, *AB* 2008, 286, m. nt. H.E. Bröring.
69 *Kamerstukken II* 1997/98, 25 892, nr. 3 (MvT), p. 93.
70 Ibid.

1912170 01165

het gevraagd of ongevraagd verstrekken van een enkel persoonsgegeven kan vallen als het bieden van inzage in het geheel aan aanwezige gegevens. Het tegen elkaar uitdraaien van bestanden om vast te stellen welke personen in beide bestanden voorkomen – en de gegevens omtrent die personen te combineren – kan bij uitstek als een als een vorm van koppelen worden beschouwd.

Al deze vormen van koppelen zijn verwerkingen in de zin van de Wbp. Daarom passeren hieronder eerst enkele relevante bepalingen uit die wet de revue. Daarnaast is er speciale aandacht voor het verstrekken van politiegegevens onder vigeur van de Wpg, het verstrekken van justitiële en strafvorderlijke gegevens onder vigeur van de Wjsg en voor het verwerken van persoonsgegevens in samenwerkingsverbanden.

2.5.1 Koppelen en de Wbp

Het begrip verwerking dekt vrijwel ieder gebruik van persoonsgegevens; daaronder het opvragen, raadplegen, verstrekken, andere vormen van terbeschikkingstelling, samenbrengen en met elkaar in verband brengen (artikel 1, sub b, Wbp). Dat impliceert dat de materiële normen uit de Wbp zowel van toepassing zijn op de verstrekking van een persoonsgegeven in een individueel geval, op de structurele verstrekking, op het geven van inzage in het geheel van de aanwezige persoonsgegevens, als op het vergelijken van twee bestanden om te zien welke personen in beide bestanden voorkomen.

Ten aanzien van deze verwerkingen is reeds aangegeven dat hier het vereiste geldt dat de verwerking niet onverenigbaar is met het doel waarvoor de gegevens zijn verzameld. Daarbij zal iedere vorm van 'koppeling' op zijn eigen merites moeten worden beoordeeld. De hiervoor al besproken zaak met betrekking tot de verstrekking van NAW-gegevens door de RDW aan de gemeente Heerlen om op te kunnen treden tegen straatprostitutie is daarvan een voorbeeld. De Afdeling achtte dat doel te ver verwijderd van het doel waarvoor de gegevens door de RDW waren verzameld. [71] Ook speelde een rol dat de gegevens gebruikt zouden worden ten behoeve van het opleggen van een dwangsom.

Liggen de doelen veeleer in elkaars verlengde, dan kunnen ook verder gaande vormen van koppeling eerder geoorloofd zijn. Heeft een bestuursorgaan bijvoorbeeld online toegang tot de NAW-gegevens uit de GBA en is de consultatie slechts bedoeld om de reeds bij het bestuursorgaan berustende gegevens up to date te houden, dan is dat al snel geoorloofd. In een dergelijk geval kan vrij snel aan de eis van verenigbaar gebruik voldaan zijn. Er bestaat immers niet de bedoeling een nieuwe groep van personen 'naar een bepaald criterium in beeld te brengen'.[72]
Dat ligt veelal anders bij het tegen elkaar uitdraaien van twee bestanden. Een dergelijke verwerking is er op gericht te zien welke personen in beide voorkomen. Op die manier wordt een nieuwe groep van personen in beeld gebracht, namelijk degenen die in beide bestanden voorkomen. Deze vorm behoeft volgens de memorie van toelichting bij de Wbp vanuit het gezichtspunt van het verenigbaar gebruik bijzondere aandacht, wat bijvoorbeeld ook blijkt uit de opname van een specifieke bepaling in de wet ten aanzien van het gebruik van identificerende nummers (artikel 24).[73]

Uit het vereiste van verenigbaar gebruik en het vereiste van subsidiariteit kan worden afgeleid dat gezocht zal moeten worden naar zodanige vormen van verwerking dat er zo min mogelijk gegevens verspreid worden. Stel dat twee bestanden van twee verschillende verantwoordelijken tegen elkaar moeten worden afgedraaid om te zien of er dubbelen in zitten. Dat is technisch mogelijk zonder dat één van de verantwoordelijken daarmee komt te beschikken over alle gegevens van de ander. Alleen de treffers

71 Afdeling bestuursrechtspraak 12 mei 2004, *LJN* AO9207, *JB* 2004, 251, m.nt. G. Overkleeft-Verburg.
72 *Kamerstukken II* 1997/98, 25 892, nr. 3 (MvT), p. 93.
73 Ibid.

1912170 01165

kunnen aan één van beide of aan beide verantwoordelijken worden meegedeeld. De memorie van toelichting bij de Wbp geeft als voorbeeld de vergelijking van het gedetineerdenbestand en het bestand van de ontvangers van een sociale uitkering om te controleren of er niet ten onrechte uitkeringen worden verstrekt aan gedetineerden. Daarbij is het niet noodzakelijk dat penitentiaire inrichtingen kennis nemen van de gegevens van de uitkeringsinstantie. Evenmin is het noodzakelijk dat de uitkeringsinstantie kennis kan nemen van alle persoonsgegevens van alle gedetineerden. De bedoeling van de koppeling is slechts dat bij de uitkeringsinstanties bekend wordt wie èn een uitkering krijgt èn gedetineerde is. Die verstrekking van treffers aan het desbetreffende uitvoeringsorgaan vindt in dat geval haar rechtvaardiging in de opdracht de criteria voor de toekenning van een uitkering toe te passen. Door technische en organisatorische maatregelen dient voorkomen te worden dat er meer gegevens uitgewisseld worden. Mede doordat de verspreiding van gegevens beperkt blijft tot het noodzakelijke minimum is er dan sprake van verenigbaar gebruik, aldus de toelichting.[74]

De huidige Wwb kent overigens een reeks van bepalingen die zien op de gegevensuitwisseling ten behoeve van de uitvoering van deze wet. Tal van instanties hebben de wettelijke plicht gekregen om aan het college van B&W opgaven en inlichtingen te verstrekken die noodzakelijk zijn voor de uitvoering van de wet (artikel 64). Deze verstrekkingen zijn daarmee te baseren op artikel 8, sub c, Wbp. Daarbij is in de Wwb uitdrukkelijk vastgelegd dat bij deze verstrekkingen gebruik gemaakt wordt van het burgerservicenummer of bij het ontbreken daarvan van het sociaal-fiscaalnummer (artikel 68 Wwb). De inlichtingenplicht van het college ten opzichte van andere in artikel 67 Wwb genoemde instanties vindt zijn grens waar de persoonlijke levenssfeer van de betrokkenen daardoor onevenredig wordt geschaad.

2.5.2 Risico-profielen

Een andere methode om te voorkomen dat in alle gegevens inzage wordt gegeven is het werken met risicoprofielen en de uitwisseling te beperken tot persoonsgegevens die passen in de opgestelde profielen. Dat wil niet zeggen dat deze methode daarmee voor kritiek gevrijwaard is. Het CBP achtte de door de SIOD uitgevoerde koppeling op grond van risicoprofielen in strijd met de wet, want disproportioneel. Een hele categorie personen werd bejegend als potentiële fraudeurs, en daarmee was het belang van controle niet in evenwicht met het belang van bescherming van de persoonlijke levenssfeer, zeker nu overbodige gegevens niet verwijderd werden en personen niet werden geïnformeerd.[75]

2.5.3 Verstrekkingen op grond van de Wpg en de Wjsg

De Wpg kent een aantal bepalingen die zien op het verstrekken van politiegegevens door de politie. Daarbij maakt de wet een onderscheid tussen de structurele verstrekking (artikel 18), de incidentele verstrekking (artikel 19) en de verstrekking ten behoeve van samenwerkingsverbanden (artikel 20). Bij iedere soort verstrekking wordt overigens aan degene die de gegevens ontvangt een geheimhoudingsplicht opgelegd, behoudens voor zover een bij of krachtens de wet gegeven voorschrift tot verstrekking verplicht of zijn taak daartoe noodzaakt (artikel 7 lid 2 Wpg).

Het eerste lid van artikel 18 Wpg stelt dat bij of krachtens algemene maatregel van bestuur personen en instanties kunnen worden aangewezen aan wie of waaraan, met het oog op een zwaarwegend algemeen belang, politiegegevens worden of kunnen worden verstrekt ter uitvoering van de bij of krachtens die algemene maatregel van bestuur aan te geven taak. Het bedoelde AMvB is het Besluit Politiegegevens. Artikel 4:2 lid 1 Besluit Politiegegevens legt vast dat bepaalde gegevens kunnen worden verstrekt aan een

74 Ibid., p. 94.
75 Zie de berichten van het CBP in *Privacy en Informatie* 2011, 2 en *Privacy en Informatie* 2010, 215.

1912170 01165

aantal in het eerste lid met name genoemde instellingen, zoals onder andere het Waarborgfonds Motorverkeer, de Halt-bureaus, de Raad voor de Kinderbescherming, en de Algemeen Inspectiedienst van het Ministerie van LNV.

Het tweede lid van artikel 18 Wpg voegt daar de meer algemene bepaling aan toe dat deze gegevens, voor zover zij deze behoeven voor een goede uitvoering van hun taak, worden verstrekt aan ambtenaren die bij of krachtens de wet zijn belast met het houden van toezicht op de naleving van de bij regeling van Onze Ministers aangewezen wetgeving, voor zover het betreft gegevens over de naleving van die wetgeving, en er tussen de verantwoordelijke en de betreffende ambtenaren afspraken zijn gemaakt over welke gegevens verstrekt worden, in welke gevallen en onder welke voorwaarden. Bij ministeriële regeling (Regeling aanwijzing wetgeving ex artikel 4:2, tweede lid Besluit politiegegevens) is een reeks van wetten aangewezen, zoals bijvoorbeeld de Wet Milieubeheer, de Arbeidstijdenwet, de Scheepvaartverkeerswet, en de Arbeidsomstandighedenwet, alsmede de gemeentelijke verordeningen betreffende het escortbedrijf.[76]

Artikel 19 Wpg, dat ziet op de incidentele verstrekking, bepaalt dat in bijzondere gevallen de verantwoordelijke, voor zover dit noodzakelijk is met het oog op een zwaarwegend algemeen belang, in overeenstemming met het op grond van de Politiewet 1993 bevoegde gezag, kan beslissen tot het verstrekken van politiegegevens aan personen of instanties voor de volgende doeleinden: a. het voorkomen en opsporen van strafbare feiten; b. het handhaven van de openbare orde; c. het verlenen van hulp aan hen die deze behoeven; d. het uitoefenen van toezicht op het naleven van regelgeving.

De Wjsg regelt de verstrekking van justitiële en strafvorderlijke gegevens die bij het OM berusten. Artikel 39f is hier het meest relevant. Het eerste lid bepaalt dat voor zover het noodzakelijk is voor een zwaarwegend belang door het College van procureurs-generaal aan personen of instanties strafvorderlijke gegevens verstrekt worden ten behoeve van:

a. het voorkomen en opsporen van strafbare feiten,
b. het handhaven van de orde en veiligheid,
c. het uitoefenen van toezicht op het naleven van regelgeving,
d. het nemen van een bestuursrechtelijke beslissing,
e. het beoordelen van de noodzaak tot het treffen van een rechtspositionele of tuchtrechtelijke maatregel, of
f. het verlenen van hulp aan slachtoffers en anderen die bij een strafbaar feit betrokken zijn.

Het tweede lid voegt daar de voorwaarde aan toe dat slechts strafvorderlijke gegevens aan personen of instanties als bedoeld in het eerste lid worden verstrekt, voor zover die gegevens voor die personen of instanties: a. noodzakelijk zijn met het oog op een zwaarwegend algemeen belang of de vaststelling, de uitoefening of de verdediging van een recht in rechte, en b. in zodanige vorm worden verstrekt dat herleiding tot andere personen dan betrokkene, redelijkerwijs wordt voorkomen. De Wjsg (artikel 52) legt daarbij vast dat de verstrekte gegevens geheim moeten worden gehouden, behoudens voorzover een bij of krachtens deze wet gegeven voorschrift mededelingen toelaat, dan wel de uitvoering van de taak met het oog waarop de gegevens zijn verstrekt tot het ter kennis brengen daarvan noodzaakt. Het College van procureurs-generaal heeft de wijze waarop deze bevoegdheid wordt uitgeoefend vastgelegd in een aanwijzing.[77]

76 Regeling van 1 februari 2008, nr. 5528485/08, houdende regels tot het aanwijzen van wetgeving, genoemd in artikel 4:2, tweede lid, van het Besluit politiegegevens.

77 Aanwijzing verstrekking van strafvorderlijke gegevens voor buiten de strafrechtspleging gelegen doeleinden (aanwijzing wet justitiële en strafvorderlijke gegevens), *Stcrt.* 2010, 11 804.

1912170 01165

Voor de verstrekking van justitiële gegevens aan bestuursorganen zijn de artikelen 8a en 9 Wjsg het meest relevant. Artikel 8a bepaalt dat voor zover dit noodzakelijk is met het oog op een zwaarwegend algemeen belang, het College van procureurs-generaal in de gevallen waarin het ingevolge artikel 39e of 39f bevoegd is strafvorderlijke gegevens te verstrekken, justitiële gegevens kan verstrekken. Artikel 9 Wjsg voegt daaraan toe dat, voor zover dit noodzakelijk is met het oog op een zwaarwegend algemeen belang en voor een goede taakuitoefening van degene aan wie justitiële gegevens worden verstrekt, bij algemene maatregel van bestuur personen of instanties die met een publieke taak zijn belast, kunnen worden aangewezen aan wie justitiële gegevens kunnen worden verstrekt. Daarbij kunnen nadere voorschriften worden gegeven in verband met de verwerking en verdere verwerking. Het Besluit Justitiële gegevens bepaalt dat bepaalde justitiële gegevens kunnen worden verstrekt aan onder meer de burgemeester (artikel 11) ten behoeve van het nemen van bepaalde besluiten in het kader van bijvoorbeeld de Drank- en Horecawet en de Wet op de kansspelen (artikel 13), ten behoeve van de uitvoering van de Wet Bibob (artikel 15), aan Onze Minister ten behoeve van de controle van rechtspersonen met het oog op de voorkoming en bestrijding van misbruik van rechtspersonen, waaronder het plegen van misdrijven en overtredingen van financieel-economische aard door of door middel van deze rechtspersonen, bedoeld in artikel 2, eerste lid, van de Wet controle op rechtspersonen (artikel 16 sub a), ten behoeve van de uitvoering van de Vreemdelingenwet (artikel 19), en aan inspecteambtenaren van Verkeer en Waterstaat (artikel 22).

De mogelijkheden tot verstrekking van onder de politie en het OM berustende gegevens zijn de afgelopen jaren verruimd. Het gevolg daarvan is dat de verwerking van strafrechtelijke gegevens in de zin van artikel 16 Wbp door anderen dan de politie en het OM is toegenomen. Deze verwerking valt onder de vigeur van de Wbp. De huidige Wbp bepaalt dat het verbod om strafrechtelijke persoonsgegevens te verwerken niet van toepassing is indien de verwerking geschiedt door organen die deze gegevens krachten de Wpg of de Wjsg hebben verkregen (artikel 22 lid 1 Wbp).

Het wetsvoorstel tot wijziging van de Wbp[78] voorzag overigens oorspronkelijk in een wijziging van artikel 23 Wbp ten aanzien van de verwerking van bijzondere gegevens door ombudsmannen, accountants-organisaties en toezichthouders. In het voorstel was de mogelijkheid opgenomen dat toezichthouders in de zin van artikel 5:11 Awb deze gegevens kunnen verwerken als dit noodzakelijk is met het oog op een zwaarwegend algemeen belang ter uitvoering van de hun wettelijk opgedragen taken en bij die uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad. Als grondslag voor deze bepaling diende artikel 8, vierde lid van de Privacyrichtlijn, waarin lidstaten de mogelijkheid wordt geboden om afwijkingen van het verbod op verwerken van bijzondere persoonsgegevens toe te staan, onder de voorwaarden dat de verwerking geschiedt om redenen van zwaarwegend algemeen belang en er tevens passende waarborgen worden genomen. De Raad van State stelde in zijn advies dat uit de toelichting bij de beoogde wijziging onvoldoende bleek dat aan deze voorwaarden was voldaan. [79] Volgens de Raad waren de categorieën van verwerkers en de specifieke situaties van verwerkingen die werden besproken in deze toelichting niet te veralgemeniseren. Voorts stelde het adviesorgaan dat er behoefte bestond aan een nadere toelichting op de betekenis, inhoud en toepassingsmogelijkheden van het in het wetsvoorstel opgenomen criterium dat de verwerking 'noodzakelijk voor de uitvoering van de wettelijk opgedragen taak' dient te zijn. Volgens de Raad moest duidelijk worden gemaakt op welke wijze dit criterium door de verschillende categorieën in de praktijk zal worden ingevuld, en welke belangen kunnen en moeten worden betrokken bij de afweging die aan deze invulling ten grondslag ligt. De minister deelde de mening van de Raad van State dat ombudsmannen,

78 *Kamerstukken II* 2008/09, 31 841, nr. 2.
79 *Kamerstukken II* 2008/09, 31 841, nr. 4 (Advies Raad van State en Nader Rapport).

1912170 01165

toezichthouders en accountantsorganisaties te verschillend zijn om in een eenduidig criterium te vatten en besloot daarom om af te zien van een algemene uitzonderingsgrond voor toezichthouders en accountantsorganisaties (de bepaling is gehandhaafd voor ombudsmannen). Niet uitgesloten is dat op termijn een uitzonderingsgrond zal worden opgenomen voor toezichthouders in sectorale wetgeving, aldus het Nader Rapport.[80]

2.5.4 Samenwerkingsverbanden

Naast het verstrekken van gegevens door het ene bestuursorgaan aan het andere en het koppelen van bestanden is er in toenemende mate ook sprake van (andere) samenwerkingsverbanden tussen bestuursorganen, soms ook aangevuld met particuliere organisaties. Deze samenwerkingsverbanden zijn veelal in het bijzonder ook bedoeld om criminaliteit tegen te gaan en de veiligheid te bevorderen. Een voorbeeld zijn de Regionale Informatie- en Expertise Centra (RIEC), die hierna nog aan de orde komen. In deze samenwerkingsverbanden worden persoonsgegevens verwerkt. Dat impliceert dat de Wbp van toepassing is (en bij participatie van de politie en/of het OM ook de Wpg respectievelijk de Wjsg). In het algemeen kan men stellen dat deze wetgeving zich niet per se verzet tegen het gebruik van persoonsgegevens in deze samenwerkingsverbanden, maar daar wel de nodige eisen aan stelt.

Voor een zorgvuldige gegevensverwerking in het samenwerkingsverband dient er in de eerste plaats een duidelijke doelomschrijving te worden geformuleerd, in het licht van de taakuitoefening van degenen die samenwerken.[81] Daarnaast moet duidelijk zijn welke partijen binnen het samenwerkingsverband toegang hebben tot welke gegevens. Steeds is ook artikel 9 Wbp van belang, waarin de eis vastligt dat het doel van de verwerking binnen het samenwerkingsverband niet onverenigbaar dient te zijn met het doel waarvoor de gegevens zijn verzameld. Voorts volgt uit de eisen van proportionaliteit en subsidiariteit dat alleen die gegevens uitgewisseld worden die nodig zijn om dat doel te bereiken. Voor de verwerking van politiegegevens in een dergelijk samenwerkingsverband is steeds een zwaarwegend belang nodig.

De Wjsg kent geen afzonderlijke bepaling die in het bijzonder ziet op samenwerkingsverbanden. Verstrekkingen van gegevens in het kader van een samenwerkingsverband is uiteraard wel onderworpen aan het regime van de Wjsg. De bijlage bij de Aanwijzing verstrekking van strafvorderlijke gegevens van het College van procureurs-generaal besteedt wel uitdrukkelijk aandacht aan samenwerking met andere partners. Daarbij wordt onder meer een onderscheid gemaakt tussen het gezamenlijk opzetten van een nieuw gegevensbestand en het uitwisselen van gegevens. In het laatste geval is justitie gebonden aan de Wjsg, en de partner(s) in het samenwerkingsverband, niet zijnde de politie, aan de Wbp.

Artikel 20 Wpg ziet speciaal op de verstrekking van politiegegevens ten behoeve van een samenwerkingsverband. De bepaling maakt dat mogelijk, voor zover dit met het oog op een zwaarwegend algemeen belang noodzakelijk is ten behoeve van een samenwerkingsverband van de politie met personen of instanties voor de volgende doeleinden: a. het voorkomen en opsporen van strafbare feiten; b. het handhaven van de openbare orde; c. het verlenen van hulp aan hen die deze behoeven; d. het uitoefenen van toezicht op het naleven van regelgeving. Daarbij bepaalt het tweede lid dat in de beslissing, bedoeld in het eerste lid, wordt vastgelegd ten behoeve van welk zwaarwegend algemeen belang de verstrekking noodzakelijk is, ten behoeve van welk samenwerkingsverband de politiegegevens worden verstrekt alsmede het doel waartoe dit is opgericht, welke gegevens worden verstrekt, de voorwaarden onder welke de gegevens worden verstrekt en aan welke personen of instanties de gegevens worden verstrekt.

80 Ibid., p. 3.
81 C.M. Bitter & F.W. Bleichrodt, 'Informatievoorziening in het kader van de bestuursrechtelijke aanpak van criminaliteit en terrorisme', in: *Bestuursrechtelijke aanpak van criminaliteit en terrorisme* (VAR-reeks 138), Den Haag: Boom Juridische Uitgevers 2007, p. 153.

1912170 01165

Voor bestuursorganen, opsporingsdiensten en OM, die samenwerken in een RIEC, is het op grond van artikel 20 Wpg aldus mogelijk om op structurele basis politiegegevens te ontvangen. Daartoe wordt een convenant gesloten. De RIEC's zijn samenwerkingsverbanden van gemeenten, provincies, politie, OM, de Belastingdienst, bijzondere opsporingsdiensten (SIOD, FIOD-ECD) en de Koninklijke Marechaussee. Er zijn elf centra die op basis van een bestuurlijk akkoord samenwerken om georganiseerde criminaliteit tegen te gaan.[82] Dit akkoord is uitgewerkt in regionale convenanten, waarin met name afspraken zijn gemaakt over het delen van informatie.[83] De RIEC's werken op hun beurt weer samen met andere expertisecentra, zoals het Expertisecentrum Mensenhandel en Mensensmokkel (EMM), het Vastgoed Intelligence Center (VIC), de Landelijke Taskforce Georganiseerde Hennepteelt, de Regionale Coördinatiepunten Fraudebestrijding (RCF) en het Centrum voor Criminaliteitspreventie en Veiligheid (CCV).

Gegevens die de verschillende convenantpartners vergaren in het kader van hun toezichts- of opsporingstaak worden zo mogelijk gedeeld met de andere partners. De technische mogelijkheden daartoe worden steeds geavanceerder, maar het delen en koppelen van gegevens bergt ook gevaren in zich. Met name bestaat het gevaar dat het doel waarvoor de bevoegdheid tot gegevensuitvraag is verleend uit het oog wordt verloren ('function creep').[84] Aangezien dit vooral problematisch is in verband met de bescherming van persoonsgegevens, wordt bij het delen zoveel mogelijk aangesloten bij de doelstellingen waarvoor de bevoegdheid tot het verzamelen van de informatie is gegeven. Voor de kwaliteit en de betrouwbaarheid van de informatie is het van groot belang dat de gegevens binnen hun context worden beschouwd. Dat is niet altijd gegarandeerd. Bij hergebruik worden gegevens die zijn bijeen gebracht en geduid in een bepaalde context in een andere context geplaatst en gecombineerd met weer andere gegevens. Daardoor kan een vertekend of zelfs onjuist beeld ontstaan. Een onjuist beeld blijkt voor de betrokkene zeer lastig te herstellen en kan hem nog lang achtervolgen.[85] Ook om deze reden is de doelbinding van belang.

Een ander voorbeeld van een samenwerkingsverband zijn de zogeheten Veiligheidshuizen, waarin verschillende partijen (politie, OM en RvK) structureel samenwerken om jeugdigen op het rechte pad te brengen/houden. Dat geschiedt in het bijzonder door bespreking van individuele gevallen in overleggen. Daarbij wordt een aanzienlijke hoeveelheid persoonsgegevens uitgewisseld, waaronder ook gevoelige gegevens als strafrechtelijke. Het CBP signaleert in zijn evaluatie van het Veiligheidshuis Fryslân (CBP maart 2011)[86] een reeks van knelpunten. Zo acht het CBP onder meer onvoldoende duidelijk vastgelegd welke gedragingen of incidenten tot bespreking in het overleg leiden, wat volgens het CBP strijdt met artikel 6 Wbp. Opname van gegevens van 6-12 jarigen, die niet strafrechtelijk vervolgbaar zijn, acht het CBP bovenmatig en daarom in strijd met artikel 11 Wbp. Voorts wijst het CBP erop dat er door het OM ook tal van gegevens verstrekt worden die tijdens de overleggen helemaal niet aan de orde komen en waarvan de verstrekking dus blijkbaar niet noodzakelijk is (in de zin van de artikelen 3f lid 1 en 39f lid 2 aanhef en sub a Wjsg).

82 Bestuurlijk akkoord Geïntegreerde Decentrale Aanpak Georganiseerde Misdaad, september 2008. Raadpleegbaar via:<www.vng.nl>.
83 Zie onder meer: *Kamerstukken II* 2010/11, 29 911, bijlage bij nr. 54 (Jaarverslag RIEC's 2010).
84 *iOverheid* (rapport van 2 maart 2011, WRR), Amsterdam: Amsterdam University Press 2011 en J.E.J. Prins, 'Function creep en privacy', *Justitiële verkenningen* 2011, 37, nr. 8, p. 9-21. Zie ook: E.J. Dommering, 'Het bestuur als de tovenaarsleerling van ICT', *NJB* 2012, 87, afl. 2, p. 109-115.
85 Y. Buruma, 'Het recht op vergetelheid. Politiële en justitiële gegevens in een digitale wereld', in: D. Broeders, C.M.K.C. Cuijpers & J.E.J. Prins (red.), *De staat van informatie* (WRR-verkenning nr. 25), Amsterdam: Amsterdam University Press 2011, p. 165-222.
86 *Veiligheidshuis Fryslân*, Onderzoek naar de verwerking van persoonsgegevens in het kader van het Justitieel Casusoverleg en JCO-Support , Rapportage van definitieve bevindingen (CBP z2010-00827).

1912170 01165

Een belangrijke uitspraak over samenwerkingsverbanden van de Afdeling bestuursrechtspraak ziet op het zogeheten Alijda project in Rotterdam.[87] Dit betrof een samenwerkingsverband van de gemeente Rotterdam, politie, justitie, de Belastingdienst en het FIOD, die daartoe een convenant hadden gesloten. Bij dit convenant hoorde een privacyregeling. Naast de convenantpartijen waren het Kadaster, de KvK en de UWV bij het project betrokken. De samenwerking was tot stand gebracht om drugsrunners, drugsdealers, de eigenaars van drugspanden, en in het verlengde daarvan ook malafide huisjesmelkers, beter te kunnen aanpakken. De Afdeling was van oordeel dat artikel 8 Wbp een afdoende grondslag bood voor de verwerking van de gewone – niet bijzondere – persoonsgegevens ten behoeve van de aanpak van malafide huisjesmelkers. Ook de verwerking van strafrechtelijke persoonsgegevens in de zin van artikel 22, eerste lid sub c Wbp kon noodzakelijk worden geacht voor de kwaliteit van de handhaving en was niet disproportioneel. De mogelijkheid dat ook instanties die niet partij waren bij het ten behoeve van het samenwerkingsverband overeengekomen convenant, inzage konden hebben in deze strafrechtelijke persoonsgegevens achtte de Afdeling echter in strijd met artikel 22 Wbp en met de toen nog geldende Wet politieregisters. Het gebruik van een 'zwarte lijst' voldeed aan het noodzakelijkheidscriterium van artikel 7 Wbp, omdat dat hierdoor de kwaliteit en de effectiviteit van toezicht en handhaving op het door het Alijda-project bestreken terrein toe bleek te nemen. De zwarte lijst voldeed echter niet aan het zorgvuldigheidscriterium van artikel 6 Wbp. De privacyregeling bevatte geen duidelijke criteria om te bepalen in welke gevallen een gedraging of incident tot plaatsing op die lijst leidde. Evenmin bleek duidelijk uit de regeling welke personen of instanties toegang tot de voor intern gebruik bedoelde lijst hadden. Uit deze uitspraak wordt daarom wel afgeleid dat artikel 6 Wbp impliceert dat er voor dit type samenwerking een convenant en een privacyregeling nodig is.

Het toegenomen belang van een zorgvuldige regeling van de samenwerking in samenwerkingsverbanden blijkt ook uit een wetswijziging van de Wbp die op 9 februari 2012 in werking is getreden.[88] In artikel 22 Wbp, dat ziet op de verwerking van strafrechtelijke gegevens, is een nieuw lid opgenomen dat het verbod om dergelijke gegevens te verwerken niet van toepassing verklaart op verwerkingen van strafrechtelijke gegevens door en ten behoeve van publiekrechtelijke samenwerkingsverbanden, indien de verwerking noodzakelijk is voor de uitvoering van de taak van de partners en bij de uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad. Het vastleggen van redenen waarom de verwerking noodzakelijk is en van de wijze waarop een zorgvuldige verwerking wordt gewaarborgd is daarbij van belang. Het voorbeeld van het Alijda-project laat zien, dat een convenant met privacyregeling daartoe een goed middel is, als dit maar helder en duidelijk gebeurt.

2.5.5 Convenanten

In het kader van dit onderzoek is een korte survey gedaan naar convenanten met betrekking tot gegevensuitwisseling.[89] Het beeld dat daaruit naar voren komt is dat deze convenanten weinig concrete handvatten bieden voor beslissingen om al dan niet over te gaan tot het doorverstrekken van gegevens in een bepaald geval. Om dit te illustreren geven we enkele voorbeelden.

In het kader van de bestuurlijke en strafrechtelijke aanpak van georganiseerde criminaliteit is er in 2008 een landelijk convenant gesloten tussen Binnenlandse Zaken, Justitie, Financiën, SZW, Defensie, de VNG en het College van procureurs-generaal. Dit Bestuurlijk Akkoord Geïntegreerde Decentrale Aanpak Georganiseerde Misdaad[90] bevat de doelstellingen van en uitgangspunten voor de regionale samenwerking. Er wordt een aantal verschijningsvormen van criminaliteit opgesomd, die in het kader van het

87 Afdeling bestuursrechtspraak 4 juli 2007, *LJN* BA8742, *JB* 2007, 165, m. nt. M.O-V., *NJ* 2007, 652, m. nt. G. Overkleeft-Verburg.
88 Wijziging Wet bescherming persoonsgegevens inzake vermindering administratieve lasten en nalevingskosten, *Stb.* 1996, 33.
89 Zie *infra*, par 6.1 voor een overzicht van de geraadpleegde convenanten.
90 Raadpleegbaar via <www.vng.nl>

1912170 01165

Akkoord zullen worden bestreden. In het laatst opgesomde punt wordt de mogelijkheid geschapen om meer verschijningsvormen te bestrijden die naar voren komen in het periodiek op te stellen nationaal dreigingsbeeld.

Het akkoord expliciteert de juridische bevoegdheden van de toekomstige regionale convenantpartners en spreekt de intentie uit dat zij op basis van gelegenheidscoalities gegevens zullen uitwisselen. De toelaatbaarheid van het ontvangen van gegevens van andere convenantpartners is gebaseerd op artikel 8 sub e en artikel 22, eerste lid, Wbp. Het Akkoord maakt ook melding van de noodzakelijkheidstoets van artikel 8 sub f Wbp. Het Akkoord zegt echter weinig meer dan dat de toets moet worden uitgevoerd en dat verwerking van persoonsgegevens noodzakelijk is ter bestrijding van de georganiseerde misdaad. Verstrekking aan andere dan de partners blijft vallen onder het specifiek op die partner betrekking hebbende verstrekkingenregime, maar de decentrale partner kan slechts gegevens die hij in het kader van de samenwerking van een convenantpartner heeft ontvangen aan derden verstrekken met uitdrukkelijke toestemming van degene van wie de gegevens zijn ontvangen.

In regionale convenanten worden deze uitgangspunten uitgewerkt ten behoeve van de samenwerking in de RIEC's. Wat betreft de persoonsgegevens wordt een gegevensset vastgesteld, die wordt aangemeld bij het College bescherming persoonsgegevens (CBP). De overige afspraken in het convenant hebben een weinig concrete inhoud. Zo wordt de intentie uitgesproken nadere afspraken te maken over de naleving van de Wbp en wordt gesteld dat men zal waken voor de verwerking van persoonsgegevens binnen de wettelijke kaders. Het toestemmingsvereiste voor doorlevering wordt vastgelegd en de wettelijke geheimhoudingsplichten bevestigd. De naleving van de Wbp wordt getoetst aan de hand van een checklist. Daarbij valt op dat de verantwoordelijkheid voor de gegevensverwerking verspreid blijft over de convenantpartners: ieder is bevoegd en verantwoordelijk op basis van het eigen wettelijk kader voor gegevensverwerking. Waar iedereen verantwoordelijk is, is in feite niemand verantwoordelijk, althans niet voor de gegevens-sets die gezamenlijk worden aangemaakt en beheerd. Dat de burgemeester wordt aangewezen als degene die aan het CBP moet melden, helpt niet voor de verantwoordelijkheid voor het beheer en de rechtmatige verwerking.

Bepaalde toezichthouders hebben de bevoegdheid toezichtgegevens te verstrekken aan andere toezichthouders. Een voorbeeld daarvan is de Opta. Op grond van artikel 24 van de Wet Opta is de Opta bevoegd om gegevens of inlichtingen omtrent een onderneming, die in het kader van het toezicht zijn verkregen, te verstrekken aan een andere toezichthoudende instantie. De wet bepaalt dat de geheimhouding van de gegevens of inlichtingen in voldoende mate moet zijn gewaarborgd, en dat voldoende is gewaarborgd dat de gegevens of inlichtingen niet zullen worden gebruikt voor een ander doel dan waarvoor deze worden verstrekt (doelbinding). Opta heeft op grond van deze bepaling een convenant gesloten met de KLPD ten behoeve van de aanpak van Malware.[91] Dit convenant valt eveneens onder artikel 20 Wpg. Het convenant bevat de doelstellingen van de informatie-uitwisseling en bevat de clausule dat uitwisseling geschiedt voor zover dit noodzakelijk is in het belang van en ten behoeve van de aan ieder der organisaties opgedragen taak.[92] Opta heeft eveneens een convenant gesloten met het Commissariaat voor de Media. Op het punt van de informatie-uitwisseling is het convenant vaag. Het bepaalt dat beide toezichthouders informatie uitwisselen over aangelegenheden die van belang

91 Informatie-uitwisselingsprotocol OPTA – KLPD/DNR, 30 augustus 2007. Raadpleegbaar via <www.opta.nl>.

92 Als doelstellingen worden genoemd: a) het ontwikkelen van kennis en expertise op het gebied van verspreiding van Malware; b) verdieping van de bestaande kennis en expertise op het gebied van verspreiding van Malware; c) het versterken van de informatiepositie op het gebied van de verspreiding en de aanpak van Malware; d) het reduceren van het aantal installaties van Malware in en vanuit Nederland; e) het versterken van de wederzijdse informatieposities door het uitwisselen van informatie met betrekking tot malware die de respectievelijke organisaties bij de uitvoering van hun taken vergaren; f) het gebruik van Onderzoeksinformatie afkomstig van OPTA in een strafrechtelijk onderzoek; g) het gebruik van Onderzoeksinformatie afkomstig van het KLPD/DNR in een bestuursrechtelijk onderzoek; h) het beperken van economische schade.

1912170 01165

kunnen zijn voor de uitoefening van hun wettelijke taken, voor zover wettelijke bepalingen daaraan niet in de weg staan. Daarnaast is de eis van doelbinding vastgelegd.

In hoofdstuk 3 wordt nog specifiek ingegaan op de convenanten die zijn gesloten op de domeinen die aan een nader onderzoek zijn onderworpen.

2.6 Geheimhoudingsplichten

Hoofdregel is dat overheidsinformatie openbaar is. Artikel 110 van de Grondwet legt vast dat de overheid bij de uitvoering van haar taak openbaarheid betracht volgens regels bij de wet te stellen. De Wet openbaarheid van bestuur (Wob) geeft uitvoering aan deze grondwetsbepaling. Die openbaarheid kan op twee manieren worden bereikt: door informatieverstrekking op verzoek (passieve openbaarheid, artikel 3 Wob) en door het uit eigen beweging verstrekken van informatie aan burgers (actieve openbaarheid, artikel 8 Wob). Om te voorkomen dat alle gegevens openbaar moeten worden gemaakt kent de Wob een stelsel van weigeringsgronden en beperkingen (artikel 10 en 11 Wob). Bij wet kan worden afgeweken van de eis van openbaarheid.

De wetgever heeft om verschillende redenen grenzen aan de openbaarheid gesteld. Deze zijn onder te verdelen in vier categorieën, te weten:

- de bescherming van private belangen (persoonlijke levenssfeer, bedrijfsgeheimen);
- de bescherming van publieke belangen (veiligheid van de staat);
- de bescherming van de bijzondere positie van bepaalde ambten (onschendbaarheid Koning);
- de zorg voor de goede werking van het openbaar bestuur (mogelijkheid van intern beraad, geheimhouding van een bepaalde werkwijze, het belang van inspectie, toezicht en controle door bestuursorganen).[93]

Binnen het kader van dit onderzoek zijn de bescherming van private belangen en de zorg voor de goede werking van het openbaar bestuur het belangrijkst. De bescherming van private belangen is overigens niet alleen een belang van burgers en bedrijven, maar eveneens van de overheid zelf. De belangen lopen parallel, daar waar bescherming bijdraagt aan het beeld van de betrouwbare overheid. Burgers en bedrijven zullen immers eerder geneigd zijn gegevens af te staan aan de overheid als zij erop kunnen vertrouwen dat deze goed worden bewaakt en niet zomaar aan de openbaarheid of aan derden worden prijsgegeven.[94] In die zin dient de bescherming van private belangen tevens het organisatiebelang en de goede werking van het openbaar bestuur. Anderzijds kan de bescherming van private belangen juist de goede werking van het openbaar bestuur belemmeren, als overheidsinstanties zich onderling beroepen op de geheimhoudingsplicht en om die reden niet tot uitwisseling van gegevens overgaan. Daarbij moet worden bedacht dat geheimhoudingsplichten in de regel in het leven zijn geroepen met het oog op een bepaald deelbelang van binnen het openbaar bestuur, zoals de richtige belastingheffing of de bewaking van de soliditeit van banken. De geheimhoudingsplicht heeft aldus meer kanten.

Artikel 2:5 Awb bepaalt dat een ieder die is betrokken bij de uitvoering van de taak van een bestuursorgaan en daarbij de beschikking krijgt over gegevens waarvan hij het vertrouwelijke karakter kent of redelijkerwijs moet vermoeden, is verplicht tot geheimhouding van die gegevens. De plicht geldt

93 Zie over de verhouding openbaarheid/geheimhouding A.M. Klingenberg, A. Logemann en S.A.J. Munneke Geheimhouding als juridische kwaliteitseis van primaire besluitvorming, in: M. Herweijer, A.T. Marseille, F.M. Noordam, H.B. Winter (red.), Alles in één keer goed. Juridische kwaliteit van bestuurlijke besluitvorming, Deventer: Kluwer 2005, p. 171-188.

94 Zie voor een extreme doorgetrokken belangenbehartiging door een korpsbeheerder in het kader van de Wpg Rb. Haarlem 16 mei 2012, *LJN*: BW7578.

1912170 01165

niet voor wie reeds uit hoofde van ambt, beroep of wettelijk voorschrift ter zake van die gegevens een geheimhoudingsplicht geldt. De plicht wijkt voor een wettelijk voorschrift dat tot mededeling verplicht, terwijl ook uit de taakuitoefening een noodzaak tot mededeling kan voortvloeien. Volgens de memorie van toelichting bij artikel 2:5 Awb hebben onder meer een vertrouwelijk karakter bedrijfs- en fabricagegegevens en gegevens die betrekking hebben op de persoonlijke levenssfeer. Als deze gegevens door een burger worden verstrekt onder vermelding dat zij een vertrouwelijk karakter hebben, is de betrokken ambtenaar gebonden aan de geheimhoudingsplicht.[95]

Het uitwisselen van gegevens kan problematisch zijn als één van de partners een strikte wettelijke geheimhoudingsplicht heeft, waarop weinig uitzonderingen zijn toegestaan. De Wpg en de Wjsg houden in beginsel een geheimhoudingsplicht in, waarop redelijk ruime uitzonderingen zijn gemaakt met het oog op bepaalde doelstellingen van algemeen belang.[96] Het uitgangspunt van de Wpg en de Wjsg is dat verstrekking van gegevens slechts gebeurt aan de personen en instanties die de wet noemt. In bepaalde gevallen kan een zwaarwegend algemeen belang rechtvaardigen dat incidenteel aan derden gegevens worden verstrekt. Verwezen wordt naar paragraaf 2.5.3, waar de verstrekkingenregimes op grond van beide wetten al zijn besproken. Hierna worden nog twee regimes besproken, te weten die van de Algemene wet inzake rijksbelastingen (Awr) en van de Wet op het financieel toezicht (Wft).

2.6.1 Geheimhoudingsplicht Belastingdienst

Ook de Awr gaat uit van de verplichting tot geheimhouding (artikel 67 Awr). De geheimhoudingsbepaling uit de Awr werpt een belangrijke drempel op als het gaat om het verstrekken van gegevens door de Belastingdienst. Artikel 67 Awr verplicht iedereen die betrokken is bij de uitvoering van de belastingwetgeving tot geheimhouding van in dat kader verkregen gegevens, zodat de Belastingdienst in beginsel geen informatie kan uitwisselen. De geheimhoudingsverplichting van de Belastingdienst wordt door de dienst van strategisch belang geacht.

'Gelet op de ruime wettelijke bevoegdheden die de Belastingdienst heeft om, soms privacy-gevoelige, informatie over belastingplichtigen te verzamelen, is de betekenis van de geheimhoudingsplicht groot. Naast het algemene belang van bescherming van persoonsgegevens gaat het om het belang dat personen niet van het verstrekken van gegevens aan de Belastingdienst moeten worden weerhouden door de vrees dat die gegevens voor andere doeleinden worden gebruikt dan voor een juiste en doelmatige uitvoering van de belastingwet', aldus de memorie van toelichting.[97]

In het tweede lid van artikel 67 is geregeld wanneer de geheimhoudingsplicht niet geldt. Dat is wanneer een wettelijke regeling tot bekendmaking verplicht. Voorbeelden van wettelijke regelingen die tot bekendmaking verplichten zijn de Comptabiliteitswet 2001 voor gegevensverstrekking aan de Algemene Rekenkamer (artikel 87), de Wwb voor gegevensverstrekking aan colleges van B&W (artikel 64) en de Wet structuur uitvoeringsorganisatie werk en inkomen voor gegevensverstrekking aan onder meer het Uitvoeringsinstituut werknemersverzekeringen en de Sociale verzekeringsbank (artikel 54).

Verder bestaat een uitzondering wanneer bij ministeriële regeling is bepaald dat bekendmaking noodzakelijk is ter vervulling van een publieke taak van een bestuursorgaan. De ministeriële regeling is de Uitvoeringsregeling Algemene wet inzake rijksbelastingen 1994 (Uitvoeringsregeling Awr). Met de

95 *Kamerstukken II*, 1988/89, 21 221, nr. 3, p. 57.
96 Zie artikel 7 Wbp en artikel 52 Wjsg.
97 *Kamerstukken II* 2005/06, 30 322, nr. 3 (MvT), p. 12.

1912170 01165

invoering van het huidige artikel 67 Awr in 2008 is als lijn neergezet dat nieuwe gevallen die in de uitvoeringsregeling worden opgenomen zoveel mogelijk worden beperkt en dat ernaar wordt gestreefd om gegevensverstrekking bij wettelijk voorschrift te gaan regelen. Hiermee wordt de betekenis van de Uitvoeringsregeling Awr teruggedrongen. Vanuit de historie echter is de lijst van ontheffingen in het kader van artikel 43c van de Uitvoeringsregeling Awr heel lang. Dit is op korte termijn niet te veranderen. Daarbij komt dat er gevallen zijn waarin wetgeving gegevensverstrekking moeilijk geregeld kan worden, bijvoorbeeld bij samenwerkingsverbanden tussen verschillende bestuursorganen. Voor dat soort situaties kan artikel 43c Uitvoeringsregeling Awr ook in de toekomst (tijdelijk) uitkomst bieden.

Op grond van artikel 55 zijn vrijwel alle overheidsorganen en de onder hen ressorterende organen en diensten (zowel van de rijksoverheid als van lagere overheden) verplicht om de gegevens en inlichtingen te verschaffen die hen ter uitvoering van de belastingwetgeving worden gevraagd. Dat geldt ook voor de politie. De Awr wordt met betrekking tot politiegegevens beschouwd als lex specialis, op grond waarvan de politie verplicht is gegevens te verschaffen.[98] Bij de parlementaire behandeling van artikel 55 is verder aandacht besteed aan de mogelijkheid dat overheden weigeren gegevens te verschaffen, omdat dit hun geheimhoudingsplicht zou doorkruisen. Volgens de minister zou dan in onderling overleg een oplossing moeten worden gevonden. Artikel 55, tweede lid, Awr biedt daarom de Minister van Financiën de mogelijkheid om ontheffing te verlenen.[99]

2.6.2 Geheimhoudingsplicht financieel toezicht

Anders ligt het met de Wft. Gegevensuitwisseling in het kader van financieel toezicht ligt gevoelig en wordt beperkt door een geheimhoudingsplicht op grond van artikel 1:89 Wft en volgende. Deze bepalingen zijn een implementatie van de bepalingen in de Herziene Bankenrichtlijn.[100] De toezichthouder (AFM of DNB) kan, in afwijking van artikel 1:89, eerste lid, vertrouwelijke gegevens of inlichtingen verkregen bij de uitvoering van zijn taak op grond van de Wft verstrekken aan de andere toezichthouder (DNB of AFM) of een toezichthoudende instantie in een andere lidstaat. Daarop zijn ook weer uitzonderingen, zoals wanneer de geheimhouding van de verstrekte gegevens niet voldoende is gewaarborgd. Op grond van artikel 1:91 kunnen AFM of DNB wel gegevens verschaffen aan een aantal met name genoemde functionarissen voor zover de gegevens of inlichtingen dienstig zijn voor de uitoefening van de eigen taak. Dit betreft de rechter-commissaris, bewindvoerder of curator wanneer zij (kort gezegd) optreden bij financiële ondernemingen op grond van de Faillissementswet. In bepaalde gevallen kunnen ook gegevens worden verstrekt aan opsporingsdiensten en het OM, maar deze bevoegdheid is restrictief geformuleerd. Daarnaast kunnen gegevens worden verstrekt aan de NZA, indien dienstig voor de taakuitoefening van deze autoriteit (artikel 1:93).

Als vertrouwelijke gegevens in de zin van de Wft worden aangemerkt: 'gegevens van financiële ondernemingen over de bedrijfsvoering, de liquiditeitspositie, de (maand)rapportages, gegevens over (potentiële) bestuurders daargelaten eventuele sancties die aan de natuurlijke persoon zijn opgelegd op basis van deze wet, (solvabiliteits)marges, gegevens over debiteuren, crediteuren of cliënten, gegevens van de afdeling R&D, plannen voor fusies of overnames en marketing/verkoopstrategieën. Het gaat derhalve om gegevens die van invloed kunnen zijn op de concurrentiepositie van de betreffende onderneming of een disproportionele inbreuk kunnen maken op de persoonlijke levenssfeer van betrokkene'.[101]

98 *Kamerstukken II* 1995/96, 23 470, nr. 14 (brief van de Staatssecretaris van Financiën).
99 *Kamerstukken II* 1990/91, 21 287, nr. 5, p. 4-5.
100 Zie onder andere de artikelen 44-52 van de Herziene Bankenrichtlijn (Richtlijn 2006/48/EG van het Europees Parlement en de Raad van 14 juni 2006 betreffende de toegang tot en de uitoefening van de werkzaamheden van kredietinstellingen (herschikking), *PbEU* 2006, L 177/1).
101 *Kamerstukken II* 2003/04, 29 708, nr. 3 (voetnoot 3 bij het antwoord van Minister De Jager van juni 2011).

1912170 01165

Deze strikte geheimhoudingsplicht is ter discussie gesteld door de Algemene Rekenkamer, die in het kader van een onderzoek naar het functioneren van DNB inzage wenste van dossiers van DNB.[102] De mate van gevoeligheid, en de contouren van de geheimhoudingsbeperking, worden duidelijk in de reactie van Minister De Jager op schriftelijke Kamervragen inzake het verzoek van de Algemene Rekenkamer, en inzake de voorlichting van de Raad van State in dezen.[103] Kort samengevat komt dit antwoord erop neer dat in de Wft sprake is van een gesloten systeem, en dat de Algemene Rekenkamer niet onder de uitzonderingen valt van artikel 1:90 Wft e.v. De minister citeert in dit verband de memorie van toelichting bij de Wft, die spreekt van 'een strikt geheimhoudingsregime met een stelsel van limitatief omschreven uitzonderingen op de geheimhouding'.[104] De minister herinnerde daarbij aan de reden voor dit strikte en gesloten geheimhoudingsregime, namelijk het ingrijpende karakter van informatieverplichtingen van financiële ondernemingen aan de toezichthouder: 'Gewaarborgd dient te zijn dat vertrouwelijke informatie vertrouwelijk blijft'.[105]

Samenwerking tussen de AFM en DNB vindt voorts plaats op grond van de Wet toezicht accountantsorganisaties (Wta), de Pensioenwet (Pw), de Wet verplichte beroepspensioenregeling (Wvb), en de Verordening ratingsbureaus. AFM en DNB hebben op 31 mei 2011 een convenant gesloten over het uitwisselen van gegevens (en coördinatie van beleid en regelgeving).[106] Dit convenant heeft tot doel om overlap te voorkomen op het raakvlak van het aan de AFM en DNB opgedragen toezicht, alsmede om de efficiency en doelgerichtheid van de uitvoering van het toezicht te bevorderen. De afspraken die in het convenant zijn gemaakt omtrent informatie-uitwisseling komen er volgens de toelichtende tekst op neer dat de toezichthouders elkaar gevraagd en ongevraagd de bij hen beschikbare informatie verstrekken over onder toezicht staande financiële ondernemingen, pensioenfondsen, accountantsorganisaties en ratingbureaus, voor zover dit nodig is voor de uitvoering van de toezichthoudende taak van de andere toezichthouder. Uitwisseling vindt plaats met inachtneming van de toepasselijke wettelijke geheimhoudingsbepalingen.

Als in de wet op basis waarvan de toezichthouders samenwerken geen speciale geheimhoudingsbepalingen zijn opgenomen, zoals de Wta, dan is de algemene geheimhoudingsbepaling uit de Awb van toepassing. Het convenant tussen AFM en DNB zegt daarover: 'Daarin is een geheimhoudingsbepaling opgenomen met in essentie dezelfde strekking als in de financiële toezichtwetten. Een bepaling voor uitwisseling ontbreekt, maar de geheimhoudingsbepaling stelt dat de vertrouwelijke informatie alleen mag worden gebruikt voor het doel waarvoor deze is verstrekt. Samenwerking in het kader van de uitoefening van de toezichttaak kan daaronder worden begrepen. Bij uitwisseling op grond van de Wta wordt dezelfde zorgvuldigheid in acht genomen als bij uitwisseling van gegevens op grond van de andere toezichtwetten. De voorwaarden voor uitwisseling zijn derhalve hetzelfde als in artikel 1:90 Wft en 205 Pw'.[107]

102 Kritisch over de absolute toepassing van de geheimhoudingsplicht zijn Ton Duijkersloot en Henk Kummeling, Parlement en geheime toezichtsinformatie, in: H.R.B.M. Kummeling e.a. (red.), *De samengestelde Besselink, Bruggen bouwen tussen nationaal, Europees en internationaal recht*, Oisterwijk: Wolf Legal Publishers 2012, p. 75-82.

103 *Kamerstukken II* 2010/11, 32 255, nr. 10.

104 *Kamerstukken II* 2003/04, 29 708, nr. 3.

105 *Kamerstukken II* 2003/04, 29 708, nr. 3. Opmerkelijk is dat ook de 'eigen' Belastingdienst, ondanks pogingen daartoe, vooralsnog geen informatie van de financiële toezichthouders krijgt.

106 Convenant van 31 mei 2011 tussen de Stichting Autoriteit Financiële Markten en De Nederlandsche Bank N.V. inzake samenwerking en coördinatie op het gebied van toezicht, regelgeving en beleid, (inter)nationaal overleg en andere taken met een gemeenschappelijk belang met betrekking tot de uitvoering van de Wta, Wft, Pw, Wvb en Verordening ratingbureaus, *Stcrt.* 2011, 10 191.

107 *Stcrt.* 2011, 10 191, p. 7, noot 10.

1912170 01165

2.7 Juridische vragen bij gegevensuitwisseling

De juridische vragen bij gegevensuitwisseling tussen toezichthouders betreffen de wettelijke beperkingen bij de uitwisseling van persoonsgegevens, in het bijzonder de bijzondere persoonsgegevens. De toepassing van artikel 9 Wbp kan veel vragen oproepen, omdat steeds moet worden onderzocht of de doeleinden waarmee de gegevens in eerste instantie zijn verzameld niet onverenigbaar zijn met de doeleinden waarvoor ze zullen worden gebruikt. Daarbij speelt een belangrijke rol in hoeverre de twee doeleinden voldoende verwantschap vertonen en in hoeverre sprake is van bijzondere c.q. gevoelige persoonsgegevens. Hoe gevoeliger het persoonsgegeven, hoe minder van het oorspronkelijke doel mag worden afgeweken. Daarbij komt dat bij de rechterlijke toetsing niet altijd duidelijk wordt wanneer de aard van de gegevens in de weg staat aan uitwisseling en wanneer sprake is van het ontbreken van voldoende verwantschap tussen de verwerkingsdoeleinden (zie hiervoor par. 2.4.3 en 2.5.1).

Wanneer gegevensuitwisseling plaatsvindt binnen vaste samenwerkingsverbanden gelden bovenstaande beperkingen evenzeer. Als wordt samengewerkt met politie en justitie is in de Wpg en de Wjsg al de door artikel 9 Wbp gevraagde afweging gemaakt. Dit betekent dat het voor bestuurlijke toezichthouders in het algemeen moeilijker zal zijn te bepalen of zij gegevens mogen doorgeven dan voor (bijzondere) opsporingsdiensten en het OM. Laatstgenoemde instanties hebben meer houvast aan de wet. Dit wil niet zeggen dat het voor degenen die moeten reageren op verzoeken om gegevensverstrekking alles steeds duidelijk is. De Wpg blijft vragen oproepen met betrekking tot de toepassing van bij voorbeeld artikel 18. Niet aanstonds zal duidelijk zijn of het gaat om gegevens die van belang zijn voor het toezicht op de naleving van de aangewezen wetten, terwijl de voorwaarden waaronder de gegevens kunnen worden verstrekt weliswaar zijn vastgelegd in convenanten, maar deze convenanten weinig concrete aanwijzingen geven. Een vergelijkbare observatie kan worden gemaakt met betrekking tot de toepassing van de artikelen 8a, 9 enl 39f Wjsg. Bij de toepassing in concrete gevallen moet immers in veel gevallen een inschatting worden gemaakt van de aard van de te verstrekken gegevens en een afweging worden gemaakt of doorgifte gerechtvaardigd is in het licht van de wettelijke bepalingen.

Afspraken in convenanten helpen om te voldoen aan de wettelijke voorwaarden van de Wpg en de Wbp. Zij maken duidelijk welke partijen samenwerken en op welke wijze zij beogen persoonsgegevens op een zorgvuldige manier te verwerken. Convenanten zijn weliswaar een veelgebruikte methode geworden om afspraken te maken over gegevensuitwisseling, de inhoud ervan leidt niet altijd tot meer duidelijkheid over de toelaatbaarheid van de verstrekking, terwijl het gevaar bestaat dat deelnemende partijen het convenant zien als garantie dat binnen de wettelijke beperkingen wordt gebleven.

Geheimhoudingsplichten kunnen een obstakel vormen voor gegevensuitwisseling. In de in dit hoofdstuk besproken regelingen zijn meer of minder uitzonderingen geformuleerd op de plicht tot geheimhouding. Geheimhouders kunnen zich rekkelijk of precies (zoals DNB en AFM) tonen en daarmee de geheimhoudingsplicht strategisch inzetten. Over het algemeen bieden de wettelijke kaders ruimte om een samenwerking aan te gaan en op basis daarvan gegevens uit te wisselen. De Belastingdienst verzamelt veel gegevens en is daarmee een aantrekkelijke partner voor gegevensuitwisseling. De Uitvoeringsregeling Awr kent weliswaar een limitatieve opsomming van partners met wie kan worden uitgewisseld, maar de lijst is zeer uitgebreid.

In hoofdstuk 3 wordt de praktijk van gegevensuitwisseling onderzocht op een drietal beleidsdomeinen.

1912170 01165

3. Inventarisatie en weging van belangen

3.1 Methoden van onderzoek

Om de belangen die spelen rond gegevensuitwisseling tussen toezichthouders en de weging van die belangen te inventariseren is gekozen voor een aanpak door middel van casus, bestudering van de relevante stukken, gesprekken met ervaringsdeskundigen, een expertmeeting en een enquête ten behoeve van de Multicriteria-analyse (MCA). In de volgende subparagrafen wordt de gehanteerde methode besproken. In de paragrafen 3.2 tot met 3.4 worden de uitkomsten van de verschillende onderzoeksmethoden beschreven, waarna in paragraaf 3.5 een overzicht van de onderzoeksesultaten volgt.

3.1.1 Casus

In verband met de beperkte opzet van het onderzoek is gezocht naar casus die voldoende representatief zijn voor de verschillende vormen van samenwerking, dat wil zeggen samenwerking tussen toezichthouders onderling, structurele samenwerking tussen toezichthouders en opsporingsdiensten (met convenant) en ad hoc samenwerking tussen toezichthouders en opsporingsdiensten. Daarbij is eveneens gekeken naar bestaande netwerken van de begeleidingscommissie en de onderzoekers. Op basis van de hiervoor beschreven uitgangspunten zijn drie casus geselecteerd en in overleg met de begeleidingscommissie vastgesteld. De onderzochte casus hebben voldoende verscheidenheid om de relevante belangen betrokken bij de uitwisseling van toezichtgegevens te detecteren en te wegen. De drie casus zijn zo gekozen dat voldoende spreiding in het toezicht- en opsporingveld wordt verkregen en dat de in de opdracht vervatte problematiek voldoende aan bod komt.

De casus worden meer gedetailleerd beschreven en besproken in paragraaf 3.2. Hier volgt ter wille van de leesbaarheid een korte samenvatting. De eerste casus betreft het toezicht op het taxibedrijf in Amsterdam en de aanpak van ongewenste situaties binnen de Amsterdamse taxiwereld. Binnen deze casus speelt een aantal voor het onderzoek relevante belangenverhoudingen tussen de verschillende betrokken bestuursorganen en toezichthouders, tussen de gemeente en de politie en tussen de bestuurlijke en de

1912170 01165

strafrechtelijke sfeer. De tweede casus betreft de samenwerking met onder meer het oog op de naleving van bepalingen inzake de belastingheffing. Deze aanpak vindt plaats binnen de RIEC's en de Landelijke Stuurgroep Interventieteams (LSI), waarin de bestuurlijke en strafrechtelijke handhavers samenwerken binnen de kaders van een convenant. De derde casus heeft als thema handhaving van regels met betrekking tot vuurwerk. Regulering van invoer, vervoer en opslag van vuurwerk gebeurt op basis van de Wet milieubeheer. Binnen deze vuurwerkcasus is het startpunt de strafrechtelijke aanpak van illegaal vuurwerk, van waaruit naar de samenwerking met het bestuurlijke veld is gekeken. Daarbij spelen met name de belangen van gegevensoverdracht in het kader van een gestart opsporingsonderzoek.

Voor het bestuderen van de geselecteerde casus is een gecombineerde methode gehanteerd. Om te beginnen is op grond van eigen ervaring van de onderzoekers en op grond van documentatie en literatuur tentatief een inventarisatie gemaakt van de mogelijke belangen die spelen bij de uitwisseling van toezichtgegevens. Deze inventarisatie is afgestemd met de begeleidingscommissie. Vervolgens zijn gesprekken gevoerd met ervaringsdeskundigen binnen het veld van de casus, met als doel te verifiëren of er belangen ontbraken en inzicht te verwerven in de feitelijk werkwijze binnen het samenwerkingsverband. Vervolgens is een enquête opgesteld voor drie doelgroepen, namelijk uitvoerings- en toezichtorganisaties, opsporingsorganisaties en vertegenwoordigers van hen die onder toezicht staan. Deze enquête is beproefd binnen het onderzoeksteam en afgestemd met de begeleidingscommissie. De aldus aangepaste enquête is voorgelegd aan een bredere kring van betrokkenen, deels betrokken bij de casus en deels daarbuiten. Daarnaast is een expertmeeting georganiseerd waarin de reeds gedetecteerde belangen zijn besproken en de gelegenheid bestond deze zo nodig aan te vullen en toe te lichten. Deze expertmeeting was verder gericht op een nadere analyse van de problematiek en op het verkennen van een mogelijke oplossingsrichting, meer in het bijzonder de mogelijkheden voor een nieuwe regeling.

3.1.2 Enquête

Zoals hiervoor aangegeven is de tentatief opgestelde lijst van mogelijke belangen bij de uitwisseling van toezichtgegevens voorafgaand aan het opstellen van de enquête als basis gebruikt voor gesprekken met een aantal ervaringsdeskundigen op het gebied van gegevensuitwisseling.[108] Om zoveel mogelijk nog niet gedetecteerde belangen boven tafel te krijgen werden ten aanzien van de belangen uitsluitend open vragen gesteld. Bij de beweegredenen om al dan niet tot gegevensverstrekking over te gaan kwamen in die gesprekken zowel de beweegredenen van de eigen organisatie van de geïnterviewde aan de orde als ook die van de andere betrokken partijen. Daarbij is behalve naar de juridische belemmeringen ook gekeken naar praktische, technische en administratieve belemmeringen die uitwisseling in de weg kunnen staan en de belangen die daarbij een rol spelen. De inventarisatie van belangen in de gesprekken heeft geleid tot een scherpere vraagstelling in de enquête, bijvoorbeeld op het snijvlak van uitvoering en opsporing.

3.1.2.1 Uitvoering enquête

Met de reeds gedetecteerde belangen als basis en de resultaten uit de gesprekken als toevoeging en verdieping is een aantal enquêtevragen geformuleerd. Deze vragen zijn, in op de doelgroep toegesneden vorm, via een internetenquête gesteld aan drie doelgroepen met als doel te komen tot een MCA. Het ging daarbij uitdrukkelijk om een kwalitatief onderzoek, waarbij de rangorde van belangen en het detecteren van nieuwe belangen voorop stonden. Zowel het aantal deelnemers als de selectie ervan laten geen kwantitatieve conclusies toe.

De eerste doelgroep, uitvoerings- en toezichtorganisaties, zijn de bestuurlijke deelnemers aan de uitwisseling van gegevens. Daarbij gaat het binnen de gekozen casus om de gemeente Amsterdam, en de

108 Het ging hierbij om personen die veel met gegevensuitwisseling te maken hebben. Zij zijn niet als vertegenwoordiger van hun organisatie aangesproken, maar als kenner van dit specifieke terrein.

1912170 01165

Belastingdienst. De tweede doelgroep betreft de opsporingsorganisaties: de politie, de FIOD en het OM. De derde groep betreft de professionele vertegenwoordigers van burgers en bedrijven die in dit geval de belangen zowel vanuit het perspectief van de klant, als vanuit hun eigen positie moesten beoordelen. Gelet op de geselecteerde casus betrof het met name advocaten en belastingadviseurs. In totaal zijn een zestal gesprekken gevoerd en is in totaal aan 27 contactpersonen gevraagd de enquête in te vullen, waarbij zij tevens zijn verzocht de enquête steeds door drie personen te laten invullen. In totaal is de enquête 32 maal ingevuld. Gebleken is dat een aantal respondenten uiteindelijk afhaakte en dat het merendeel van de respondenten, ondanks telefonisch contact en mondelinge toezegging vooraf toch niet in staat bleken meer nieuwe respondenten te genereren. Niettemin zijn per categorie voldoende enquêtes ingevuld om de belangrijkste belangen per categorie kwalitatief te kunnen duiden. Een integrale kwantitatieve ranking van gepercipieerde belangen over alle categorieën is op basis van deze in omvang beperkte enquête niet mogelijk, maar was ook niet voorzien.

In de enquête is aan *de bestuurlijke toezichthouders c.q. uitvoeringsorganisaties* gevraagd een rangorde aan te brengen tussen een aantal belangen. Zodoende is de onderlinge waardering van die belangen gepeild. Bij deze enquête is een aantal vragen gesteld, te beantwoorden vanuit verschillende invalshoeken. Deze invalshoeken waren om te beginnen die van ontvanger van toezichtgegevens en van verstrekker van toezichtgegevens. Dit onderscheid kwam voort uit de interviews waarbij bleek dat de afwegingen bij verstrekking en verkrijging kunnen verschillen, bijvoorbeeld omdat voor de verstrekker de kosten van de benodigde inspanningen een belangrijker rol spelen dan bij de ontvanger. Verder is onderscheid gemaakt tussen gegevensuitwisseling binnen een geheel bestuurlijk kader, en gegevensuitwisseling waarbij een opsporingsorganisatie is betrokken. In dat laatste geval is de uitvoeringsinstantie gevraagd zowel belangen die spelen bij de levering aan die opsporingsinstantie, als belangen die spelen bij de ontvangst van opsporingsgegevens van een opsporingsorganisatie als uitgangspunt te nemen bij het rangschikken van de belangen. Ten slotte is bij elke categorie van belangen de mogelijkheid geboden een nog niet gesignaleerd belang in tekst toe te voegen en te betrekken in de rangschikking. Tevens zijn per categorie vragen gesteld over de kwaliteit van de geleverde gegevens in de vorm van score-vragen.

Bij de enquête voor de *opsporingsorganisaties* is gevraagd naar de gesignaleerde belangen vanuit de posities als ontvanger of als leverancier van gegevens. Het onderscheid tussen bestuursrechtelijk toezicht en opsporing is niet gemaakt aangezien het bij deze categorie altijd om opsporing gaat. Wel is ook hier bij elke categorie van belangen de mogelijkheid geboden een nog niet gesignaleerd belang in tekst toe te voegen en te betrekken in de rangschikking, en is gevraagd naar de kwaliteit van de geleverde gegevens in de vorm van score-vragen.

Bij de enquête onder *vertegenwoordigers van burgers en bedrijven* waarvan gegevens worden uitgewisseld in het kader van toezicht of opsporing werd de vertegenwoordigers gevraagd om zowel vanuit het belang van hun cliënt, als vanuit hun eigen belang als vertegenwoordiger te rangschikken. Daarnaast is ook hier onderscheid gemaakt tussen de uitwisseling in het kader van bestuurlijk toezicht en die in het kader van de opsporing. Over de kwaliteit van de uitgewisselde gegevens zijn geen vragen gesteld aan de vertegenwoordigers, omdat zij deze gegevens veelal in verwerkte vorm te zien krijgen.

3.1.2.2 Vragen

De deelnemers werd gevraagd om de op het internetformulier aangegeven belangen te rangschikken op volgorde van belangrijkheid, steeds vanuit het bij de vraag aangegeven perspectief. De vragen hadden betrekking op enerzijds de juridische noties, zoals doelbinding, geheimhouding en de privacy van zowel het subject als mogelijke derden, en anderzijds op meer praktische noties.

1912170 01165

Deze praktische noties zijn kortweg in te delen in kosten en baten. Bij kosten moest worden gedacht niet alleen aan financiële kosten, maar ook aan de inspanning die nodig is voor de verstrekking van de toezichtgegevens. De inzet van personeel en de technische en/of organisatorische aanpassingen die moeten worden gemaakt om de gevraagde gegevens te kunnen leveren horen daar ook onder. Ook de gepercipieerde risico's zouden als kosten kunnen worden aangemerkt. Vanuit de deelnemers werd bijvoorbeeld het niet of niet goed ontvangen van de gegevens als risico aangemerkt.

Bij de baten spelen zowel de baten voor de ontvangende organisatie als die voor de leverende organisatie. Bij de laatste vraag was een tekstruimte opgenomen waarbij met het gemiste belang kon invullen, en de gewenste plaats in de rangorde kon geven.

De volledige vragenlijsten en resultaten zijn opgenomen in bijlage 7.2. Een samenvatting van de resultaten is opgenomen in paragraaf 3.4.

3.1.3 Expertmeeting

Omdat de interactie tussen de verschillende doelgroepen bij de oriënterende gesprekken en de enquête feitelijk ontbrak is tevens gekozen voor een expertmeeting, gehouden op 29 februari 2012. Bij de bijeenkomst waren vertegenwoordigers die betrokken zijn bij de casus, de onderzoekers, het CBP en een lid van de begeleidingsgroep aanwezig.[109] Op deze manier was ook interactie tussen de doelgroepen mogelijk. Beide onderdelen van het onderzoek, het detecteren van belangen en een mogelijke wettelijke regeling voor de uitwisseling van toetsingsgegevens in de Awb, zijn besproken.[110] De vraagpunten die in de expertmeeting zijn geagendeerd waren:

- Welke knelpunten zijn er bij gegevensuitwisseling?
- Is de juridische basis voor uitwisseling voldoende verzekerd?
- Is er behoefte aan een algemene wettelijke regeling?
- Hoe zou zo'n algemene regeling eruit moeten zien?

3.2 Casusbeschrijving en uitkomsten

De resultaten uit het onderzoek naar de belangen die spelen bij de uitwisseling van toezichtgegevens en de weging van die belangen zijn in de achtereenvolgende fasen van het onderzoek op verschillende manieren gevonden. In het vooronderzoek is een opsomming gemaakt van mogelijke belangen en mogelijke belanghebbenden. Vervolgens zijn in de gesprekken met de direct bij de onderscheiden casus betrokkenen nieuwe belangen naar voren gekomen en is ook kleuring gegeven aan de samenwerking tussen uitvoerings- en toezichtinstanties op basis van convenanten. Ook is vanuit de praktijk licht geworpen op de wenselijkheid van een algemene wettelijke regeling voor de uitwisseling van toezicht-gegevens. Hierna volgt een beschrijving van de drie casus, gevolgd door de knelpunten die de betrokkenen stellen te ervaren.

3.2.1 Casus Taxivervoer

De problematiek waarmee de taximarkt in de grote steden (en met name in Amsterdam) geconfronteerd wordt, is dat de kwaliteit van de dienstverlening op de zogenaamde 'opstapmarkt' en de service die er

109 Een lijst met deelnemers aan de expertmeeting van 29 februari 2012 is opgenomen in bijlage 7.3.
110 Een verslag van de expertmeeting is beschikbaar.

1912170 01165

geleverd wordt, vaak te wensen overlaat. Taxichauffeurs weigeren herhaaldelijk korte ritten, rijden om en gedragen zich soms intimiderend.

Om deze problemen het hoofd te kunnen bieden is in de Wet Personenvervoer 2000 de mogelijkheid opgenomen dat enkele grote gemeenten (in de praktijk: de grootste) het gebruik van de gemeentelijke openbare weg kunnen voorbehouden aan chauffeurs die deel uitmaken van een organisatorisch verband. Aan de bij dergelijke verbanden aangesloten chauffeurs kunnen dan – in aanvulling op de landelijke chauffeurspas – gemeentelijke vergunningen worden verleend.

In Amsterdam wordt momenteel gewerkt aan het opzetten van zogenaamde 'Toegelaten Taxi-organisaties' (TTO's). De bedoeling is dat deze organisaties de bij hen aangesloten chauffeurs controleren en aldus bijdragen aan de handhaving van de taxiregels. De gemeente kan zich dan in het kader van de handhaving beperken tot het beslissen omtrent het toelaten van TTO's en het toezien daarop via audits en tot meer steekproefsgewijze controles.

3.2.1.1 Juridisch kader inzake de gegevensuitwisseling

In de Wet Personenvervoer 2000 is geen bepaling te vinden die de gegevensuitwisseling tussen de verschillende bij de taxiproblematiek betrokken overheids- en andere partijen mogelijk maakt of daartoe verplicht of daaraan normen stelt. In de visie van de gemeente ontbreken daardoor de concrete middelen om de toegekende bevoegdheden goed te kunnen uitoefenen.

3.2.1.2 Samenwerking met gegevensverstrekkers en -ontvangers Taxiconvenant G4

In 2008 hebben de staatssecretaris van Verkeer en Waterstaat en de gemeenten Amsterdam, Rotterdam, Den Haag en Utrecht een convenant gesloten inzake de aanpak van de problematiek met betrekking tot het taxivervoer.[111] In dit convenant is bepaald dat zogenaamde handhavingsplatforms zullen worden ingesteld in de vier steden; binnen deze platforms zullen handhavingsinstanties periodiek overleg voeren. Een van de doelen van de platforms is de realisatie van een onderlinge uitwisseling van informatie conform de geldende (privacy)regels. In het convenant is hiervan geen nadere uitwerking opgenomen.

Taxi-database

In de Hoofdlijnennotitie Taxibeleid[112] schrijft de gemeente Amsterdam dat een zogenaamd Taxi-informatiesysteem ontwikkeld zal worden. Dit systeem heeft tot doel om in samenwerking met de handhavingspartners de taximarkt goed in beeld te brengen. Een van de resultaten die met het systeem bereikt moet worden is het doorbreken van de anonimiteit van chauffeurs, opdat er bij incidenten snel kan worden ingegrepen. Tevens wordt met het systeem beoogd om de informatie op meta-niveau te kunnen analyseren om de handhaving efficiënt in te kunnen zetten.

In de Uitwerking Hoofdlijnenplan Taxi[113] van december 2011 wordt dit plan verder uitgewerkt. Onder de naam Taxi-database beoogt de gemeente een kerndatabase op te stellen met daarin de belangrijkste gegevens van TTO's en chauffeurs. Aan deze database zullen in elk geval de data gekoppeld worden die bij de gemeente zelf binnenkomen, waaronder klachten en waarnemingen van toezichthouders. Als een van de risico's van het taxibeleid als geheel, benoemt de gemeente het risico van (wettelijke) beperkingen aan gegevensdeling en de opbouw van de database.[114] De gemeente stelt dit risico te willen beperken door vooral eigen gegevens te gebruiken, in combinatie met gegevens van huidige, bekende partners. Met deze

111 G4 Taxiconvenant 20 maart 2008, *Kamerstukken II* 2007/08, 25 910, nr. 84.
112 Hoofdlijnen Taxiplan Amsterdam, 2011. Raadpleegbaar via de website van de gemeente Amsterdam: <www.amsterdam.nl>
113 Toelating en toezicht op de Amsterdamse Taximarkt: nieuw samenspel tussen klanten, branche, gemeente en partners, Uitwerking Hoofdlijnenplan Taxi, 11e versie, 8 december 2011. Raadpleegbaar via de website van de gemeente Amsterdam: <www.amsterdam.nl>
114 Ibid., p. 17.

1912170 01165

partners zullen duidelijke doelen moeten worden afgesproken over het delen van informatie, aldus de gemeente.

Samenwerkingspartners
Voor de handhaving van de taxiregels en -normen is de gemeente Amsterdam mede afhankelijk van informatie van de Inspectie Verkeer en Waterstaat (IVW) die verantwoordelijk is voor de verlening van de landelijke chauffeurspas (vergunning), het OM, de politie, de Belastingdienst en het Landelijk Klachtenmeldpunt, maar ook van gemeentelijke diensten zoals de Dienst Stadstoezicht en de Dienst Persoons- en Geo-informatie (DPG). Met het oog op samenwerking en gegevensuitwisseling zijn verschillende convenanten afgesloten en moeten andere nog worden afgesloten. Hoewel de gemeente graag gegevens over chauffeurs van het CBR zou willen krijgen, blijkt dat in de praktijk niet mogelijk. Het CBR verstrekt deze gegevens niet. Ook het Landelijk Klachtenmeldpunt is terughoudend met het verstrekken van gegevens over ingediende klachten. Daarnaast moeten afspraken worden gemaakt met de TTO's. Er bestaat geen specifieke regelgeving op basis waarvan de gemeente de bevoegdheid heeft gegevens bij de TTO's op te vragen. Een convenant moet uitkomst brengen, waarbij de Wbp als kader geldt.

3.2.1.3 Soorten gegevens
De IVW beschikt in het kader van het verlenen van de landelijke chauffeurspas over de nodige gegevens omtrent het gedrag van individuele taxichauffeurs, mede doordat daarbij een verklaring omtrent gedrag (VOG) vereist is. De Taxi-database van de gemeente zal mogelijk worden aangevuld met periodieke gegevens van het IVW over de risicoprofielen van TTO's en meldingen dat een chauffeur een nieuwe VOG moet aanvragen.[115] Deze gegevens omtrent het gedrag zijn essentieel voor de gemeentelijke handhaving. Ook strafrechtelijke gegevens over de bij een TTO aangesloten taxichauffeurs van politie en OM zijn nodig voor een goede handhaving. Graag zou de gemeente ook beschikken over gegevens van het CBR met betrekking tot de geschiktheid van chauffeurs (en maatregelen die in het kader daarvan zijn opgelegd), maar zoals reeds aangegeven worden deze gegevens niet aan de gemeente verstrekt. De gegevens van het landelijk klachtmeldpunt betreffen klachten van cliënten.

Aangezien de TTO's (mede) belast zijn met de handhaving, dienen ze over de nodige gegevens met betrekking tot het gedrag van de bij hen aangesloten taxichauffeurs te beschikken. De gemeente gaat er vanuit dat de TTO's hun chauffeurs zelf scherp houden en dwingen tot het verstrekken van de benodigde gegevens over overtredingen etc. (bijvoorbeeld door te dreigen met verlies van het lidmaatschap van de organisatie). Toch kan het nodig zijn dat de gemeente de TTO's van informatie voorzien die ze zelf hebben of via andere instanties verkregen hebben. De gemeente wil echter niet zonder meer de bij haar binnenkomende gegevens over chauffeurs aan TTO's verstrekken. Of en in hoeverre gegevens verstrekt worden hangt mede af van de privacygevoeligheid van de gegevens en van de risico's van het verspreiden van gevoelige gegevens.

3.2.1.4 Ervaringen en knelpunten
De Wet Personenvervoer 2000 geeft geen wettelijke basis voor gegevensuitwisseling. Dit wordt in de gemeente als een gemis ervaren, omdat hierdoor een taak zonder bijbehorende bevoegdheid bij de gemeente wordt gelegd. Daardoor moeten de gewenste gegevens op basis van convenanten of ad hoc worden uitgewisseld. Met iedere partner moet op die manier een convenant worden gesloten of een afspraak worden gemaakt. Respondenten van de gemeente geven aan dat in de tot dan toe afgesloten convenanten vaak weinig meer staat dan dat uitwisseling mogelijk is. Van een duidelijke normering van de gegevensverstrekking of van de doelbinding is weinig sprake. Dat wreekt zich volgens de respondenten

115 Ibid., p. 13.

1912170 01165

regelmatig bij de daadwerkelijk gegevensuitwisseling, omdat men dan bang is bepaalde gegevens te verstrekken zonder te weten of dat gelet op met name de Wbp wel is toegestaan. Vooral als degene die de gegevens zou moeten verstrekken de reikwijdte van de privacybescherming niet goed kent, komt het vaak voor dat de gegevens niet of slechts in beperkte mate verstrekt worden uit angst voor het schenden van privacy-bepalingen. Ook komt het voor dat men zich verschuilt achter de privacybescherming om gegevens niet te hoeven delen of dat men überhaupt geen gegevens wil uitwisselen. Ten slotte komt het voor dat gegevens afkomstig zijn van een instantie die deze gegevens weer van een andere instantie verkregen heeft. Het probleem hiervan kan zijn dat de gegevens bewerkt zijn en daardoor gefilterd.

3.2.1.5 Behoefte aan een wettelijke regeling?

Vanuit de gemeente Amsterdam bestaat zeker behoefte aan een wettelijke regeling omtrent de uitwisseling van gegevens. Zo'n wettelijke regeling kan enerzijds fungeren als legitimering van de gegevensuitwisseling, zodat mogelijke angst voor uitwisseling wordt weggenomen, anderzijds als verplichting tot uitwisselen, zodat onwillige partijen gedwongen kunnen worden gegevens uit te wisselen. Wel wordt benadrukt dat de doelbinding duidelijk in de wettelijke regeling dient te zijn opgenomen. Het is van groot belang dat volstrekt helder is waarom bepaalde informatie wordt uitgewisseld. Het ligt niet voor de hand dat een algemene regeling omtrent gegevensuitwisseling in de Awb wordt opgenomen. Eerder ligt het voor de hand een regeling in de Wet personenvervoer 2000 op te nemen of in een op deze wet gebaseerde uitvoeringsregeling (AMvB of ministeriële regeling).

3.2.2 Casus Gegevensuitwisseling samenwerkend toezicht belastingheffing

Een van de casus die binnen het kader van dit onderzoek nader in kaart wordt gebracht is de belastingheffing. Voor dit onderzoek is met name het toezicht op de naleving van de regelgeving van belang. Hoewel de Belastingdienst geen toezichthouder is in de zin van artikel 5:11 Awb ligt het toezicht op de naleving van de fiscale wetgeving wel primair bij de Belastingdienst. Bij het toezicht maakt de Belastingdienst mede gebruik van gegevens van andere uitvoeringsinstanties en toezichthouders en werkt zij daarmee samen in verschillende samenwerkingsverbanden. In deze samenwerkingsverbanden levert de Belastingdienst gegevens, waaronder toezichtgegevens, aan de partners binnen het samenwerkingsverband op grond van de afspraken in de desbetreffende convenanten.

Binnen het kader van het onderzoek is met name om praktische redenen in eerste instantie gesproken met betrokkenen van de Belastingdienst. Daarbij was de verwachting dat hiermee voldoende aanvullende input voor de enquête ten behoeve van de MCA zou kunnen worden verkregen. Met deze enquête worden ook de andere deelnemers van het RIEC en de LSI bij het onderzoek betrokken.

3.2.2.1 Juridisch kader inzake gegevensuitwisseling

In artikel 47 Awr is de toegang tot gegevens van de Belastingdienst geregeld. Daarin zijn tevens de informatieplicht in internationale verhoudingen (artikel 47a) en de identificatieplicht (artikel 47b) geregeld. In artikel 53 is de levering van gegevens van derden aan de dienst voorgeschreven, en in artikel 55 de levering van gegevens door overheidsinstanties. Ten aanzien van het verstrekken van gegevens kent de Awr een geheimhoudingsplicht voor een ieder die belastinggegevens onder zich heeft (artikel 67). In hoofdstuk 2 werden deze geheimhoudingsplicht en de uitzonderingen daarop op basis van de Uitvoeringsregeling Awr al besproken. Het uitzonderingsregime op basis van de Uitvoeringsregeling Awr maakt mede mogelijk dat de Belastingdienst participeert in samenwerkingsverbanden zoals de RIEC's en LSI.

3.2.2.2 Samenwerking gegevensverstrekkers en -ontvangers

De Belastingdienst beheert enkele van de grootste databanken met financiële gegevens van personen en bedrijven in ons land. Daarnaast werkt de Belastingdienst zowel op het gebied van het vergaren van

1912170 01165

gegevens als bij het uitwisselen samen met vele andere toezichthouders en opsporingsdiensten. Deze samenwerking vindt veelal plaats op basis van samenwerkingsconvenanten. Het gaat om de samenwerking in de RIEC's en binnen de LSI. Hierin werken Belastingdienst, SIOD, Gemeenten, OM, politie en andere diensten samen in het kader van bestrijding van georganiseerde misdaad en fraude.

Als het gaat om samenwerking bij de handhaving, dan zijn de RIEC's een goed voorbeeld van een bestuurlijke aanpak, hoewel later uitgebreid naar de opsporingskant met het toetreden van politie en het OM. Een groot voordeel van de RIEC's is de totstandkoming van een bestuurlijk netwerk, waardoor de communicatie over mogelijke belemmeringen in de gegevensuitwisseling laagdrempelig is. De RIEC's opereren regionaal onder voorzitterschap van de gemeenten. De Belastingdienst ondersteunt de RIEC's en streeft daarbij naar duidelijkheid over de uitwisseling van gegevens op landelijk niveau. Een aandachtspunt is dat de kleinere gemeenten vaak door een van de grotere gemeenten uit de regio worden vertegenwoordigd, en zich op operationeel niveau niet altijd aan het convenant gebonden achten. Dit leidt ertoe dat gemeenten op verschillende manieren omgaan met de uitwisseling van gegevens.

De verstrekking van gegevens door de Belastingdienst is in dit samenwerkingsverband in de praktijk geen probleem, aangezien een convenant wordt gesloten tussen de deelnemende partijen. Wel vindt verstrekking uitsluitend plaats aan overheidsinstanties of andere organisaties met een publieke taak. In dat geval is voorzien in een ontheffing voor de verstrekking van concrete subject informatie door de Belastingdienst op grond van artikel 43c van de Uitvoeringsregeling Awr.

In voornoemd artikel 43c is een ruime ontheffingsregeling opgenomen met een reeks van specifieke ontheffingen op grond waarvan aan tal van overheden gegevens mogen worden doorgegeven. Een aantal daarvan krijgt gegevens ten behoeve van de toezichthoudende taak, zoals de NVWA, de Arbeidsinspectie, DNB, AFM, UWV etc. In bepaalde gevallen stelt de Uitvoeringsregeling Awr als voorwaarde dat wordt samengewerkt met een bepaald doel, zoals fraudebestrijding of de bestrijding van witwassen. Deze samenwerking wordt als gezegd vastgelegd in een convenant tussen partijen, waarbij de voorwaarden voor de uitwisseling evenals de betrokken gegevensset nader kunnen worden uitgewerkt. Een voorbeeld van een dergelijk convenant is het in hoofdstuk 2 genoemde Bestuurlijk Akkoord Geïntegreerde Decentrale Aanpak Gereorganiseerde Misdaad en de Regionale Akkoorden die daarop zijn gebaseerd. Deze vormen de basis voor een RIEC. Samenwerkende partners zijn politie, OM, Belastingdienst en een of meer gemeenten, UWV en bijzondere opsporingsdiensten, zoals FIOD-ECD en SIOD en de Koninklijke marechaussee.

3.2.2.3 Soorten gegevens

In de convenanten moet zoveel mogelijk worden vastgelegd welke gegevens kunnen worden uitgewisseld. In het convenant binnen het RIEC moet bijvoorbeeld worden vastgelegd welke gegevenssets beschikbaar zijn ten behoeve van welke vorm van georganiseerde misdaad. Deze gegevenssets omvatten gewone en bijzondere persoonsgegevens, zoals strafrechtelijke gegevens.

3.2.2.4 Doelbinding

De regels voor doelbinding en het verbod op het doorleveren van gegevens zijn binnen de samenwerking onverkort van kracht. In de hiervoor genoemde Regionale Akkoorden wordt bepaald voor welke doeleinden zal worden samengewerkt. Deze doeleinden zijn soms tamelijk ruim geformuleerd, zoals 'het overheidsoptreden op basis van fiscale wetten doeltreffender maken'.[116] In andere gevallen, zoals bij de vorming van RIEC's, zijn ze concreter geformuleerd, zoals ter bestrijding van mensenhandel, georganiseerde hennepteelt en fraude in de vastgoedsector.

116 Ontleend aan het Convenant integrale overheidshandhaving Leeuwarden. Raadpleegbaar via de website van het Centrum Criminaliteitspreventie Veiligheid: <www.hetccv.nl>.

1912170 01165

3.2.2.5 Geheimhouding en verstrekking aan derden

De Regionale Akkoorden bepalen dat partijen gegevens niet aan derden verstrekken, tenzij betrokkene toestemming heeft gegeven en met inachtneming van het in het Akkoord omschreven juridisch kader. In welke situaties zich dat voordoet wordt in het convenant niet in concreto aangegeven. Het juridisch kader waarnaar wordt verwezen zijn de Wbp, de Wpg en de Wjsg. Verder dient het Akkoord te bepalen dat medewerkers van partijen een geheimhoudingsplicht moet worden opgelegd.

3.2.2.6 Ervaringen en knelpunten

In het kader van de casus belastingheffing hebben wij ons met name gericht op de toezichtkant van de Belastingdienst en in het bijzonder de deelname van de Belastingdienst in de diverse hiervoor besproken interdisciplinaire samenwerkingsverbanden: de RIEC's en de LSI. De verschillende toezichthoudende diensten, politie en OM werken hierin samen bij het bestrijden van fraude, en bij het RIEC in het bijzonder van georganiseerde misdaad. De Belastingdienst kijkt bij de verstrekking van gegevens in eerste instantie naar de juridische mogelijkheden, namelijk of de gevraagde gegevens en de geadresseerde binnen het kader van artikel 43c van de Uitvoeringsregeling Awr vallen. Mede om die reden is de Belastingdienst nog voorzichtig met de deelname in grootschaliger uitwisselingsmogelijkheden zoals bijvoorbeeld via Inspectieview. Met dit instrument dat door het Ministerie van SZW is ontwikkeld, kunnen inspecties elkaars toezichtgegevens inzien en zo de inspecties beter op elkaar afstemmen.

Daarnaast wordt door de Belastingdienst ook een doelmatigheidsafweging gemaakt, waarbij onder meer elementen als kosten van inwilliging van het verzoek, mogelijke baten voor de Belastingdienst en de wederkerigheid van de uitwisseling een rol kunnen spelen. In geval de uitkomst is dat gegevens niet of slechts beperkt worden verstrekt, wordt de daaraan ten grondslag liggende afweging besproken met de gegevensvragende dienst.

De Belastingdienst heeft als voornaamste fiscale taak het heffen en innen van de wettelijk verschuldigde belasting. Aan deze taak wordt op verschillende niveaus invulling gegeven. Het is voor de Belastingdienst van groot belang om bij het invullen van de loonaangifte, en het tegelijkertijd betalen van de belasting, de bereidheid om informatie te verstrekken aan de dienst te maximaliseren. In dit streven speelt de combinatie van artikel 47 Awr, de informatieverplichting en artikel 67 Awr, de geheimhoudingsverplichting een belangrijke rol. De aangever kan vrijuit aangeven, omdat hij er vanuit mag gaan dat de gegevens die hij verplicht is te leveren vertrouwelijk zullen worden behandeld. Vervolgens is toezicht nodig om te controleren of de belastingplichtige aan zijn informatie- c.q. betalingsverplichtingen heeft voldaan. In die zin zijn de gegevens naast heffingsgegevens ook toezichtgegevens.

In het kader van toezicht is in het algemeen sprake van meer gerichte gegevensuitvraag vanuit een convenantspartner bij de Belastingdienst. De toezichtgegevens kunnen worden opgevraagd in het kader van een bepaald concreet onderzoek, bijvoorbeeld een onderzoek naar een aannemer en zijn onderaannemers. Een andere mogelijkheid is dat aan de start van een onderzoek naar een bepaalde branche of beroepsgroep wordt gevraagd om de gegevens van die groep, bijvoorbeeld alle aannemers in een bepaald postcodegebied.

Bij de Belastingdienst wordt de huidige juridische inbedding als adequaat ervaren. Binnen het kader van de Uitvoeringsregeling kunnen gegevens worden verstrekt aan de partners. Daartoe worden afspraken gemaakt binnen de doelstellingen van de convenanten. Daarbij lijkt te worden gekozen voor een vrij ruime interpretatie van de ontheffing, in die zin dat de keuze vooral pragmatisch is en gericht op het resultaat van de samenwerking. De ervaringen met het ontvangen van informatie zijn wisselend. Daarbij zit de voornaamste potentiële beperking op de grens van de bestuursrechtelijke en de opsporingssfeer. Met name het verkrijgen van gegevens van politie en OM is niet altijd gemakkelijk. Niet zelden hangt het

1912170 01165

af van het niveau in de organisatie waarop de gegevens moeten worden verstrekt of zelfs van de persoonlijke relaties tussen betrokkenen. In die zin lijkt het eerder een besturingsprobleem dan een juridische drempel.

Gegevens worden in beginsel verstrekt op verzoek op subject-niveau (de gegevens van Dhr. Jansen BSN 000). In bepaalde gevallen kan hiervan worden afgeweken, en worden gegevens per groep verstrekt, bijvoorbeeld in verband met een handhavingactie. Zo heeft de SIOD op verzoek de gegevens van warme bakkers op postcode in een bepaald gebied gekregen in verband met een gericht onderzoek naar deze groep. Bij een dergelijk, niet op een individueel subject betrokken, verzoek kunnen enkele praktische toetsingscriteria een wat grotere rol gaan spelen. Zo moeten de gegevens logistiek en technisch beschikbaar zijn en moet de vraag proportioneel zijn met de leveringsinspanning. Tevens blijkt het te helpen als er een zeker belang is bij de leverende partij, bijvoorbeeld doordat de vragende dienst ook informatie heeft voor de leverancier.

3.2.2.7 Behoefte aan een wettelijke regeling?

Door de invoering van artikel 43c Uitvoeringsregeling Awr zijn er voldoende mogelijkheden om gegevens uit te wisselen. Het uitgangspunt is echter wel dat bestuursorganen worden aangespoord om een wettelijke verplichting aan de Belastingdienst om informatie te verstrekken, in hun eigen wetgeving op te nemen. Zo kan op termijn art. 43c worden uitgefaseerd. Regeling in de Awb ligt voor de Belastingdienst niet direct voor de hand. Een Awr-bepaling die in algemene zin tot uitwisseling verplicht lijkt lastig te verenigen met de geheimhoudingsbepaling van artikel 67 Awr. Vanwege de geheimhoudingsplicht vergt de verstrekking van gegevens door de Belastingdienst een wettelijke grondslag. Naast de Uitvoeringsregeling Awr kan dat ook een ander wettelijk voorschrift zijn. De regeling is zo flexibel dat zelfs vooruitlopend op een wettelijke grondslag een uitzondering kan worden opgenomen in 43c Uitvoeringsregeling Awr. Dit was aan de orde toen het Ministerie van BZK verzocht om de fiscale gegevens van kandidaat burgemeesters. Omdat het Ministerie het voornemen had om dit wettelijk te regelen was een brief van die strekking aan de Tweede Kamer voldoende om deze gegevenslevering onder artikel 43c te brengen. [117] Een ander voorbeeld is de discussie tussen het OM en de Belastingdienst of bij het vorderen van gegevens ten behoeve van strafrechtelijk onderzoek gebruik moet worden gemaakt van de formele machtiging op grond van artikel 126 Sv. Het OM vindt dat het convenant voldoende basis biedt voor de levering. De Belastingdienst vraagt echter om de machtiging en wordt daarin ondersteund door een recente uitspraak van de Rechtbank Utrecht.[118] In ieder geval maken deze voorbeelden duidelijk dat de vereiste wettelijke basis voor de gegevensuitwisseling niet licht wordt opgenomen.

Door de verschillende regelingen ontstaat soms onduidelijkheid over wat wel en wat niet is toegestaan. In die gevallen grijpt men terug op het credo 'bij twijfel niet inhalen'. Het komt overigens ook voor dat het bij twijfel niet zozeer gaat om een juridische belemmering maar om een organisatorisch of communicatieprobleem. Met de juiste aansturing kan de verstrekking dan alsnog plaatsvinden.

Vanuit de Belastingdienst wordt de samenwerking overigens door de gesprekspartners als goed aangemerkt. Wel zouden zij wensen dat ook andere diensten een met artikel 43c Uitvoeringsregeling Awr vergelijkbaar artikel in hun wetgeving opnemen, zodat alle uitwisseling in hetzelfde convenant geregeld kan worden. Vanuit het opsporingsapparaat wordt iets anders aangekeken tegen de uitwisseling van toezichtgegevens. Binnen de vanuit de bestuurlijke kant (BZK) opgezette vormen van samenwerking vinden de opsporingsdiensten de bereidheid om gegevens te leveren soms niet ver genoeg gaan.

117 Zie: *Kamerstukken II* 2010/2011, 32500 VII, nr. 99.
118 Rb. Utrecht (strafsector) 26 augustus 2011, *LJN* BR5924.

1912170 01165

3.2.3 Casus Vuurwerk

Het toezicht in het kader van vuurwerk betreft toezicht op de invoer daarvan, de opslag, de verkoop en het gebruik. In verband hiermee is een landelijke aanpak nodig en zijn er veel toezichthouders bij betrokken. Om informatie tussen een aantal betrokken toezichthouders uit te wisselen is er bij wijze van pilot een zogenaamde kruispuntbank opgericht. Daarmee hebben toezichthouders toegang tot informatie vergaard door andere handhavende instanties.

3.2.3.1 Juridisch kader inzake de gegevensuitwisseling

In het kader van vuurwerk en toezicht is geen specifieke regelgeving tot stand gebracht als het gaat om gegevensuitwisseling tussen de diverse op dit gebied werkzame toezichthouders. Daarom zijn de algemene wettelijke regelingen op dit toezicht van toepassing.

Voor betrokken bestuursorganen is de bevoegdheid tot uitwisseling gebaseerd op de algemene regels van de Wbp (artikelen 7, 8 en 9). Als het gaat om politiegegevens is de Wpg van toepassing. Onder een zwaarwegend algemeen belang als bedoeld in artikel 20 Wpg vallen het voorkomen en opsporen van strafbare feiten als hier aan de orde. Daarnaast is artikel 39 f Wjsg van toepassing. Een en ander betekent dat de doelbinding van groot belang is.

3.2.3.2 Samenwerking met gegevensverstrekkers en –ontvangers

De pilot met betrekking tot samenwerking en gegevensuitwisseling omvat provincies, gemeenten, regiopolitie, regionale vestigingen van het OM, de Belastingdienst, de IVW en de zogenaamde vliegende brigade vuurwerk.[119] Ten behoeve van de samenwerking is een convenant gesloten, het Ketendossier Vuurwerk convenant.[120] De bij het convenant aangesloten partijen zijn: het Korps landelijke politiediensten, het Functioneel Parket van het OM, de FIOD, de VROM-Inspectie (VI), de VROM-Inlichtingen- en opsporingsdienst (VROM-IOD), de Belastingdienst, de IVW, de Douane, bepaalde gemeentes, bepaalde provincies en de Dienst Centraal Milieubeheer Rijnmond.

3.2.3.3 Soort gegevens

De partijen wisselen gegevens uit die nodig zijn ter bestrijding en voorkoming van handelingen met verboden consumentenvuurwerk (artikel 2 convenant). Welke gegevens dat in concreto zijn vermeldt het convenant niet. Wel vermeldt de inleiding bij het convenant nog apart dat gegevens die onder de Wpg vallen in het kader van een op artikel 20 Wpg gebaseerde samenwerkingsovereenkomst aan de Minister van VROM ter beschikking kunnen worden gesteld.

3.2.3.4 Bijzondere persoonsgegevens

Artikel 7a bepaalt dat de partijen ook bijzondere persoonsgegevens verwerken. Artikel 7b bepaalt dat bijzondere persoonsgegevens niet verder worden verstrekt, 'tenzij daarvoor een rechtmatige verstrekkingsgrondslag plus een uitzondering op het verbod tot verwerking van bijzondere persoonsgegevens is aan te wijzen.' Dit heeft betrekking op de artikelen 16 en verder van de Wbp, maar werkt dit verder niet uit voor de specifieke informatie waar het convenant betrekking op heeft.

3.2.3.5 Doelbinding

Artikel 2 van het convenant bepaalt dat gegevens worden uitgewisseld als dat noodzakelijk is met het oog op: a. het voorkomen en opsporen van strafbare feiten, b. het uitoefenen van toezicht op het naleven van regelgeving, c. het geven van een bestuursrechtelijke of strafrechtelijke reactie of het nemen van een vervolgbeslissing naar aanleiding van een geconstateerde overtreding, en ten slotte d. met het oog op

119 Zie Uitwisseling van handhavingsinformatie, Den Haag 16 juni 2010.
120 Op het moment van publicatie van dit rapport was dit convenant nog niet openbaar gemaakt.

1912170 01165

informatievergaring en informatieveredeling ten behoeve van het onder a t/m c genoemde. De onder a en b genoemde doelen zijn direct ontleend aan artikel 20, eerste lid, onder a en d, Wpg.

Artikel 6 bepaalt dat de gegevensuitwisseling slechts plaatsvindt met het oog op de in artikel 2 geformuleerde doelen. Verder verplicht artikel 5c de partijen de beschikbare gegevens uitsluitend te gebruiken met het oogmerk de doelstellingen van het convenant te bewerkstelligen. Deze verplichting vloeit al voort uit artikel 7 Wbp en 9 Wbp.

Artikel 7 van het convenant bepaalt dat de partijen alleen gegevens zullen verwerken, indien en zolang dit noodzakelijk is voor het realiseren van bovengenoemde doelstellingen. Bovendien zullen partijen volgens hetzelfde artikel 7 hierbij niet meer gegevens verwerken dan noodzakelijk voor het bereiken hiervan. De gegevens zijn bovendien gelet op de doeleinden waarvoor ze worden verwerkt toereikend, ter zake dienend en niet bovenmatig. Deze eis is ook opgenomen in artikel 11, eerste lid, Wbp, artikel 3, tweede lid, Wpg en artikel 39c, tweede lid, Wjsg.

3.2.3.6 Geheimhouding en verstrekking aan derden

Artikel 6b van het convenant bepaalt dat partijen gegevens niet aan derden verstrekken, tenzij betrokkene toestemming heeft gegeven of als de verstrekking plaatsvindt op basis van een er wettelijke bevoegdheid of een wettelijke plicht is die om gegevens te verstrekken. In welke situaties zich dat voordoet wordt in het convenant niet in concreto aangegeven. Artikel 6c bepaalt dat aan medewerkers van partijen een geheimhoudingsplicht moet worden opgelegd.[121] Al met al biedt het convenant behalve de geheimhoudingsplicht weinig meer dan een bevestiging van de wettelijke kaders.

3.2.3.7 Ervaringen en knelpunten

Een van de problemen die hier volgens de betrokkenen in het veld speelt is dat niet alle deelnemers een even grote bereidheid hebben om informatie te leveren. Een eerste oorzaak hiervoor is dat de verschillende betrokken toezichthouders tot op zekere hoogte verschillende belangen hebben. Zo zijn gemeenten gegeven hun bevoegdheden meer gericht op problemen die zich direct binnen hun eigen gemeente afspelen en heeft landelijke handhaving een minder grote prioriteit.

Sommige betrokken toezichthouders zijn terughoudend met het verstrekken van informatie, aldus een respondent, omdat het hen niet altijd even duidelijk is in hoeverre het wettelijk is toegestaan de gevraagde informatie te verstrekken. Deze onduidelijkheid kan worden veroorzaakt door het feit dat er niet één algemene regeling is die handelt over deze vraag of omdat de bestaande wetgeving niet op alle punten even helder is. Bovendien zorgt de doelbinding voor extra onduidelijkheid en onzekerheid op dit punt: vertonen de doeleinden van gegevensverwerking van de leverancier en ontvanger wel voldoende verwantschap? Een ander ervaren probleem is dat niet alle aangeleverde informatie even betrouwbaar blijkt te zijn.

Door de vuurwerkramp in Enschede is milieuhandhaving veel steviger op de kaart gezet, met name naar aanleiding van het rapport van de Commissie Mans (2008).[122] Het veld van de milieuhandhaving is complex. Naast elkaar bestaan twee regimes ter handhaving van het milieurecht: het bestuursrecht en het strafrecht. Op beide terreinen gezamenlijk zijn zo'n 400-450 handhavingsinstanties actief. De keten omvat import-vervoer-opslag-gebruik en met name ook de tussenliggende overdrachtsmomenten. Van belang is vooral zicht krijgen op voldoende relevante toezichtinformatie.

121 Een dergelijke voor een individuele medewerker geldende geheimhoudingsplicht kan niet rechtstreeks op een convenant berusten, maar wel op een (interne) aanwijzingsbevoegdheid (over het gebruik waarvan door het bevoegde gezag een afspraak is gemaakt).

122 *De tijd is rijp* (advies van de Commissie Mans, het onderzoeksteam Herziening handhavingsstelsel VROM-regelgeving, juli 2008), *Kamerstukken II* 2007/08, 22 343, nr. 201.

1912170 01165

Zo wordt bij de bestrijding van illegaal vuurwerk gebruik gemaakt van informatie-uitwisseling tussen de verschillende handhavers door middel van de kruispuntbank. Daarmee hebben handhavers direct toegang tot de beschikbaar gestelde informatie, en kunnen zij deze downloaden en bewerken.

De vuurwerkramp is een belangrijke testcase voor de milieuhandhaving geweest. Ondanks de verschillende rechtssystemen en wetgeving is volgens een respondent bij het Vuurwerkdossier niet zozeer sprake van juridische belemmeringen. Bij de pilot Vuurwerk die is gehouden kwamen vooral de grote verschillen in belang van de diverse spelers aan het licht. Betrokkene wijt dat aan het feit dat met name provincies en gemeenten een geografisch begrensd belang hebben. Zij willen enerzijds veiligheid in hun eigen gemeente of provincie, maar anderzijds willen zij hun burgers en bedrijven ter wille zijn en niet zozeer handhaven. Daarmee kunnen zij in een belangenspagaat komen. Kijkend over gemeente en provinciegrenzen heen kan de belangentegenstelling er toe leiden dat de ene gemeente meewerkt en de andere gemeente terughoudend is, ook al is er sprake van duidelijke overtreding van de regels. Daarbij speelt ook dat het gemeenteveld wordt gekenmerkt door een grote verscheidenheid en er geen sprake is van eenduidige kwaliteit van het toezicht.

Gewerkt wordt aan een Inspectieview voor milieuhandhaving. Tevens worden steeds meer regionale milieudiensten gevormd wat tot de nodige professionalisering moet leiden. De huidige convenanten voldoen maar in beperkte mate vanuit de strafrechtoptiek. Een wettelijke regeling wordt meer wenselijk gevonden met het idee dat goede duidelijke wetgeving drempels en vermeende koudwatervrees bij de betrokken toezichthouders kan wegnemen.

Een probleem vormt volgens een respondent de beleefde 'eigendom' van gegevens bij uitvoeringsorganisaties. Voor het OM zijn de belangen van uitvoeringsinstanties, zoals geheimhouding en doelbinding, niet altijd voldoende helder. Daardoor wordt het vasthouden aan deze noties soms als lastig ervaren. Ook het risico van de doorlevering van onrechtmatig verkregen informatie kan een drempel vormen om gegevens te leveren. De vraag rijst dan wie op welke wijze aansprakelijk is en kan worden gesteld voor deze onrechtmatigheid. Een gemeenschappelijk afwegingskader zou hier volgens een respondent wellicht een oplossing kunnen bieden.

Gegevensuitwisseling maakt nu steeds deel uit van de convenanten. Vanuit het OM bestaat een voorkeur voor eenduidige en op de gegevensuitwisseling tussen de verschillende domeinen gerichte wetgeving. Hiermee kan veel onnodige discussie worden voorkomen, zeker als de informatie in strafzaken wordt gebruikt en de rechtmatigheid van de verkrijging moet komen vast te staan. De representant van het OM geeft aan dat standaardisatie nodig is bij de technische invulling van de samenwerking, bijvoorbeeld standaardschermen bij de kruispuntbank. Tot slot worden de verhouding tussen opsporing en uitvoering en een classificatiesysteem voor informatie (hoe hard en betrouwbaar is deze informatie) als aandachtspunten geformuleerd.

3.2.3.8 Behoefte aan een wettelijke regeling?

Niet alle problemen die spelen bij de informatie-uitwisseling tussen toezichthouders kunnen volgens de betrokkenen opgelost worden door regelgeving. Op sommige punten zou regelgeving wellicht wel een verbetering kunnen realiseren.

Ook als de uitwisseling wettelijk is toegestaan blijken volgens betrokkenen niet alle toezichthouders even actief bij het uitwisselen van gegevens. Hier zou de wetgever, als uitwisseling in het algemeen belang is, in een regeling kunnen bepalen in hoeverre bestuursorganen verplicht zijn in het belang van handhaving en toezicht gegevens uit te wisselen.

1912170 01165

Voor zover er onduidelijkheid kan bestaan over de vraag of uitwisseling is toegestaan, zou een algemene regeling volgens betrokkenen meer duidelijkheid kunnen brengen. Een van de bronnen van onduidelijkheid is dat er op de relevante toezichthouders in het vuurwerkdossier drie verschillende wetten ten aanzien van de gegevensuitwisseling van toepassing zijn (de Wbp, de Wpg en de Wjsg), die niet op alle vergelijkbare punten eenzelfde regeling kennen.

Volgens betrokkenen zou een algemene wettelijke regeling ook verduidelijking kunnen bieden bij vragen over welke wijzen van gegevensuitwisseling zijn toegestaan. Daarnaast zien betrokkenen de eisen van de doelbinding soms als een oorzaak voor onduidelijkheid. Wie is er bijvoorbeeld aansprakelijk voor een gebruik in strijd met de doelbinding? Handelt alleen degene die ze gebruikt in strijd met het doel of ook de verstrekker van de gegevens? Wie controleert eigenlijk of aan de eisen van doelbinding voldaan wordt? Hoe kan dit gecontroleerd worden in een keten van gegevensuitwisseling? Bijvoorbeeld als A informatie levert aan B en B vervolgens aan C. Hoe weet C met het oog op welk doel A de informatie verzamelde, als C die informatie aantreft in een gezamenlijke databank? Voor dit soort problemen zou een algemene regeling een oplossing kunnen bieden, stellen betrokkenen.

Omdat sommige van deze problemen sterk sector gerelateerd zullen zijn, ligt een regeling in de Awb volgens een respondent minder voor de hand. Een kaderwet, die in nadere regelingen per sector uitgewerkt kan worden is wellicht effectiever.

3.3 Expertmeeting en uitkomsten

De expertmeeting op 29 februari 2012 was bedoeld om scherper zicht te krijgen op de praktische en juridische problemen met het verstrekken of uitvragen van gegevens en om te peilen of een algemene regeling uitkomst zou bieden. In de loop van het gesprek met de genodigden, allen werkzaam bij overheidsinstanties en private kantoren die dagelijks te maken hebben met gegevensuitwisseling,[123] ontstond geleidelijk een beeld van de knelpunten en van ontwikkelingen waarop dient te worden ingespeeld. Hierna volgt een kort verslag van hetgeen is besproken.[124] Het reflecteert hetgeen door de experts is ingebracht en geeft niet het oordeel van de onderzoekers weer.

Sommige punten zijn specifiek voor de betreffende dienst. De meeste hebben een algemeen karakter en betreffen onduidelijkheid over welke gegevens mogen worden verstrekt, onduidelijkheid over wat uiteindelijk met de gegevens gebeurt, kleuring van gegevens tijdens het verzamelen ervan en daarmee samenhangend een mogelijk ontoereikende betrouwbaarheid voor hergebruik, ondoordacht aanleggen van databestanden, en de opkomst van 'cloud computing'. Een algemene regeling, althans in de Awb, werd niet als oplossing gezien.

3.3.1 Organisatie-specifieke punten

De gemeenten verkeren in een lastige positie, omdat gefragmenteerd geregeld is wanneer een gemeente gegevens mag krijgen. Een hindernis is dat wanneer wel is geregeld dat gegevens kunnen worden ontvangen, de omschrijving van de soort gegevens en het doel waarvoor deze mogen worden gebruikt zo specifiek is, dat bij een nieuw aanpalend geval weer aanpassing van de regelgeving nodig is. Een voorbeeld vormt de beperkte reikwijdte van de Wet Bibob: gemeentebesturen kunnen wel informatie ontvangen over coffeeshops, maar niet over headshops. Om dat te bereiken is een aanpassing van het Besluit Bibob

123 Gemeente Amsterdam, Belastingdienst, OM (Functioneel Parket), Dienst Justis, CBP, Fort Advocaten, Kloosterman Statistical Audit Consulting. Zie *infra* bijlage 7.3 voor de lijst van deelnemers aan de expertmeeting van 29 februari 2012.
124 Een verslag van deze bijeenkomst is beschikbaar.

1912170 01165

nodig.[125] Die versnipperdheid zou volgens een expert kunnen worden aangepakt door een specifiek op de gemeenten toegesneden regeling te maken, bijvoorbeeld in de Wpg met een spiegelbeeld in de Gemeentewet.

Wat de Belastingdienst betreft zijn er vooral problemen met het verstrekken van gegevens in een voorfase, namelijk wanneer nog niet een bepaald persoon in het vizier is. De aanwezige expert verwijst naar het Amsterdamse project Emergo.[126] Problemen kwamen op bij het verstrekken van informatie over een bepaalde wijk. Er werd toen gekozen voor een 'black box' waarin de informatie verzameld werd. Pas als daar iets uitkwam, werd de informatie naar de overheidsdienst gestuurd die er iets mee moest doen. Dit was een praktische – *ad hoc* – oplossing.

Voor het overige wordt gegevensverstrekking van en aan de Belastingdienst niet als een *juridisch* probleem ervaren. Praktisch is het wel vaak veel werk omdat datasets worden gevraagd met specifieke kenmerken, die technisch gezien lastig te genereren zijn.

3.3.2 Onduidelijkheid bij verstrekking

Experts brachten naar voren dat overheidsdiensten wel steeds meer samenwerken in een geïntegreerde aanpak, maar dat gegevensuitwisseling daarbij onvoldoende wordt geregeld. Dit heeft tot gevolg dat terughoudendheid ontstaat bij verstrekking. Men wil aan de veilige kant blijven, terwijl daarnaast ook een rol speelt dat diensten de gevraagde gegevens als hun terrein beschouwen.

3.3.3 Onduidelijk zicht van verstrekker op gebruik

Voor gegevensuitwisseling is communicatie het eerste vereiste. Niemand verstrekt graag gegevens als niet duidelijk is wat ermee gebeurt, aldus de experts. Zicht op het hele proces is nodig, zowel inhoudelijk als bijvoorbeeld in het tijdsverloop. De originele bronhouder wil weten of en, zo ja, welke actie plaatsvindt op grond van de ontvangen gegevens. Wat gebeurt er bijvoorbeeld met gegevens nadat de actie in het kader waarvan de gegevens zijn verkregen is afgelopen? Het overdragen zelf kan ook een knelpunt vormen. Hierbij geldt: hoe minder overdrachtsmomenten, hoe minder knelpunten zich zullen voordoen. Met name moet worden voorkomen dat taken over meerdere toezichthouders worden verdeeld. Als dat toch het geval is wordt veelal het 'gazo' principe gehanteerd: 'geen actie zonder overleg'. Dit gebeurt bijvoorbeeld bij diensten die te maken hebben met 'Wid/MOT'[127] zaken, zoals het Financieel Expertise Centrum. Het gaat dan vooral om bedrijfsgevoelige gegevens, niet om persoonsgegevens.

3.3.4 Kleuring van gegevens en betrouwbaarheid voor hergebruik

De experts brachten naar voren dat onder andere bij politiegegevens (processen-verbaal) de gegevens niet altijd even hard zijn. Welke hardheidsgraad de gegevens hebben, is vaak niet bekend. De gegevens kunnen uit meerdere bronnen komen, of het relaas kan onvolledig zijn. Dat is niet goed te controleren. In ieder geval dient volgens bepaalde experts onderscheid te worden gemaakt tussen 'data' en 'informatie'. Achter 'data' ligt namelijk een beslissingsproces dat tot 'informatie' leidt. In het enkele geval zal de rechter toetsen op zorgvuldigheid, maar zorgwekkend voor de praktijk vinden de experts dat databestanden

125 *Kamerstukken II* 2010/11, 32 676 (de Evaluatie- en Uitbreidingswet Bibob).

126 Gezamenlijke, geïntegreerde aanpak van zware criminaliteit in het postcodegebied 1012 (Wallen, Dam en Rokin), gestart medio 2007, en voortvloeiend uit het rapport *Grenzen aan de handhaving. Nieuwe ambities voor de Wallen*, Bestuursdienst Gemeente Amsterdam, Directie OOV/Van Traa-team, september 2007. Het eindrapport van de Projectgroep Emergo, getiteld *De gezamenlijke aanpak van de zware (georganiseerde) misdaad in het hart van Amsterdam*, Bijlage bij *Kamerstukken II* 2011/12, 29 911, nr. 55, verscheen in 2011 bij uitgeverij Boom, Amsterdam.

127 Wet identificatie dienstverlening (Wid) en Wet ongebruikelijke transacties (MOT), in 2008 samengevoegd in de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft). Het 'gazo' principe is vastgelegd in artikel 4 van het Informatieprotocol FEC 2011, 14 november 2011. Zie: <www.fec-partners.nl/nl/nieuws/nieuwsbericht/63>.

1912170 01165

'vervuild' kunnen zijn met zachte informatie, en daardoor onbruikbaar voor hergebruik. Een eventuele algemene regeling zal volgens de experts dan ook het hele verzamelproces moeten bestrijken, inclusief tussentijdse aggregaties.[128]

3.3.5 Organisatorische aspecten van gegevensuitwisseling

In het WRR rapport *iOverheid* komen behalve juridische kaders ook organisatorische aspecten van gegevensuitwisseling ter sprake.[129] De experts geven aan dat in de praktijk dataverzamelingen vaak worden opgezet zonder dat van te voren goed bedacht is wat ermee gaat gebeuren. Pas wanneer men vervolgens deze gegevens wil delen en dataverzamelingen koppelen, wordt nagedacht over wat men heeft, wat men er mee wil en of het juridisch wel kan. Deze werkwijze van eerst doen, dan pas afvragen of het kan qua wettelijke basis en bevoegdheden, levert weliswaar vaak op dat het kan, op voorwaarde dat er voldoende waarborgen worden ingebouwd, maar geeft aan dat naast het juridisch kader organisatorische aspecten eveneens belangrijk zijn.

3.3.6 Technische ontwikkelingen

Gesignaleerd wordt dat steeds vaker verzamelingen worden aangelegd die zich lenen voor collectieve uitvraag. Dat kan middels een 'mid-office', of 'cloud-computing'. Het gaat dan niet langer om het koppelen van specifieke databestanden van bepaalde instanties. De vraag is hoe je daar juridisch mee omgaat. Als je weet wie verantwoordelijk is voor het opzetten van een dataverzameling, dan nog zijn er vele beslismomenten waarbij ook partijen met wie gegevens worden gedeeld, of die de dataverzameling aanvullen, invloed en zeggenschap hebben. Van wie zijn de gegevens, waar komen ze vandaan, wie kun je aanspreken? Dat zijn vragen die steeds moeilijker kunnen worden beantwoord.[130]

3.3.7 Algemene regeling?

Van de zijde van het CBP wordt benadrukt dat de Wbp in principe een wettelijk kader biedt dat op alle vragen een antwoord zou moeten geven. Toepassing van de Wbp op de verschillende vormen van gegevensuitwisseling blijkt in de praktijk niet gemakkelijk, mede door de samenloop met andere regelingen. Alvorens een nieuwe algemene regeling te maken zouden volgens de experts de knelpunten nader moeten worden onderzocht, om stapeling van regelingen te voorkomen.

Een algemene regeling in de Awb vinden de experts minder voor de hand liggen vanwege het feit dat de Awb niet alle betrokken gegevensregimes afdekt. Met name het strafvorderlijke traject heeft een eigen regime. Blijft over een regeling in een Kaderwet, of in de betreffende bijzondere wetten. De vraag is of een dergelijke regeling nut heeft als in verband met doelbinding toch weer allerlei uitzonderingen moeten worden gemaakt, en een deel van de problemen kan worden opgelost door een coöperatieve houding van de betrokken diensten. De experts opperen dat een standaard convenant met een goede toelichting hier mogelijk meer soelaas kan bieden dan een nieuwe wettelijke regeling.

128 De EU ontwerprichtlijn gegevensbescherming bevat een verplichting daartoe. Zie *supra*, hoofdstuk 2, par. 2.3.2.

129 Zie *iOverheid* (rapport van 2 maart 2011, WRR), Amsterdam: Amsterdam University Press 2011, hoofdstuk 8, par. 8.5.2., 'Ontbreken van noodzakelijke organisatorische en institutionele inbedding', p. 203-204, en hoofdstuk 9, par. 9.2.2., 'Organisatorische inbedding voor duurzame en rechtvaardige informatiestromen', p. 219-220.

130 Zie ook: *iOverheid* (rapport van 2 maart 2011, WRR), p. 222-223 (over *WikiLeaks* en het risico van oncontroleerbare migratie van overheidsinformatie op internet), en p. 82 (risico's voor de privacy van burgers).

1912170 01165

3.4 Enquêteresultaten en MCA

Op basis van de geraadpleegde stukken, een 'brainstorm' binnen het onderzoeksteam, verificatie van de gevonden belangen bij zowel ervaringsdeskundigen als bij de begeleidingscommissie zijn vragenlijsten opgesteld voor de enquête ten behoeve van de Multicriteria-analyse (MCA).[131] De formulieren zijn uitgezet bij drie doelgroepen, bestuurlijke toezichthouders, de opsporingsinstanties en vertegenwoordigers van burgers en bedrijven, waarbij gebruik is gemaakt van de deelnemers in de verschillende casus en van eigen netwerken van de onderzoekers. Voor een verdere uiteenzetting van de gehanteerde methode verwijzen we naar paragraaf 3.1. Ongelukkigerwijs viel het moment van uitzetten samen met het begin van een voorjaarsvakantieperiode van twee weken. Daardoor verliep het retourneren van de ingevulde formulieren minder vlot dan werd verwacht.

In de enquête zijn de belangen opgenomen die in het voorafgaande traject als meest relevante waren gedetecteerd. Het ging daarbij om de doelbinding, de privacy, zowel van het subject als van mogelijk betrokken derden, de geheimhouding, de kosten van het verstrekken van gegevens en de baten voor zowel de ontvanger als voor de leverancier. Deze belangen zijn voorzien van een toelichting. De toelichting voor de overheidsinstanties verschilde van die voor de vertegenwoordigers van burgers en bedrijven, aangezien zij vanuit een ander perspectief handelen.

Voor de overheidsinstanties werden de belangen als volgt toegelicht. Onder doelbinding van de uit te wisselen toezichtgegevens is verstaan de doelbinding zoals die in de Wbp is geregeld. Ter toelichting is in de enquête vermeld dat de gegevens met het oog op een bepaald doel door het subject zelf zijn afgegeven of buiten hem om verzameld. Bij de privacy van het subject is ter toelichting vermeld dat het leveren van toezichtgegevens mogelijk tot aantasting van de privacy van het subject leidt. Het belang van de privacy van een eventuele derde is aldus toegelicht dat het leveren van gegevens mogelijk leidt tot aantasting van de privacy van een derde. Op het punt van de geheimhouding van de toezichtgegevens is aangegeven dat er een organisatiebelang is gediend met geheimhouding van de gegevens. Vervolgens is gevraagd naar het belang van de kosten in tijd, geld, personeel en technische en/of organisatorische aanpassingen die moeten worden gemaakt om de gevraagde gegevens te kunnen leveren. En omgekeerd naar de baten voor de eigen organisatie (wederkerigheid) indien gegevens worden geleverd. Hierbij gaat het om het verlangen van een tegenprestatie in de sfeer van gegevensuitwisseling. Als volgende belang is genoemd de baten voor de ontvangende organisatie, dat wil zeggen het belang dat de ontvangende organisatie heeft bij de levering van gegevens.

Voor de vertegenwoordigers van burgers en bedrijven luidde de toelichting op de eerste drie belangen (doelbinding, privacy van het subject, privacy van een derde) hetzelfde. Bij de volgende belangen was de toelichting meer toegesneden op de positie van verstrekkende burger/vertegenwoordiger. Bij geheimhouding van de toezichtgegevens werd aangegeven dat de gegevens uitsluitend binnen de uitwisselende organisaties worden gebruikt. Bij kosten c.q. moeite van het verstrekken van de gegevens werd gevraagd naar het belang van de kosten in tijd, geld, personeel en technische en/of organisatorische aanpassingen die moeten worden gemaakt om de gevraagde gegevens te kunnen uitwisselen. Bij de baten voor het subject c.q. de vertegenwoordiger werd gevraagd naar het belang van stroomlijning van controles of minder administratieve lasten.

Alle drie de geënquêteerde groepen blijken een groot belang toe te kennen aan wat in het WRR rapport I-Overheid wordt aangeduid met de 'verankerende beginselen'.[132] Zowel aan de kant van de overheid als bij

131 Zoals in hoofdstuk 1 is opgemerkt is een Multicriteria-analyse (MCA) is een wetenschappelijke evaluatiemethode met behulp waarvan een rationele keuze kan worden gemaakt tussen verschillende alternatieven op basis van meer dan één onderscheidingscriterium.

132 *iOverheid* (rapport van 2 maart 2011, WRR), p. 79.

1912170 01165

de vertegenwoordigers van burgers en bedrijven komt dezelfde top drie van belangen naar voren: Doelbinding, Geheimhouding en Privacy van het subject. Deze belangen scoren over de hele linie het hoogst. Doelbinding eindigt zelfs bij alle lijsten in de top drie, geheimhouding ontbreekt maar een keer, verdrongen door het belang van de ontvanger. Kennelijk wordt aan deze beginselen een groot belang toegekend. In absolute zin is er wel een onderscheid tussen de verschillende groepen. Zo scoren de drie hoogste belangen voor de bestuurlijke toezichthouders weliswaar ook bij de opsporingsorganisaties als hoogste, maar wel met beduidend minder stemmen.

Een aantal keren wordt de privacy van het subject verdrongen uit de top drie. Zo bleek bij de leveranciers van toezichtgegevens het belang van de leverancier zelf de privacy van het subject te verdringen van de derde plaats. Bij ontvangers van opsporingsgegevens en in de opsporingsfeer bleken de baten voor de ontvanger hoger te scoren dan de privacy. Samenvattend worden voldoen aan de eis van doelbinding, voldoen aan geheimhoudingsplichten, bescherming van de privacy en de eigen baten voor de organisatie als belangrijkste punten gezien met betrekking tot de gegevensuitwisseling. Drie van deze punten zijn normatief van aard: de toezichthouders vinden het naleven van de wettelijke kaders kennelijk zeer belangrijk. Opvallend was de lage score van kosten in alle gevallen.

Bij alle vragenlijsten die aan de *bestuurlijke toezichthouders c.q. uitvoeringsorganisaties en de opsporingsinstanties* zijn voorgelegd werd ook gevraagd naar de gepercipieerde kwaliteit van de gegevens. De kwaliteit was onderverdeeld in de noties tijdigheid, compleetheid, betrouwbaarheid, actualiteit en passendheid. Wat bij de beantwoording is opgevallen zijn de zeer hoge scores. De laagste score is 3,8 op de schaal van 5, de hoogste zelfs 4,9. Opvallend was dat niet alleen de leveranciers hun eigen leveranties goed beoordelen maar dat de ontvangers dat ook doen.

Bij de *vertegenwoordigers van burgers en bedrijven* blijft de top drie – doelbinding, geheimhouding en privacy van de cliënt – bij alle invalshoeken overeind. Verder vielen de aandacht bij de vertegenwoordigers voor de privacy van derden en de relatief lage klassering van de baten voor de cliënt op.

Bij alle vragenlijsten is de ruimte opengelaten om een belang dat in de lijst werd gemist aan te vullen. Van deze gelegenheid is slechts beperkt gebruik gemaakt. Bij de respondenten van *bestuurlijke toezichthouders c.q. uitvoeringsorganisaties* zijn twee belangen aangegeven: het algemeen belang en het belang van de juistheid van de gegevens. Ook is gewezen op het risico van het niet of niet correct ontvangen van de toezicht-gegevens. Bij de respondenten uit de opsporing werd het belang van een overheidsbreed effectief optreden genoemd, het gemeenschappelijk overheidsbelang en het organisatieoverstijgend belang. Het ontbreken van een gemeenschappelijk of algemeen belang in de lijst werd kennelijk door enkele respondenten als een gemis ervaren.

Bij de *vertegenwoordigers van burgers en bedrijven* werd de lijst aangevuld met 'transparantie', een belang dat in het rapport iOverheid als procesmatig belang wordt aangegeven, en het risico aansprakelijk te worden gesteld. Gelet op de beperkte omvang van het onderzoek en de kwalitatieve aard ervan zijn de uitkomsten indicatief en kunnen hieraan slechts in beperkt mate conclusies worden verbonden.

3.5 Resultaten

Hierna volgen de resultaten van het onderzoek met betrekking tot het in paragraaf 3.2. tot en met 3.4 gepresenteerde materiaal. De resultaten zijn onderverdeeld in rubrieken.

1912170 01165

3.5.1 Juridisch kader

In de casus valt op dat bij het gemeentelijk taxivervoer, noch bij de vuurwerkketen kan worden teruggevallen op een specifieke op het domein toegesneden regeling voor de uitwisseling van toezicht- en opsporingsgegevens. Dit maakt dat gekozen moet worden voor ad hoc oplossingen of aanpassing van specifieke regelgeving. Een hindernis is dat wanneer wel is geregeld dat gegevens kunnen worden ontvangen, de omschrijving van de soort gegevens en het doel waarvoor deze mogen worden gebruikt zo specifiek is, dat bij een nieuw aanpalend geval weer aanpassing van de regelgeving nodig is. Tijdens de expertmeeting werd in dit verband het voorbeeld gegeven van de beperkte reikwijdte van de Wet Bibob: gemeentebesturen kunnen wel informatie ontvangen over coffeeshops, maar niet over headshops.

Wel is het zo dat de betrokken partners in de samenwerking soms gegevens kunnen uitwisselen op basis van een eigen wettelijk geregelde bevoegdheid daartoe. De Belastingdienst is daarvan een goed voorbeeld: deze dienst heeft op grond van de Uitvoeringsregeling Awr een duidelijk kader voor gegevensverstrekking aan andere toezichthouders en opsporingsdiensten, terwijl de Awr zelf duidelijke regels stelt over het opvragen van gegevens door de Belastingdienst bij andere toezichthouders en opsporingsdiensten. In veel gevallen kan vanwege de verplichting tot gegevensverstrekking in artikel 55 Awr geen beroep worden gedaan op een geheimhoudingsplicht ter afwering van een informatieverzoek van de Belastingdienst. Een uitzondering is de geheimhoudingsplicht op grond van de Wft. [133] Dit valt te verklaren uit de omstandigheid dat de belastingheffing zodanig belangrijk wordt gevonden, dat moet worden verzekerd dat de benodigde gegevens ook kunnen worden verzameld. Daar waar een toegesneden regeling ontbreekt, werken de betrokken toezichthouders en opsporingsdiensten met de algemene regeling van de Wbp (zie hiervoor Hoofdstuk 2).

3.5.2 Samenwerking en basis voor uitwisseling

Samenwerking is domeinspecifiek. Dat betekent dat steeds op grond van object en inhoud van de toezichtsactiviteiten wordt gezocht naar partners die relevante toezichtsinformatie hebben. In vrijwel alle samenwerkingsverbanden komen we de Belastingdienst tegen. Ook gemeenten zijn vaak partner. Een opvallend verschil tussen beide partners is dat de Belastingdienst op grond van eigen domeinspecifieke regelgeving gegevens kan verstrekken en kan opvragen, terwijl gemeenten opereren in zeer verschillende domeinen en daardoor steeds opnieuw moeten onderzoeken wat de mogelijkheden en bevoegdheden zijn. Gemeenten hebben daardoor vaak moeite om aan relevante toezichtgegevens te komen, juist in samenwerkingsverbanden waarin ook de politie is betrokken. De Wpg noemt gemeentebesturen (met uitzondering van de burgemeester in het kader van de handhaving van de openbare orde) namelijk niet als vaste partij waaraan gegevens kunnen worden verstrekt. Daarnaast zoeken partners soms samenwerking met partijen die niet tot de overheid behoren of semi-overheid zijn. Een voorbeeld daarvan is het taxidossier, waarin de gemeente Amsterdam samenwerking zoekt met de TTO's. Het blijkt lastig om van dergelijke partijen gegevens te verkrijgen, omdat zij particulieren zijn, er geen domeinspecifieke regelgeving ter zake is en dus op grond van de Wbp moet worden geopereerd.

Zowel in het vuurwerkdossier als in het taxidossier is sprake van recente samenwerking. De basis voor die samenwerking wordt gevonden in convenanten, die specifiek met het oog op deze domeinen zijn gesloten. De samenwerkende partners in het vuurwerkdossier hebben een zogenoemde kruispuntbank opgericht, waarmee gegevensuitwisseling wordt gefaciliteerd. Een belangrijke vorm van structurele samenwerking in de zin van artikel 22 Wpg betreft die in de RIEC's. Deze vindt plaats op basis van een landelijk convenant, dat wordt uitgewerkt in regionale akkoorden.

133 Zie hierover paragraaf 2.6.2

1912170 01165

Het valt op dat de meeste convenanten die tijdens het onderzoek zijn geraadpleegd op belangrijke punten geen concrete en heldere afspraken bevatten. Dit betreft vooral de vraag wanneer precies gegevens kunnen worden verstrekt, welke gegevens worden verstrekt en in hoeverre de ontvanger daarvan vrijelijk gebruik kan maken. Wel wordt gestipuleerd dat de partners moet handelen binnen de voor henzelf 'toepasselijke wettelijke kaders'. Ook is niet altijd duidelijk wie precies de verantwoordelijke is in de zin van de Wbp met betrekking tot sets van gegevens die tot stand zijn gekomen door koppeling van informatie. Soms bestaat bij de betrokkenen de indruk dat als er maar een convenant is, elke uitwisseling van gegevens toelaatbaar is.

3.5.2.1 Soorten gegevens

In alle bestudeerde cases worden persoonsgegevens, bijzondere persoonsgegevens en overige gegevens uitgewisseld. Het gaat daarbij in de meeste gevallen om politiegegevens en strafvorderlijke en justitiële gegevens. Daarnaast komt het ook voor dat andere persoonsgegevens, zoals rijgeschiktheid, klantbejegening, functie binnen een bedrijf, financiële gegevens, proces-verbalen van inspecties e.d. worden uitgewisseld.

3.5.3 Ervaringen en knelpunten/Betrokken belangen en weging

Hierna worden de knelpunten en ervaringen besproken, die in het onderzoek zijn gesignaleerd en door de experts tijdens de expertmeeting naar voren zijn gebracht.

3.5.3.1 Gefragmenteerde regelgeving

De gemeente vindt dat zij in een lastige positie verkeert, omdat – buiten de context van specifieke beleidsterreinen met sectorwetgeving, zoals de sociale zekerheid – gefragmenteerd geregeld is wanneer een gemeente gegevens mag krijgen. Dit klemt, omdat gemeenten steeds meer toezichtstaken krijgen, zonder dat de bijbehorende rechten om gegevens te ontvangen duidelijk zijn geregeld. Dit heeft tot gevolg dat gemeentebesturen gebruik moeten maken van de ad hoc constructies die de wet toestaat. Vanuit de gemeente is gesuggereerd dat deze versnipperdheid zou kunnen worden aangepakt door een specifiek op de gemeente toegesneden algemene regeling te maken.

3.5.3.2 Ontbreken verplichting tot informatieverstrekking

Verschillende gesprekspartners ergeren zich aan de terughoudendheid of soms ook de gepercipieerde onwil om gegevens te verstrekken, terwijl duidelijk is dat de bevoegdheid ertoe wel bestaat. Politie en OM zijn niet scheutig met het verstrekken van gegevens, terwijl omgekeerd het OM meer gegevens zou willen ontvangen van de verschillende overheidsdiensten. Ook de gemeente Amsterdam heeft moeite om gegevens te krijgen van politie en OM. Een wettelijke regeling wordt door de gemeente gezien als een oplossing, als daarin voor bepaalde nader aangegeven gevallen een verplichting wordt opgenomen tot het verstrekken van informatie, indien een verzoek daartoe wordt gedaan.

3.5.3.3 Praktische problemen

Niet alle obstakels bij de uitwisseling van toezichtgegevens zijn van juridische aard. Vaak blijkt dat het juridisch kader op zich wel duidelijk is, of op managementniveau helder is, maar dat de communicatie hierover onvoldoende is. Dit geven met name de respondenten in de expertmeeting aan. Om die reden moet naar het oordeel van de onderzoekers de bijdrage van een meer uitputtende wettelijke regeling niet worden overschat. Daarbij komt dat sommige uitwisselingen niet gemakkelijk onder een eenduidig juridisch kader zijn te vatten. Wat de Belastingdienst betreft zijn er vooral problemen met het verstrekken van bijvoorbeeld gegevens voor meer algemene onderzoeksdoelen, wanneer nog niet een bepaald persoon in het vizier is. Dan is het moeilijk om in te schatten in hoeverre de Uitvoeringsregeling Awr zo'n verstrekking toelaat. Voor het overige zijn er vooral ook praktische problemen, bijvoorbeeld om

1912170 01165

gegevenssets zo aan te leveren dat zij geschikt zijn voor de ontvanger, of logistieke en technische problemen bij het aan elkaar koppelen van geautomatiseerde gegevensverzamelingen.

3.5.3.4 Onduidelijkheid bij verstrekking

Uit de interviews en tijdens de expertmeeting is gebleken dat partijen behoefte hebben aan verduidelijking van de toelaatbaarheid van gegevensverstrekking. Door de verknoping van verschillende wettelijke regimes (Wbp, Wpg, Wjsg, Awr en bijzondere wetten) is het de werkvloer niet altijd duidelijk wanneer welke gegevens kunnen worden verstrekt. Er bestaat de angst dat door de verstrekking ongeoorloofde privacyschending plaatsvindt, doordat (bijzondere) persoonsgegevens worden verstrekt aan een ontvanger die geen recht heeft om deze gegevens te verzamelen. Daarnaast is men beducht om gegevens te verstrekken aan het OM, omdat niet met zekerheid kan worden vastgesteld of deze gegevens zijn verkregen op een manier die spoort met waarborgen die een persoon als verdachte geniet. Daarmee staat in relatie tot het OM ook de rechtmatige verkrijging van de informatie ter discussie. Verstrekkende partijen proberen bijvoorbeeld te voorkomen dat het OM gegevens verkrijgt die vallen onder het zwijgrecht. In dergelijke gevallen geldt het adagium 'bij twijfel niet inhalen'.

3.5.3.5 Geen zicht op doeleinden gebruik bij doorverstrekking

Uit ons onderzoek is gebleken dat de verschillende partijen zich sterk verantwoordelijk voelen voor de bescherming van de (bijzondere) persoonsgegevens die zij onder zich hebben. Zij willen dan ook zekerstellen dat de ontvanger van de gegevens deze niet gebruikt voor andere doelen dan waarvoor de verstrekker ze heeft verzameld. Hier spelen de convenanten een rol, maar door de soms vage formuleringen zijn de verantwoordelijkheden en de vereiste doelbinding niet altijd helder. Met name is onduidelijk in hoeverre het doel waaraan de eerste gegevensverwerker is gebonden samenhangt met het doel waarmee de volgende verwerkers de gegevens gaan gebruiken. Dit leidt bij sommige partijen tot de stellingname: 'geen actie zonder overleg' (gazo). In convenanten wordt dit soms vertaald in 'third party rules', waarbij de verstrekker toestemming moet verlenen voor doorverstrekking. Met name wanneer de ontvanger de gegevens weer doorverstrekt aan een volgende partij, ontstaat het risico dat de relatie tussen gebruiksdoel en feitelijk gebruik verloren gaat. Een wettelijke regeling zou dit kunnen ondervangen, zo verwachten onze respondenten. De onderzoekers vragen zich af of een wettelijke regeling zo te construeren is dat deze complexe situatie afdoende wordt geregeld. In hoofdstuk 4 wordt op deze vraag ingegaan.

3.5.3.6 Kleuring van gegevens en betrouwbaarheid voor hergebruik

Verder blijkt uit het onderzoek dat het risico dat gegevens niet helemaal betrouwbaar zijn wanneer deze binnen een gegevensverzameling worden verrijkt met subjectieve informatie, een belangrijke wegingsfactor is. Dit leidt tot kleuring van de gegevens, die in een andere context en binnen een andere gegevensverzameling verkeerd of onjuist kan worden opgevat. Omgekeerd kunnen gegevens worden gefilterd alvorens zij worden verstrekt aan een andere partij, waardoor belangrijke elementen verloren kunnen gaan. Daarbij komt dat veel informatie bij toezichthouders naar haar aard 'zacht' is, en dus gevoelig voor interpretatie. Voor de onderzoekers is onduidelijk gebleven in hoeverre de Europese eis dat de mate van juistheid en betrouwbaarheid moet worden geregistreerd een oplossing biedt voor dit risico.

Overigens blijkt uit onze enquête dat op de werkvloer de kwaliteit van de ontvangen gegevens hoog wordt ingeschat. De vraag die dat bij de onderzoekers oproept is op basis waarvan die inschatting plaatsvindt.

1912170 01165

3.5.4 Enquête

Alle drie de geënquêteerde groepen (bestuurlijke toezichthouders, de opsporingsinstanties en vertegenwoordigers van burgers en bedrijven) blijken dezelfde top drie van belangen aan te geven: 1 Doelbinding, 2. Geheimhouding en 3. Privacy van het subject. Alleen bij ontvangers van gegevens bleken de baten voor de ontvanger hoger te scoren dan de privacy. Hieruit blijkt dat voldoen aan de eis van doelbinding, voldoen aan geheimhoudingsplichten, bescherming van de privacy en de eigen baten voor de organisatie als belangrijkste punten worden gezien met betrekking tot de gegevensuitwisseling. Drie van deze punten zijn normatief van aard: zowel de toezichthouders als de vertegenwoordigers van de rechtssubjecten vinden het naleven van de wettelijke kaders kennelijk zeer belangrijk. Opvallend was overigens de lage score van kosten in alle gevallen.

3.5.4.1 Behoefte aan een wettelijke regeling

Met betrekking tot deze vraag is er een opvallend verschil tussen de resultaten uit de casus, waarbinnen vooral met de 'werkvloer' is gecommuniceerd en de expertmeeting, waar meer beleidsmatige aspecten aan de orde kwamen. De experts waren van oordeel dat de bestaande wettelijke regels veel mogelijk maken, ook al is het ingewikkeld. Er is meer behoefte aan verduidelijking dan aan een nadere wettelijke regeling. Daarbij komt dat de Wbp al een algemeen kader biedt voor gevallen die nog niet in bijzondere wetgeving zijn geregeld.

In het veld lijkt in eerste instantie wel behoefte te bestaan aan meer duidelijkheid over de juridische basis bij het uitwisselen van gegevens. Het tot stand brengen van een algemene wettelijke regeling wordt daarbij door het merendeel van de betrokkenen als oplossing gezien, met uitzondering van de Belastingdienst die in de regeling in de Awr een afdoende juridisch kader ter beschikking heeft. De naar voren gebrachte argumenten voor een algemene regeling van de uitwisseling van toezichtgegevens zijn te verdelen in vier groepen die hiervoor al werden besproken: a) legitimering voor de uitwisseling (doelbinding en sfeerovergang), b) het creëren van een verplichting tot uitwisseling, c) het verkrijgen van een beter zicht op 'doorverstrekking' en doelbinding, en d) het verkrijgen van een beter zicht op de kwaliteit van de ontvangen gegevens.

1912170 01165

4. Naar een algemene regeling?

4.1 Inleiding

Uit het onderzoek blijkt dat de huidige wettelijke regeling inzake gegevensverstrekking in sommige opzichten onduidelijk, gefragmenteerd en lacuneus is en dat er daarom bij bepaalde partijen behoefte bestaat aan een brede(re) wettelijke regeling inzake de gegevensuitwisseling. Deze wettelijke regeling zou niet alleen legitimerend en faciliterend moeten zijn, maar tevens voldoende normerend. In dit hoofdstuk wordt bekeken of gelet op de voorgaande hoofdstukken wijzigingen of aanpassingen nodig zijn van de bestaande regelgeving.

De behoefte aan zo'n wettelijke regeling vloeit ook voort uit de als onwenselijk ervaren praktijk dat de gegevensuitwisseling vaak ad hoc plaatsvindt of op basis van convenanten die op belangrijke punten geen concrete en heldere afspraken bevatten of zelfs vrijwel inhoudsloos zijn. Dat brengt niet alleen mee dat men voor het verkrijgen van gegevens steeds weer afhankelijk is van de medewerking van degene die (namens de verstrekkende instantie) op een verzoek om gegevens reageert, maar ook dat deze medewerking eenvoudig beëindigd kan worden en in de praktijk ook soms beëindigd wordt.

Voor deze praktijk worden blijkens ons onderzoek twee oorzaken aangegeven. Ten eerste het feit dat de gegevensverstrekking soms onder verschillende wettelijke regimes valt die niet met elkaar sporen. Dat maakt het moeilijk om vast te stellen wat de (on)mogelijkheden voor gegevensuitwisseling zijn. Een tweede oorzaak ligt in de bepalingen uit de Wbp over doelbinding en het verstrekken van gegevens (met name de artikelen 7, 8 en 9). Deze bepalingen zijn vaag, zodat bij de toepassing ervan vaak onzekerheid over hun reikwijdte ontstaat. Dat maakt de regeling in de praktijk moeilijk hanteerbaar. Daar komt nog bij dat de Wbp in eerste instantie gericht is op de bescherming van burgers. Daardoor zijn veel potentiële gegevensverstrekkers bang dat ze door gegevens te verstrekken in strijd handelen met de Wbp. Het resultaat daarvan is dan dat de gevraagde gegevens geweigerd worden.

1912170 01165

Dat er behoefte bestaat aan een bredere wettelijke regeling, betekent echter niet dat zo'n regeling als panacee kan worden beschouwd. Bepaalde obstakels bij de gegevensuitwisseling zijn immers niet van juridische aard en laten zich dan ook niet wegnemen door een wettelijke regeling. Bovendien zijn er ook obstakels van meer algemeen juridische aard die zich niet goed laten oplossen in een specifieke regeling inzake de gegevensuitwisseling (zie hierover par. 4.7.2 en 4.7.3).

4.2 Regeling in de Awb?

Hoewel het opnemen van een regeling over gegevensuitwisseling in de Awb niet onmogelijk is, lijkt zo'n regeling in de Awb op verschillende bezwaren te stuiten. In de eerste plaats is de problematiek van de gegevensuitwisseling een veelomvattende, waarbij naast bestuursorganen ook natuurlijke personen en privaatrechtelijke organisaties (zonder openbaar gezag) betrokken zijn. Dat blijkt ook uit de Wbp, die zich tot al deze mogelijke actoren richt. Een (uitputtende) regeling in de Awb, die nu juist gericht is op het handelen van bestuursorganen, ligt daarom niet voor de hand. Wel zou er voor gekozen kunnen worden om in de Awb alleen die regels op te nemen die gelden voor toezichthouders. Dat zou echter alleen maar tot (verdere) versnippering van regelgeving leiden en juist niet tot vereenvoudiging en verduidelijking van regelgeving .

Bovendien is de problematiek ook zo veelvormig dat een wettelijke regeling waarschijnlijk voor een belangrijk deel in bijzondere wetgeving en daarop gebaseerde regelingen moet worden uitgewerkt (zie hierover uitgebreider in par. 4.6.5). Dat brengt mee dat zo'n algemene regeling niet goed bij de doelstellingen van de Awb past. De Awb is immers primair gericht op regeling van leerstukken en onderwerpen die geen nadere uitwerking in bijzondere wetgeving behoeven.

4.3 Regeling in een kaderwet?

Een andere mogelijkheid is de regeling over gegevensuitwisseling op te nemen in een kaderwet. Hierin kunnen dan de zaken geregeld worden die momenteel als belemmerend worden gezien voor de gegevensuitwisseling in het algemeen, zoals een duidelijke regeling inzake de bevoegdheid om gegevens uit te wisselen en wellicht ook de mogelijkheid om een plicht daartoe in het leven te roepen. Daarnaast moeten natuurlijk ook de aspecten die nu in de Wbp geregeld zijn in zo'n kaderwet worden opgenomen. Door het opnemen van onderwerpen in een kaderwet kan worden voorkomen dat verschillende, niet met elkaar te verenigen regimes over de gegevensverstrekking ontstaan. Bovendien kan een kaderwet, voor zover deze onderwerpen regelt die gemeenschappelijk zijn aan de verschillende deelgebieden, aan de kenbaarheid en inzichtelijkheid van de regels bijdragen. Tegelijkertijd laat een kaderwet ruimte om onderwerpen die specifiek voor een bepaald beleidsterrein gelden, in bijzondere wetgeving en daarop gebaseerde (lagere) regelingen te regelen.

4.4 Een nieuwe kaderwet of een omgebouwde Wbp?

Op zich is het mogelijk om – los van de bestaande Wbp – een nieuwe kaderwet in het leven te roepen. In dat geval kunnen echter weer afbakeningsproblemen ontstaan tussen deze nieuwe wet en de Wbp. Het ligt daarom wellicht meer voor de hand om de Wbp als uitgangspunt te nemen en deze wet om te bouwen tot een brede wet inzake de gegevensverstrekking. De Wbp heeft immers momenteel al min of meer het karakter van een kaderwet (zij het met een beperkte en eenzijdige invalshoek), en de onderwerpen die er in geregeld worden, zullen ook in de brede kaderwet geregeld moeten worden. Als de Wbp wordt om- of uitgebouwd tot een brede kaderwet inzake de gegevensverstrekking, is het zaak dat

1912170 01165

ook de verhouding tot de Wpg en de Wjsg wordt bezien. Momenteel fungeren deze wetten, voor zover het om de verwerking van strafrechtelijke persoonsgegevens gaat, als lex specialis ten opzichte van de Wbp. De vraag is of de uitwisseling van strafrechtelijke persoonsgegevens nog steeds een apart wettelijke regime rechtvaardigt of dat deze gegevens ook in een brede kaderwet geregeld kunnen of moeten worden. Indien de huidige Wbp wordt omgebouwd tot een brede(re) kaderwet ligt het voor de hand deze wet een andere naam te geven die meer recht doet aan het uitgangspunt van gegevensverstrekking.

4.5 De rol van convenanten

Dat de gegevensverstrekking op basis van convenanten in het verleden vaak niet tot de gewenste resultaten heeft geleid, heeft vooral te maken met het feit dat deze convenanten vaak nauwelijks inhoudelijke criteria bevatten, met name op het punt van de doelbinding. Zelfs in het meest uitgewerkte convenant (Ketendossier Vuurwerk) wordt daarover niet veel meer bepaald dan wat al uit de Wbp voortvloeit. Daardoor is het vaak onduidelijk in hoeverre men over en weer bevoegd is tot het uitwisselen van gegevens.

De vraag is echter of het mogelijk is deze onduidelijkheden te vermijden door in de convenanten meer concrete en precieze criteria vast te leggen met betrekking tot informatie-uitwisseling. Het antwoord op die vraag luidt vermoedelijk ontkennend. Het onderliggende probleem is dat de Wbp op dit punt te weinig houvast geeft aan betrokken partijen, met als gevolg dat het voor hen vaak onduidelijk is welke informatie zij met wie kunnen uitwisselen. Maar zelfs als in convenanten concreter zou worden vastgelegd welke informatie wordt uitgewisseld, blijft nog steeds de vraag bestaan of de criteria in een dergelijk convenant in overeenstemming zijn met de wet. Het is daarom niet realistisch te verwachten dat convenanten meer concrete criteria zullen bevatten, als de wet zelf (in een kaderwet of in sectorale wetgeving) ook niet voldoende concrete criteria bevat.

Convenanten lenen zich daarom in het bestaande systeem niet goed als inhoudelijke basis voor de gegevensuitwisseling. Het is echter wel mogelijk dat convenanten worden afgesloten om praktische en procedurele afspraken te maken tussen de gegevensverstrekker en ontvanger. De kans is dan groter dat de gegevensverstrekking effectief en soepel verloopt.

4.6 Problemen met betrekking tot de eis van doelbinding

In de Wbp ligt een sterke nadruk op doelbinding. Artikel 7 regelt dit voor de verzameling van persoonsgegevens, artikel 11 voor de verwerking, terwijl artikel 9 vereist dat persoonsgegevens niet worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen.[134] Daarbij speelt blijkens het tweede lid van artikel 9, aanhef en onder a, de vraag of er voldoende verwantschap bestaat tussen het doel van de beoogde verwerking en het doel waarvoor de gegevens verkregen zijn een belangrijke rol. Dat laatste criterium komt er op neer dat als een toezichthouder informatie krijgt van een andere toezichthouder, de ontvangende toezichthouder die informatie alleen kan gebruiken als de verstrekkende toezichthouder die informatie heeft verzameld met het oog op een doel dat *voldoende verwantschap* vertoont met het doel waar de ontvangende toezichthouder de informatie voor wil gaan gebruiken. In dit rapport is dit verschijnsel ook wel aangeduid als dubbele doelbinding.

134 Zie nader paragraaf 2.4.

1912170 01165

4.6.1 Verwantschap tussen doelen

Tijdens het onderzoek is gebleken dat de doelbinding die artikel 9 Wbp oplegt voor nogal wat problemen zorgt. In de eerste plaats omdat de norm van artikel 9 moeilijk hanteerbaar is. Voor veel betrokkenen is vaak niet duidelijk of bepaalde informatie die verzameld is met het oog op doel A, verwerkt mag worden met het oog op doel B.[135] Artikel 9 Wbp bepaalt dat gegevens niet mogen worden verwerkt op een wijze die onverenigbaar is met het doel waarvoor die gegevens zijn verkregen. Uit artikel 9, tweede lid aanhef en onder a blijkt, dat dit onder andere vastgesteld dient te worden aan de hand van de vraag of er tussen de twee doelen voldoende verwantschap bestaat. Deze vraag is echter vaak moeilijk met zekerheid te beantwoorden. Dit leidt er toe dat veel partijen die over persoonsgegevens beschikken bij twijfel (en die ontstaat dus al heel snel) over de vraag of uitwisseling toegestaan is, dan maar afzien van uitwisseling.

Daarnaast veroorzaakt de doelbinding van artikel 9 het praktische probleem dat niet altijd duidelijk is met het oog op welk doel bepaalde gegevens in het verleden verzameld zijn. Daardoor is niet altijd duidelijk of deze gegevens verzameld zijn met het oog op een doel dat voldoende verwantschap vertoont met het doel dat nagestreefd wordt door een eventuele volgende verwerker van gegevens.
Deze twee factoren werken in de hand dat het moeilijk vast te stellen is *wanneer* gegevens aan andere toezichthouders verstrekt mogen worden en aan *welke* andere toezichthouders deze gegevens verstrekt mogen worden.

Dit probleem zou op drie manieren opgelost kunnen worden. De eerste mogelijkheid zou zijn het criterium van artikel 9 (voldoende verwantschap) helderder en concreter te formuleren zodat een maatstaf bestaat die voor de praktijk beter hanteerbaarder is. De tweede mogelijkheid is het laten vallen van de eis van de dubbele doelbinding zoals die nu in de wet geformuleerd is. De derde mogelijkheid is in een nadere regeling specifiek voor een bepaald beleidsterrein op te sommen welke gegevens aan welke toezichthouders verstrekt mogen worden.

4.6.2 Een concreet, direct toepasbaar criterium

De eerste mogelijke aanpassing, een heldere en meer concrete formulering van het criterium van artikel 9, is moeilijk haalbaar. De beleidsterreinen, soorten gegevens en betrokken actoren waar de gegevensverwerking betrekking op heeft, zijn dermate divers, dat het niet of nauwelijks mogelijk is de norm van artikel 9 zo te herformuleren dat deze én een algemene regeling geeft én zodanig concreet is hij onmiddellijk toepasbaar is in de praktijk.

Het is in dit kader verhelderend om te wijzen op het reeds in paragraaf 2.5.3 besproken wetsvoorstel om artikel 23 Wbp te wijzigen. Dat artikel heeft weliswaar betrekking op de verwerking van bijzondere persoonsgegevens als bedoeld in artikel 16, maar kan, gezien de aard van de hier besproken problematiek, toch als voorbeeld dienen. Dit wetsvoorstel behelsde een wijziging van artikel 23 Wbp ten aanzien van de verwerking van bijzondere gegevens door toezichthouders.[136] Het voorstel voorzag in de mogelijkheid dat ombudsmannen, accountantsorganisaties en toezichthouders deze gegevens kunnen verwerken als dit noodzakelijk is met het oog op een zwaarwegend algemeen belang ter uitvoering van de hun wettelijk opgedragen taken. Als grondslag voor deze bepaling diende artikel 8, vierde lid van de Privacyrichtlijn, waarin lidstaten de mogelijkheid wordt geboden om afwijkingen van het verbod op verwerken van bijzondere persoonsgegevens toe te staan, onder de voorwaarde dat de verwerking geschiedt om redenen van zwaarwegend algemeen belang en dat er bovendien passende waarborgen worden vastgesteld. Zoals

135 Zie ook *supra*, paragraaf 3.5.3.5.
136 *Kamerstukken II* 2008/09, 31 841, nr. 2.

1912170 01165

besproken in Hoofdstuk 2 was het volgens de Raad van State niet mogelijk om een eenduidig criterium te formuleren zodat voor al deze situaties verzekerd zou zijn dat voldaan werd aan de maatstaf van 'zwaarwegend algemeen belang', mede omdat ombudsmannen, toezichthouders en accountants-organisaties te verschillend zijn om in een eenduidig criterium te vatten. De minister heeft vervolgens opgemerkt dat wellicht op termijn in sectorale wetgeving alsnog een uitzonderingsgrond zal worden opgenomen voor toezichthouders 'voor concreet bepaalde taken'.[137]

Net zomin als het mogelijk is om voor de hierboven geschetste situaties een eenduidig criterium te geven is het mogelijk om de eis van artikel 9 Wbp, dat er voldoende verwantschap moet bestaan, in een criterium te vangen dat recht doet aan de diversiteit van gegevens en omstandigheden die zich kunnen voordoen, maar tegelijkertijd ook voldoende houvast geeft om voor de praktijk hanteerbaar te zijn. Het gevolg hiervan is echter wel dat steeds in concrete gevallen moet worden gezocht naar de mate van verwantschap, hetgeen belemmerend werkt op de uitwisseling.

4.6.3 Het vervallen van het element van verwantschap

De tweede mogelijke aanpassing is het laten vallen van het criterium zoals dat in artikel 9, tweede lid aanhef en onder a geformuleerd is. Dit criterium stelt de vraag of twee doelen onverenigbaar zijn, mede afhankelijk van de vraag of er wel of niet 'voldoende verwantschap' bestaat tussen die twee doelen. De eerste vraag die zich dan voordoet is of dit, gelet op hogere rechtsnormen, wel mogelijk is. Artikel 10 van de Grondwet verzet zich daar niet tegen. Het EVRM en de EU Privacyrichtlijn verzetten zich daar evenmin tegen. Artikel 6 eerste lid onder b van de Privacyrichtlijn regelt dat persoonsgegevens niet worden verwerkt op een wijze die onverenigbaar is met het doel waarvoor ze zijn verzameld. Ook in de nieuwe Privacyverordening is het criterium dat de verwerking niet onverenigbaar mag zijn met de oorspronkelijke doelen.[138] Het criterium van het tweede lid van artikel 9, aanhef en onder a Wbp, dat de doelen onderling voldoende verwantschap vertonen, gaat naar ons oordeel veel verder dan nodig is.

Uit artikel 9, eerste lid Wbp vloeit namelijk voort dat gegevens niet mogen worden verstrekt op een wijze die 'onverenigbaar' is met de doeleinden waarvoor ze zijn verkregen. De gegevensverstrekking moet dus altijd op deze '(on)verenigbaarheid' worden getoetst, en wel aan de hand van - in elk geval - de in het tweede lid van artikel 9 Wbp genoemde factoren. Het element van de verwantschap dat in het tweede lid van artikel 9 Wbp als eerste wordt opgesomd, is een van deze mogelijke factoren om de verenigbaarheid te beoordelen. Aangezien deze factor in de praktijk vaak tot interpretatie- en kwalificatieproblemen leidt, ligt schrapping voor de hand. Te meer, nu in de memorie van toelichting staat dat de opsomming van factoren niet limitatief is en dat geen van de genoemde factoren op zichzelf van doorslaggevende betekenis is.[139] Het schrappen van de factor 'verwantschap' betekent dus wel dat een belemmering bij de gegevensverstrekking wordt weggenomen, maar niet dat niet langer op een goede wijze beoordeeld kan worden of de gegevensverstrekking 'verenigbaar' is in de zin van het eerste lid. Voor een 'function creep' zijn we dan ook niet bang. Ook zijn we van mening dat de Afdeling bestuursrechtspraak paragraaf 2.4.4 genoemde uitspraak, waarin gebruik van RDW-gegevens in het kader van optreden tegen straatprostitutie ontoelaatbaar werd geacht vanwege gebrek aan verwantschap, niet tot een andere uitspraak zou zijn

137 Ibid., p. 3.

138 In het voorstel voor een EU-Privacyverordening (COM (2012) 11 final) wordt op dit punt geregeld dat als de doelen voor verwerking niet verenigbaar zijn, dat slechts is toegestaan als er een basis is in de wet en als de verwerking (voor zover hier relevant) noodzakelijk is om te voldoen aan een wettelijke plicht of als de verwerking noodzakelijk is met het oog op het uitvoeren van een publieke taak (artikel 6, vierde lid).

139 *Kamerstukken II* 1997/98, 25892, nr. 3, p. 90

1912170 01165

gekomen als de factor van 'verwantschap' niet zou bestaan.[140] De onverenigbaarheid zou ook op grond van een van de andere factoren aangenomen kunnen worden.

Als het in artikel 9, tweede lid, Wbp genoemde element van verwantschap van doelen voor toezichthouders zou komen te vervallen, zou dat de eisen die de Wbp op dit punt stelt, voor de praktijk beter hanteerbaar maken.

Verschillende wetten staan overigens in een aantal gevallen al toe dat gegevens worden gebruikt voor een doel dat geen verwantschap vertoont met het doel waarvoor die gegevens zijn verzameld. Artikel 3, derde lid, Wpg regelt bijvoorbeeld dat politiegegevens kunnen worden verwerkt voor een ander doel dan waarvoor deze zijn verkregen, zij het dat dit een uitdrukkelijke wettelijke grondslag vereist.[141] De Wwb verplicht in artikel 64 een aantal bestuursorganen informatie te verschaffen aan het college van B&W met het oog op de uitvoering van deze wet. Het gaat dan onder andere om informatie van de Belastingdienst, het College zorgverzekeringen, de Nederlandse zorgautoriteit en de korpschef of de bevelhebber van de Koninklijke marechaussee in de zin van de Vreemdelingenwet. Van verwantschap tussen het doel waarvoor deze instanties de betreffende informatie hebben verzameld en het doel waarvoor het college van B&W deze informatie wil gaan gebruiken, is nauwelijks sprake. Vergelijk ook artikel 27 van de Wet Bibob.

De vraag is kortom of de meerwaarde voor de bescherming van de privacy die de eis van de dubbele doelbinding met zich brengt, opweegt tegen de problemen die deze eis veroorzaakt bij gegevensuitwisseling tussen toezichthouders. Dat is echter uiteindelijk geen juridische, maar een politieke vraag.

Wel moet worden bedacht dat de waarborgen die artikel 6 EVRM verbindt aan het opleggen van bestraffende sancties aanleiding geven tot extra alertheid. Met name als het gaat om de cautieplicht, wanneer gegevens worden verzameld door het stellen van vragen en de antwoorden niet worden ondersteund door andere bewijsmiddelen.[142] Informatie die vrijwillig verstrekt is aan een toezichthouder die geen cautie heeft gegeven, zal in beginsel niet door een volgende instantie gebruikt mogen worden, als deze laatste de informatie wil gebruiken met het oog op het opleggen van een bestraffende sanctie. Het niet in acht nemen van een fundamentele waarborg als het zwijgrecht bij het verzamelen van bewijs, leidt er immers toe dat het bewijs als onrechtmatig verkregen wordt beschouwd en dient te worden uitgesloten.[143]

4.6.5 Specifieke opsomming van gevallen waarin verdere verwerking is toegestaan

Het probleem met de dubbele doelbinding van artikel 9 is, zoals gezegd, dat vaak niet duidelijk is of gegevensverwerking in strijd is met deze norm. Een derde mogelijkheid om dit probleem te verkleinen is door in bijzondere wetgeving zoveel mogelijk via een opsomming aan te geven welke gegevens door welke organen uitgewisseld mogen worden. Een opsomming stelt dan buiten twijfel dat de in de wet genoemde vormen van verwerking zijn toegestaan, ervan uit gaande dat de wetgever bij het opsommen hogere rechtsnormen in acht heeft genomen.

Een voorbeeld hiervan is artikel 64 Wwb. Dat artikel bepaalt dat het UWV, de Sociale verzekeringsbank, de Belastingdienst en een aantal andere instanties verplicht zijn gegevens te verstrekken aan het college

140 Afdeling bestuursrechtspraak 12 mei 2004, *LJN* AO9207, *JB* 2004, 251, m. nt. G. Overkleeft-Verburg.
141 In de EU-Privacyverordening wordt deze eis ook zo gesteld. Zie ook *supra*, hoofdstuk 2.
142 EHRM 3 mei 2001, nr. 31827/96, *LJN* AN6999, *NJ* 2003/354 m.nt. Schalken (*JB/Zwitserland*) en EHRM 17 december 1996, nr. 19187/91, *LJN* ZB6862, *NJ* 1997/699 m.nt. Knigge (*Saunders/Verenigd Koninkrijk*).
143 CRvB 16 november 2011. *LJN* BU6392, *AB* 2012, 39 m. nt. R. Stijnen, *JB* 2012, 18 m. nt. C.L.G.F.H. Albers en artikel 359a, eerste lid, sub c, Sv.

1912170 01165

van B&W als die gegevens noodzakelijk zijn voor het uitvoeren van de Wwb. Een soortgelijk voorbeeld is te vinden in artikel 27 Wet Bibob. Een dergelijke opsomming hoeft overigens niet bij wet in formele zin plaats te vinden. De in paragraaf 4.3 besproken kaderwet zou het bijvoorbeeld mogelijk kunnen maken om bij AMvB of bij ministeriële regeling per sector een opsomming te geven van het soort gegevens dat uitgewisseld kan worden tussen bepaalde toezichthouders. Op sommige plaatsen gebeurt dat nu al, zoals de Uitvoeringsregeling Awr laat zien.

Het eerste lid van artikel 18 Wpg maakt het ook mogelijk dat bij of krachtens AMvB personen en instanties kunnen worden aangewezen aan wie of waaraan, met het oog op een zwaarwegend algemeen belang, politiegegevens worden of kunnen worden verstrekt ter uitvoering van de bij of krachtens die algemene maatregel van bestuur aan te geven taak. Op grond van deze bevoegdheid is het Besluit Politiegegevens vastgesteld. Artikel 4:2 lid 1 Besluit Politiegegevens legt vast dat bepaalde gegevens kunnen worden verstrekt aan een aantal in het eerste lid met name genoemde instellingen zoals onder andere het Waarborgfonds Motorverkeer, de Halt-bureaus, de Raad voor de Kinderbescherming, en de Algemene Inspectiedienst van het Ministerie van LNV.

Een nadeel van deze oplossing is echter dat het risico bestaat dat een specifieke opsomming verstarrend gaat werken. Omdat het vaak niet mogelijk is voor een regelgever om alle toekomstige gevallen te overzien, zal een dergelijke opsomming meestal niet limitatief bedoeld zijn, zoals de in paragraaf 2.6.1 besproken Uitvoeringsregeling Awr laat zien. De lijst met ontheffingen op grond van deze regeling is lang en wordt voortdurend aangepast. Het is echter niet uit te sluiten dat deze opsomming in de praktijk wel als zodanig beschouwd zal worden.

Een ander nadeel van deze oplossing is dat, als de wetgever een dergelijke opsomming achterwege laat, men teruggeworpen is op de moeilijker hanteerbare norm van artikel 9 Wbp.

4.7 Andere problemen

4.7.1 Een wettelijke verplichting tot gegevensverstrekking?

Uit het onderzoek is gebleken dat er in een enkel geval niet alleen behoefte bestaat aan een wettelijke bevoegdheid, maar ook aan een verplichting om gegevens te verstrekken. Dat is met name het geval als er – ondanks een bevoegdheid daartoe – sprake is van onwil om gegevens te verstrekken. De vraag is echter of dit moet leiden tot een algemene verplichting om gegevens te verstrekken. Hoewel sommigen zo'n verplichting wensen, gaat deze wellicht te ver. Vooral, omdat van onwil lang niet overal sprake is. Het ligt daarom niet voor de hand een verplichting in een eventuele kaderwet zelf op te nemen, omdat die zo'n algemene strekking zou hebben. Wel zou in een kaderwet de bevoegdheid opgenomen kunnen worden om 'bij of krachtens de wet' zo'n verplichting in het leven te roepen. Een eventuele verplichting zou dan in een bijzondere wet of een daarop gebaseerde AMvB of ministeriële regeling gestalte kunnen krijgen.

Momenteel kennen zowel de Wwb (artikel 64) als de Wet Bibob (artikel 27) een verplichting voor bepaalde bestuursorganen om gegevens te verstrekken. Hoofdregel is dat gegevens worden verstrekt aan de overheidsorganen die in de wet worden genoemd. Verstrekking kan echter worden geweigerd om zwaarwegende redenen. Hiervan moet rekenschap worden afgelegd in een nadere motivering van de beslissing tot weigering. Een dergelijke regeling doet enerzijds recht aan het streven van ontvangende overheidsinstanties om effectief en efficiënt op te treden door gebruikmaking van reeds bij de overheid beschikbare gegevens. Anderzijds wordt ook recht gedaan aan het organisatiebelang van de verstrekkende

1912170 01165

instantie door de mogelijkheid open te laten dat – mits goed gemotiveerd – gegevens niet worden verstrekt.

4.7.2 De kwaliteit van de te verstrekken of verstrekte gegevens

Een niet te onderschatten probleem bij de gegevensverstrekking is dat vaak niet bij voorbaat duidelijk is in hoeverre de te verstrekken of verstrekte gegevens juist, betrouwbaar en volledig zijn. Met name is niet altijd duidelijk of de gegevens 'blote' feiten betreffen of feiten die gekleurd zijn, doordat degene die ze verstrekt er een bepaalde kwalificatie aan gegeven heeft. In de nieuw voorgestelde EU Privacyrichtlijn wordt geëist dat zoveel mogelijk wordt onderscheiden naar de graad van juistheid en betrouwbaarheid van de gegevens. De lidstaten moeten erop toezien dat persoonsgegevens die op feiten zijn gebaseerd, voor zover mogelijk, worden onderscheiden van persoonsgegevens die op een persoonlijke oordeel zijn gebaseerd.[144]

De vraag is of in een kaderwet aan dit probleem het hoofd kan worden geboden. Voorop staat natuurlijk dat zowel de verstrekker van gegevens als degene die de gegevens ontvangt en gebruikt zich ervan moet vergewissen dat de gegevens feitelijk juist zijn en volledig. Dat vloeit al uit artikel 3:2 Awb en uit het algemene zorgvuldigheidsbeginsel voort. Aangezien de zorgvuldigheidsnorm van artikel 3:2 Awb zich – op grond van artikel 3:1, tweede lid, Awb – ook uitstrekt over feitelijke handelingen van bestuursorganen, zal deze norm vaak toereikend zijn. Voor zover het om organen gaat waarvan de handelingen – gelet op artikel 1:6 Awb – niet onder de reikwijdte van de Awb vallen, kan worden teruggevallen op het algemene zorgvuldigheidsbeginsel. Wellicht kunnen in een kaderwet nadere eisen aan deze algemene zorgvuldigheidsnorm worden ontleend. Deze zouden dan min of meer in de lijn van artikel 6 Wbp, artikel 4 Wpg of artikel 3 Wjsg opgesteld kunnen worden. De vraag is wel of daarmee veel gewonnen is, omdat de in deze artikelen opgenomen eisen nogal vanzelfsprekend zijn.

4.7.3 De interpretatie van de verstrekte gegevens

In het verlengde van het voorgaande probleem ligt dat van de interpretatie van de verstrekte gegevens. Wie gegevens gebruikt in een bepaalde toezichtcontext zal deze kwalificeren. In deze kwalificatie schuilt onvermijdelijk een subjectief element dat nu juist bij de gegevensverstrekking afwezig zou moeten zijn. Belangrijk is immers dat degene die de gegevens ontvangt en gebruikt, deze 'schoon' kan gebruiken. De moeilijkheid is echter dat de vaststelling van feiten vaak ongemerkt overloopt in de kwalificatie van feiten. De vraag is dan ook hoe voorkomen kan worden dat gegevens verstrekt worden die gekleurd zijn en of daarover in een kaderwet normen opgenomen kunnen en moeten worden. Ook hier zal het weer op de te betrachten zorgvuldigheid aankomen. In eerste instantie van degene die gegevens verstrekt (het gaat immers over zijn gegevens), maar vervolgens ook van de ontvanger van deze gegevens (die erop toe moet zien dat de verstrekte gegevens geen oordelen bevatten en anders om nadere informatie zou moeten verzoeken).

144 Zie paragraaf 2.3.8.

1912170 01165

5. Conclusies en aanbevelingen

5.1 Inleiding

In het rapport iOverheid schetst de WRR een afwegingskader voor het maken van beleidskeuzes ten aanzien van digitalisering van informatie en het gebruik ervan. De beoordelingsmaatstaven zijn ondergebracht in drie groepen, die de WRR aanduidt als stuwende, verankerende en procesmatige beginselen. De stuwende beginselen zijn verbonden met de drive van de overheid om ICT in tal van domeinen in te zetten en zij staan in het teken van verbetering en kwaliteitswinst. De WRR noemt als veelvoorkomende stuwende beginselen: veiligheid en het koppel effectiviteit en efficiëntie. De verankerende beginselen staan voor het waarborgen van vrijheden, het in kaart brengen van 'stille verliezen' bij voortgaande digitalisering en voor het vrijwaren van de autonomie van het individu. De verankerende beginselen vormen een tegenwicht voor de stuwende beginselen. Privacy en de keuzevrijheid van het individu zijn belangrijke verankerende beginselen. Om tot een uitgebalanceerde applicatie of beslissing over de inzet van ICT te komen, moeten beginselen ten slotte tegen elkaar worden afgewogen, aldus de WRR. De procesmatige beginselen staan voor de procedurele omlijsting die het mogelijk maakt dat de stuwende en verankerende beginselen op een zorgvuldige manier gewogen worden. Deze afwegingsprocessen moeten vooral toetsbaar en inzichtelijk zijn, vandaar dat transparantie en accountability gelden als belangrijke beginselen bij de afweging.

Dit beoordelingskader heeft goede diensten bewezen in dit onderzoek, dat gericht was op

I. de vraag met welke belangen rekening moet worden gehouden bij de verstrekking van toezichtgegevens tussen toezichthouders onderling en tussen toezichthouders enerzijds en het OM, de politie en de buitengewoon opsporingsambtenaren anderzijds, en

1912170 01165

II. de vraag in hoeverre het gewenst en juridisch mogelijk is om voor het verstrekken van toezichtgegevens tussen genoemde partijen een algemene regeling in de Algemene wet bestuursrecht en/of eventuele andere wetten op te nemen.

Deze twee hoofdvragen zijn onderzocht aan de hand van acht deelvragen:

1. *Welke belangen spelen een rol bij de afweging of al dan niet sprake kan zijn van het uitwisselen van gegevens?*
2. *Is er mogelijk sprake van nog andere belanghebbenden dan de onder vraag 1 genoemden bij het verstrekken van toezichtgegevens?*
3. *Onder welke condities kunnen de vastgestelde belangen met elkaar in botsing komen?*
4. *Hoe worden de (potentieel botsende) belangen juridisch gelabeld?*
5. *Zijn er belangen bij die juridisch (nog) niet erkend zijn?*
6. *Welke van de vastgestelde juridisch erkende belangen (rechten) hebben voorrang op andere vastgestelde rechten en waarom?*
7. *Is een algemene voorziening in de Awb of in andere wetten gewenst en juridisch mogelijk?*
8. *Wat zijn mogelijke neveneffecten van een algemene voorziening?*

Om de belangen die spelen rond gegevensuitwisseling tussen toezichthouders en de weging ervan te inventariseren is gekozen voor een aanpak door middel van bestudering van de relevante stukken, een quickscan, casus, gesprekken met ervaringsdeskundigen, een expertmeeting en een internetenquête onder ervaringsdeskundigen op de werkvloer ten behoeve van de Multicriteria-analyse. In paragraaf 1.3 en 3.1 zijn de onderzoeksmethoden nader toegelicht.

De onderzoekers benadrukken dat de onderzoeksmethodiek gericht was op het verkrijgen van kwalitatieve gegevens ten aanzien van de belangen die een rol spelen bij gegevensuitwisseling. De groep geënquêteerden was te klein was om kwantitatieve conclusies te trekken. De verwachting is echter gerechtvaardigd dat onderzoek onder een grotere groep de meest eenduidige uitkomsten uit de enquête, zoals hieronder aangegeven, niet wezenlijk zou hebben veranderd.

5.2 Deelvragen 1 en 2: de bij de uitwisseling van toezichtgegevens betrokken belangen en belanghebbenden

5.2.1 Uitgangspunten inventarisatie

Ten aanzien van deze vragen was een nadere inventarisatie nodig van de belangen die hier in het geding kunnen zijn. De onderzoekers hebben een quickscan uitgevoerd op enkele vormen van samenwerking en zijn nagegaan welke belangen een rol (kunnen) spelen bij de wettelijk geregelde gegevensuitwisseling. Op basis van deze quickscan is een lijst van mogelijke belangen samengesteld die, door middel van open vragen aan betrokkenen, is aangevuld ten behoeve van de te houden kwalitatieve enquête (zie verder paragraaf 3.1 voor een uiteenzetting van de aanpak).

Uit het onderzoek blijkt dat gaat het om een uiteenlopend palet van belanghebbenden. In de eerste plaats zijn dat de in deelvraag 1 genoemde inspectie- en opsporingsdiensten, de toezichthoudende functionarissen en opsporingsambtenaren. In de tweede plaats zijn dat de in deelvraag 2 bedoelde andere belanghebbenden, te weten onder toezicht gestelde burgers en bedrijven en hun vertegenwoordigers. Deze belanghebbenden hebben ieder vanuit hun eigen positie belang bij de uitwisseling

1912170 01165

van gegevens. In paragraaf 3.2, 3.3 en 3.4, alsmede in bijlage 7.2 zijn de gedetailleerde resultaten te vinden van de inventarisatie van belangen.

Het antwoord op de vraag welke belangen een rol spelen hangt af van de soort gegevens die zullen worden uitgewisseld. Zoals in hoofdstuk 2 is uiteen gezet kunnen toezichtgegevens worden onderverdeeld in persoonsgegevens, bedrijfs- of fabricagegegevens en overige gegevens. Voor laatstgenoemde categorie bestaan geen belemmeringen voor de uitwisseling: veelal wordt aangenomen dat uitwisseling bijdraagt aan de efficiency en de effectiviteit van het overheidsoptreden, terwijl er geen belangen zijn die pleiten tegen uitwisseling.

Voor de eerste twee categorieën geldt dat het belang bij privacy c.q. bescherming van bedrijfsgegevens wettelijk worden gewaarborgd. Het behoeft geen betoog dat de belangen groter zijn als de gegevens bedrijfs- of fabricagegegevens of persoonsgegevens betreffen. De laatste categorie is het meest gevoelig, hetgeen ook blijkt uit de mate van bescherming die deze categorie ten deel valt. De aard van de uit te wisselen gegevens en het gewicht van de betrokken belangen hangen aldus sterk samen.

5.2.2 Resultaat inventarisatie

Aan de kant van de overheidsinstantie zijn in dit onderzoek onderscheiden de bestuurlijke toezichthouders en de opsporingsinstanties. Onder bestuurlijke toezichthouders vallen inspecties en andere toezichthouders, uitvoeringsorganisaties, decentrale besturen, en het College bescherming persoonsgegevens. Ook de Belastingdienst is gerekend onder de bestuurlijke toezichthouders. Hoewel de Belastingdienst primair is belast met het heffen en innen van rijksbelastingen houdt de dienst ook toezicht op de naleving van de belastingwetgeving. Onder de opsporingsinstanties zijn gerekend, OM, politie en buitengewone opsporingsdiensten als de FIOD, SIOD, etc.

Verder kan enig onderscheid worden onderkend in belangen van de gegevensverstrekker en die van de gegevensontvanger. Bij verstrekkers van de gegevens is de zorg voor wat er met de gegevens gebeurt, wie daarvoor verantwoordelijk is en wat de risico's zijn als het misgaat bij de gegevensontvanger van belang. Een overweging daarbij is dat de burgers die gegevens verstrekken erop moeten kunnen vertrouwen dat hun gegevens in veilige handen zijn bij het overheidsorgaan waaraan zij ze hebben gegeven. Wettelijke geheimhoudingsplichten spelen daarop in (zie hierover paragraaf 2.6 en hierna paragraaf 5.2.3). De bescherming van de belangen van de burger wordt daarbij ook als het belang van de eigen organisatie gezien, omdat daarmee de informatiestroom open wordt gehouden. Dit blijkt met name als we de ontvangers van gegevens onder de loep nemen. Bij de ontvangers ontbreekt de directe relatie tot het subject, en leven de noties geheimhouding, bescherming van de privacy en doelbinding minder sterk bij de verwerking van gegevens. Voor de ontvanger nemen de resultaten die met de verkregen gegevens kunnen worden gerealiseerd een prominente plaats in. In dit onderzoek is dit belang aangeduid als de eigen baten voor de organisatie. Kosten in termen van geld of moeite bij het verstrekken of ontvangen van gegevens speelde een kleine rol voor de bestuurlijke organisaties en de opsporingsdiensten, zo blijkt uit de internetenquête. Toch speelt dit meer praktisch georiënteerde belang wel een rol bij gegevensuitwisseling, zoals blijkt uit paragraaf 3.2.2.6, 3.2.3.7 (gemeenschappelijke databank), 3.3.1.

In de internetenquête zijn op basis van de gemaakte inventarisatie als belangen opgenomen: doelbinding, privacy subject, privacy derde, geheimhouding, kosten verstrekken gegevens, eigen baten (bij verstrekken of ontvangen, wederkerigheid). De bestuurlijke toezichthouders c.q. uitvoeringsorganisaties noemen nog enkele belangen: het algemeen belang, het belang van de juistheid van de

1912170 01165

gegevens en het risico van het niet of niet correct ontvangen van de toezichtgegevens. Bij de respondenten uit de opsporing werd het belang van een overheidsbreed effectief optreden genoemd, het gemeenschappelijk overheidsbelang en het organisatieoverstijgend belang.

Burgers en bedrijven hebben als belang dat hun gegevens vertrouwelijk worden behandeld. Bedrijfs- en fabricagegegevens mogen niet zomaar bekend kunnen worden aan concurrenten. Persoonsgegevens moeten slechts in handen komen van toezichthouders en opsporingsdiensten voor zover dat noodzakelijk is voor de taakuitoefening en voor zover andere middelen niet toereikend zijn.

De groep vertegenwoordigers van burgers en bedrijven omvat in het kader van dit onderzoek met name advocaten en belastingadviseurs. Bij de inventarisatie bleek dat het met name gaat om: doelbinding, privacy subject, privacy van een derde, geheimhouding van de toezichtgegevens, de kosten van het verstrekken (moeite en geld) en de baten voor het subject (bijvoorbeeld verminderen administratieve lasten), en tot slot de baten voor de vertegenwoordiger (vermindering administratieve lasten).

De vertegenwoordigers hebben enerzijds belangen die parallel lopen aan die van hun cliënten: vertrouwelijke behandeling van gegevens, bescherming van bedrijfs- en fabricagegegevens en van persoonsgegevens. Daarnaast blijkt uit het onderzoek dat zij ook transparantie ten aanzien van de uitwisseling van gegevens belangrijk vinden, zodat duidelijk is wat er met aangeleverde gegevens gebeurt of kan gebeuren en welke andere overheidsinstantie deze gegevens in handen heeft gekregen of kan krijgen. De mogelijke baten of voordelen die een cliënt kan hebben van gegevensuitwisseling doordat administratieve lasten verminderen, kan wel als een belang worden aangemerkt, maar dit staat niet hoog op de lijst van de vertegenwoordigers. Daarnaast hebben de vertegenwoordigers ook een eigen belang dat de gegevensverzameling en –verwerking zorgvuldig gebeurt. Zij willen niet het risico lopen dat zij in strijd met de belangen c.q. wettelijke plichten van hun cliënt of in strijd met de eigen beroepsregels gegevens verstrekken. Zij lopen immers het risico aansprakelijk te worden gesteld. De vertegenwoordigers komen daarnaast op voor de privacy van derden. De procesmatige beginselen spelen voor deze groep aldus met name een rol.

5.2.3 Samenvatting belangen

Private belangen zijn de vertrouwelijke behandeling van gegevens (geheimhouding), de bescherming van bedrijfs- en fabricagegegevens en de bescherming van persoonsgegevens (ook van derden), de transparantie ten aanzien van de uitwisseling van gegevens, de mogelijke baten doordat administratieve lasten verminderen, en het belang bij zorgvuldige gegevensverzameling en verwerking met het oog op beroepsaansprakelijkheid.

Overheidsbelangen zijn de efficiency en de effectiviteit van het overheidsoptreden, het openhouden van de informatiestroom (geheimhouding en organisatiebelang), de betrouwbaarheid van de overheid bij het beschermen van privacy c.q. en andere vertrouwelijke gegevens (privacy, imago en organisatiebelang), het zicht op gegevens bij doorverstrekking in verband met de eigen verantwoordelijkheid en het vertrouwen van de burger (doelbinding), de resultaten die met de verkregen gegevens kunnen worden gerealiseerd (eigen baten), de nadelen voor de eigen informatiepositie bij verstrekking van de gegevens, het belang van de juistheid/goede kwaliteit van de gegevens en het risico van het niet of niet correct ontvangen van de toezichtgegevens.

1912170 01165

5.3 Deelvragen 4 en 5: juridische erkenning van de gevonden belangen

Een aantal van de hiervoor in paragraaf 5.2 genoemde belangen is juridisch erkend, doordat deze in wetgeving zijn neergelegd met het oog op de verankering van met name de bescherming van de privacy en de vrijheid van het individu. Op de vraag in hoeverre genoemde belangen juridisch erkend zijn, wordt hierna ingegaan.

5.3.1 Deelvraag 4: juridisch gelabelde belangen

In paragraaf 2.6 is beschreven dat openbaarheid van bestuur een belangrijk uitgangspunt is in het Nederlandse recht. Van dit uitgangspunt wordt afgeweken in het belang van de bescherming van private belangen en in het belang van de goede werking van het openbaar bestuur. In het verband van dit onderzoek betreft dat vooral het belang bij het toezicht op de naleving en het opsporingsbelang. Hierachter ligt een parallel belang dat hiervoor in paragraaf 5.2 ook al aan de orde kwam: het vertrouwen in de overheid. Burgers en bedrijven zullen immers eerder geneigd zijn gegevens af te staan aan de overheid als zij erop kunnen vertrouwen dat deze goed worden bewaakt en niet zomaar aan de openbaarheid of aan derden worden prijsgegeven. In wezen zijn een aantal van de belangen die uit ons onderzoek naar voren kwamen terug te voeren op het belang bij vertrouwen in de overheid.

Dit zijn aan de kant van de overheid de efficiency en de effectiviteit van het overheidsoptreden, het openhouden van de informatiestroom (geheimhouding en organisatiebelang), de betrouwbaarheid van de overheid bij het beschermen van privacy c.q. en andere vertrouwelijke gegevens (geheimhouding, imago en organisatiebelang), het zicht op gegevens bij doorverstrekking in verband met de eigen verantwoordelijkheid en het vertrouwen van de burger (doelbinding). Van de kant van de burger zijn dit het belang bij vertrouwelijke behandeling van gegevens (geheimhouding), de bescherming van bedrijfs- en fabricagegegevens en de bescherming van persoonsgegevens (ook van derden) en de transparantie ten aanzien van de uitwisseling van gegevens.

Deze belangen zijn juridisch te labelen onder de categorieën bescherming van persoonsgegevens, bescherming van bedrijfs- en fabricagegegevens en geheimhoudingsplichten.

5.3.1.1 De bescherming van persoonsgegevens

Bescherming van vertrouwelijke gegevens dient zowel het belang van de burger als dat van de overheid. De belangen lopen hier parallel: de burger zal immers eerder gegevens verstrekken aan de overheid als de vertrouwelijke behandeling is gewaarborgd. De overheid kan door vertrouwelijke behandeling te waarborgen efficiënt optreden. Over de bescherming van vertrouwelijke gegevens gaat Hoofdstuk 2, waarnaar wordt verwezen. Daarin is uiteengezet dat de verschillende soorten toezichtgegevens op verschillende manieren worden behandeld als het gaat om het waarborgen van de vertrouwelijkheid.

Persoonsgegeven en bijzondere persoonsgegevens ondervinden bescherming via de Wbp, de Wpg en de Wjsg. Persoonsgegevens mogen worden gebruikt en verder verwerkt met het oog op het doel waarvoor zij zijn vergaard (doelbinding). Strafrechtelijke gegevens gelden als bijzondere persoonsgegevens, die slechts op grond van de Wpg en de Wjsg mogen worden verwerkt. Uitwisseling van persoonsgegevens is onder omstandigheden toelaatbaar, mits is voldaan aan de eis dat de verwerking niet onverenigbaar is met het doek waarvoor de gegevens zijn verzameld (doelbinding).

1912170 01165

Strafrechtelijke persoonsgegevens kunnen worden uitgewisseld binnen de kaders van de Wpg en de Wjsg. Beide laatstgenoemde wetten benoemen de soorten gegevens die kunnen worden uitgewisseld, alsmede de overheidsinstanties aan wie gegevens kunnen worden verstrekt. De Wpg maakt verder een onderscheid tussen soorten verstrekking: incidentele en structurele verstrekking en verstrekking aan samenwerkingsverbanden. De verstrekking vindt plaats met het oog op een zwaarwegend algemeen belang (zie verder Hoofdstuk 2 en in het bijzonder paragraaf 2.5).

5.3.1.2 De bescherming van bedrijfs- en fabricagegegevens

Bedrijfs- en fabricagegegevens mogen wel worden verwerkt, maar voorkomen moet worden dat concurrenten hiervan op de hoogte raken. Toezichthouders die deze gegevens verwerken mogen deze daarom wel verstrekken aan andere toezichthouders of opsporingsdiensten, maar niet aan derden buiten het openbaar bestuur. De regeling in de Wob en de procesrechtelijke bepalingen met betrekking tot beperkte kennisneming van de stukken vormen hiervoor de waarborg. Zie hierover paragraaf 2.3.5.

5.3.1.3 Geheimhoudingsplichten

Los van de kwalificatie als persoonsgegeven of bedrijfs- of fabricagegegeven wordt het belang bij bescherming van de vertrouwelijkheid van gegevens gewaarborgd door geheimhoudingsplichten. In paragraaf 2.6 is hierop ingegaan. Een geheimhoudingsplicht betreft dus alle gegevens die in het kader van de overheidstaak door de bevoegde instantie worden verkregen. Geheimhoudingsplichten zijn over het algemeen niet absoluut. Bij of krachtens de wet kunnen uitzonderingen worden geformuleerd. Deze uitzonderingen zijn zo geformuleerd dat wordt aangegeven onder welke voorwaarden welke gegevens aan een bepaalde, benoemde partij mogen worden doorgegeven. De Uitvoeringsregeling Awr, besproken in paragraaf 2.6.1, is daarvan een voorbeeld. De geheimhoudingsplicht biedt aldus de mogelijkheid om het eigen organisatiebelang af te wegen tegen dat van de gegevensvragende instantie.

Het belang van geheimhouding van gegevens door de Belastingdienst is voor de dienst zelf bijvoorbeeld een belangrijke factor om de informatiestroom naar de dienst zo open mogelijk te houden. Als de gegevens van de Belastingdienst te gemakkelijk in handen van andere instellingen komen, dan kan dit de bereidheid van burgers en bedrijven om gegevens te leveren doen afnemen. Ook in de opsporingssfeer kan geheimhouding een belang zijn voor het onderzoek. De opsporingsinstantie zal in veel gevallen informatie in het strafdossier niet geven om te voorkomen dat daardoor het onderzoek in gevaar komt.

5.3.1.4 Eigen verantwoordelijkheid voor doorverstrekking

Bij doorverstrekking aan een andere toezichthouder of aan opsporingsinstanties is niet altijd duidelijk, noch gegarandeerd dat de gegevens door deze derde partij zullen worden gebruikt voor dezelfde doeleinden als waarvoor zij zijn vergaard en aan de norm van doelbinding kan worden voldaan. Dit valt samen met de wens van burgers en bedrijven dat gegevensuitwisseling transparant is en met het belang van vertegenwoordigers bij zorgvuldige gegevensuitwisseling. Die transparantie c.q. zorgvuldigheid kan niet altijd op het gewenste niveau worden geboden. Uit het onderzoek blijkt dat onzekerheid daarover bij overheidsinstanties leidt tot terughoudendheid bij de doorverstrekking. Het belang niet in strijd te handelen met de wettelijke eis van doelbinding komt het duidelijkst naar voren in die gevallen waarin deze onzekerheid wordt opgelost met *third party rules*: de verstrekker dekt zich in door de eis dat de ontvanger van de gegevens uitdrukkelijk toestemming vraagt voor doorverstrekking aan een derde partij. Doelbinding is aldus een verankerend juridisch gelabeld belang dat eveneens een vrij prominente rol speelt.

1912170 01165

In het onderzoek is eveneens gebleken dat de gesignaleerde onzekerheid of er wel of niet gegevens mogen worden verstrekt kan worden geconcretiseerd met een beroep op de geheimhoudingsplicht. Een voorbeeld vormt onzekerheid over het in acht nemen van de waarborgen die de strafvordering biedt aan de verdachte, in het bijzonder het zwijgrecht. Respondenten zijn beducht voor het verstrekken van gegevens (of het nu wel of geen persoonsgegevens zijn), die wanneer deze in het kader van de voorbereiding van een strafzaak of een punitieve bestuurlijke sanctie waren vergaard zouden vallen onder het zwijgrecht en de cautieplicht. Wanneer de ontvangende instantie deze gegevens zou kunnen of willen gebruiken in een strafprocedure of een bestuurlijke sanctieprocedure, acht de verstrekkende instantie zich gehouden het belang van de betrokken persoon te beschermen door een beroep op de waarborgen van artikel 6 EVRM om zo te voorkomen dat men zelf wordt beticht van onrechtmatige verstrekking. Het besef dat dit slechts in uitzonderlijke gevallen zal voorkomen, gelet op de jurisprudentie van het EHRM, leeft niet in brede kring. De weigering om informatie te verstrekken kan dan een grond vinden in een geheimhoudingsplicht of in de doelbinding.

Bovengenoemde belangen zijn juridisch gekwalificeerd als een verbod, een recht, een plicht of een procedurele waarborg. Uit het onderzoek blijkt dat daarnaast nog een aantal belangen een rol speelt dat geen juridische inbedding heeft. Deze belangen zijn terug te voeren op organisatorische, praktische, en ICT-gerelateerde omstandigheden.

5.3.2 Deelvraag 5: niet juridisch erkende belangen

In meer praktisch opzicht spelen, zo is in het onderzoek gebleken, ook een aantal belangen een rol. Bij de private belangen zijn dat de mogelijke baten doordat administratieve lasten verminderen. Aan de kant van de overheid zijn dat belangen die weliswaar voortvloeien uit wettelijke bevoegdheden, maar niet juridisch zijn te duiden. We doelen hier op zaken die kunnen worden samengevat onder de noemer 'organisatiebelang'. Het gaat daarbij om het belang bij efficiency en de effectiviteit van het overheidsoptreden, het openhouden van de informatiestroom, het imago van de overheid als betrouwbare partner voor de burger en voor de andere overheidsinstanties (wederkerigheid), de resultaten die met de verkregen gegevens kunnen worden gerealiseerd (eigen baten), de nadelen voor de eigen informatiepositie bij verstrekking van de gegevens, het belang van de juistheid/goede kwaliteit van de gegevens en het risico van het niet of niet correct ontvangen van de toezicht-gegevens.

5.3.2.1 Samenwerkende overheden

Het hiervoor als organisatiebelang getypeerde fenomeen betreft om te beginnen de verhouding tussen wat de respondenten ketenpartners noemen. Op bepaalde beleidsvelden, zoals de belastingheffing en de bestrijding van illegaal en gevaarlijk vuurwerk, werken verschillende overheidsinstanties, toezichthouders en opsporingsdiensten samen aan het verwezenlijken van een gemeenschappelijk doel. In andere beleidsvelden, zoals de verbetering van de kwaliteit en de integriteit van het taxivervoer werkt één overheidsinstantie, in casu de gemeente, aan dat beleidsdoel, maar heeft deze andere overheidsinstanties nodig om aan gegevens te komen. In het laatste geval is er geen georganiseerde samenwerking (zoals via een convenant) en vindt gegevensuitvraag en –uitwisseling op ad hoc basis plaats. In die situatie bestaat veelal geen wederkerigheid: de gemeente is de vragende partij, andere instanties en toezichthouders hebben geen belang bij het bereiken van de beleidsdoel-stellingen.

Deze twee omstandigheden – het ontbreken van een vast samenwerkingsverband en het ontbreken van een gezamenlijk beleidsdoel – maken dat de vragende partij met moeite de gegevens kan

1912170 01165

bemachtigen die zij nodig heeft. De verstrekkende partij heeft geen belang bij het verstrekken en voelt zich uit dien hoofde niet verplicht om aan het verzoek om gegevens te voldoen. Bij ad hoc gegevensuitvraag door gemeenten bestaat op grond van de Wbp, de Wpg of de Uitvoeringsregeling Awr ook geen duidelijke wettelijke basis, zodat steeds op basis van een nieuw te maken afweging moet worden beslist op het verzoek, en geen zicht of moeilijk zicht bestaat op de toelaatbaarheid van de verstrekking (doelbinding en geheimhouding) en op de mogelijkheden en moeilijkheden voor doorverstrekking aan derde partijen. Omdat een verplichting tot gegevensverstrekking ontbreekt, stelt de verstrekkende partij zich terughoudend op, terughoudender dan op grond van de regelgeving noodzakelijk is. Hier vinden we bevestiging van de observatie van de WRR dat verspreiden en bewerken van informatie in netwerken een dynamiek geeft die het soms zeer lastig maakt te bepalen wie verantwoordelijkheid draagt voor (de juistheid van) bepaalde informatie over burgers.

Ter illustratie kan het voorbeeld worden genoemd waarbij een gemeente gevraagd wordt gegevens te verstrekken over een bedrijf in de gemeente in het kader van een strafrechtelijk onderzoek. Daarbij wordt de gemeente niet op de hoogte gebracht van de achterliggende onderzoeksinformatie. In zo'n geval is het moeilijk om een afweging te maken tussen enerzijds het verstrekken van de informatie met voor de gemeente onvoorziene gevolgen voor een van de bedrijven in de gemeente. Als de informatie terecht is gegeven wordt het bedrijf wellicht veroordeeld, met mogelijke gevolgen voor de gemeente, en als de gegevens ten onrechte blijken te worden verstrekt komt het bedrijf mogelijk met een schadeclaim. In die omstandigheden zijn er geen eigen baten bij verstrekking en zal de gemeente terughoudend zijn met het verstrekken van gegevens.

5.3.2.2 Efficiency en effectiviteit

Efficiëntie in de zin van tijdigheid en betrouwbaarheid wat betreft de ontvangst van gegevens speelt ook een rol, zo blijkt uit het onderzoek. Respondenten houden bij het doen van een informatieverzoek rekening met de kans dat de gegevens niet of niet op tijd komen. Is die kans groot, dan wordt in sommige gevallen afgezien van het opvragen ervan. Een voorbeeld is het inwinnen van informatie omtrent buitenlandse veroordelingen. De ervaring leert dat de procedure daarvoor erg tijdrovend is en het belang bij het verkrijgen van die informatie wordt dan ook afgewogen tegen het nadeel van het ontbreken ervan. Hetzelfde geldt voor de inschatting dat gegevens niet of niet goed worden ontvangen.

Een ander praktisch probleem dat is gesignaleerd in het onderzoek ligt in de beperkingen van de technologie (zie paragraaf 3.3). Bij een gegevensuitvraag wordt met regelmaat gevraagd naar bepaalde categorieën, kenmerken, of eigenschappen. Een voorbeeld is informatie over panden met bepaalde kenmerken (eigenaar, verkoopprijs) in een bepaalde wijk. In sommige gevallen komen de coderingen of rubriceringen in de bevraagde gegevensverzameling niet overeen met de kenmerken die de verzoeker heeft aangegeven. Het vergt dan van de verstrekker veel tijd en moeite om tot een dataset te komen die overeenkomt met de zoekvraag, en de verstrekker zal dan traag reageren of het verzoek afwijzen, ook al is gegevensverstrekking toelaatbaar. Praktische uitvoerbaarheid en organisatiekosten (tijd en moeite) spelen daarom ook een rol. In dit verband komt ook het begrip wederkerigheid op; niet zozeer een belang, maar wel een smeermiddel om de relaties in het gegevensnetwerk te optimaliseren. Deze wederkerigheid heeft zowel juridisch als beleidsmatig geen status, maar blijkt in operationele samenwerkingsverbanden de samenwerking positief te kunnen beïnvloeden.

5.3.2.3 Kwaliteit van gegevens

Een volgend punt dat naar voren is gekomen in het onderzoek is de kwaliteit van de gegevens (zie met name paragraaf 3.3.4, 4.7.2 en 7.2). Zoals ook in het rapport iOverheid is aangegeven, hebben de vermenging van informatie, de bewerking ervan en het bezien van informatie in een andere context

1912170 01165

dan waarin deze in eerste instantie is opgenomen gevolgen voor de kwaliteit en betrouwbaarheid voor informatie. Gegevens worden verrijkt met (soms subjectieve) oordelen, inschattingen en waarnemingen. Een voorbeeld is CIE-informatie: de databank van de CIE wordt door een code expliciet aangegeven hoe betrouwbaar informatie is (wel/niet uit eigen waarneming, van een derde gehoord etc.).[145] Er worden kruisrelaties aangebracht met andere gegevens of juist andersom: de beslissing wordt genomen dat er geen relatie is met andere gegevens. Ook het labelen van gegevens is waardering die kan berusten op subjectieve beoordeling. In dat verband kan worden gewezen op de eis die ook in de nieuwe EU-richtlijn (die in paragraaf 2.3.2 werd besproken) is opgenomen, dat de verschillende categorieën persoonsgegevens die worden verwerkt, voor zover mogelijk worden onderscheiden naar de graad van juistheid en betrouwbaarheid, en dat persoonsgegevens die op feiten zijn gebaseerd, worden onderscheiden van persoonsgegevens die op een persoonlijke oordeel zijn gebaseerd.

Daarnaast kan het zo zijn dat de verstrekker zelf al keuzes heeft gemaakt voor de ontvanger door gegevens in datasets te filteren op bepaalde kenmerken waardoor van belang zijnde gegevens ontbreken in de geleverde set. Een volgend probleem is de door de WRR ook besproken situatie dat gegevens zijn vervuild of ronduit onjuist. Dat maakt de ontvangende partij huiverig, zo blijkt uit ons onderzoek. In de internetenquête gaven de ontvangende uitvoeringsorganisaties aan de betrouwbaarheid van de ontvangen gegevens lager in te schatten dan zij doen vanuit de positie van leverancier (zie de staatjes in paragraaf 7.2). Het belang bij kwaliteit, juistheid en betrouwbaarheid van de gegevens is daarmee een van de betrokken belangen.

5.4 Deelvragen 3 en 6: onderlinge verhouding van betrokken belangen

De onderlinge verhouding van de verschillende belangen is onderzocht door middel van een MCA, waarvoor een internetenquête de input leverde (zie paragraaf 3.1.2 voor de gehanteerde methode en paragraaf 7.2 voor de enquête en de uitkomsten). In het rapport iOverheid wordt opgemerkt dat nagenoeg elke bestuurder, politicus en ambtenaar de beginselen die appelleren aan gezond verstand, verantwoordelijkheid, grondwettelijke waarden en zorgvuldigheid zullen onderschrijven. Uit het onderzoek, en in het bijzonder uit de enquête, blijkt dat de respondenten groot belang hechten aan de 'verankerende beginselen': privacy, geheimhouding en doelbinding. Wel is er een verschil te zien tussen de verschillende groepen respondenten.

5.4.1 Samenvatting van de enquêteresultaten en MCA

Het zoeken naar evenwicht tussen de verankerende en de stuwende beginselen komt ook tot uitdrukking in de resultaten van het onderzoek. Bij de enquêteresultaten blijken de verankerende beginselen bij alle deelnemers hoog te scoren (doelbinding en geheimhouding).

Bij de vertegenwoordigers van burgers en bedrijven stonden doelbinding, geheimhouding en privacy steevast het hoogst genoteerd. Transparantie, als procesmatig beginsel werd als ontbrekend belang toegevoegd vanuit de vertegenwoordigers van de burgers en bedrijven.

Bij de gegevensuitwisseling in de bestuurlijke sfeer hadden doelbinding, geheimhouding en privacy de hoogste prioriteit in gevallen waarin gegevens moesten worden geleverd met het oog op opsporing. Als gegevens vanuit de opsporing werden ontvangen scoorde het eigen belang van de ontvanger hoger dan de privacy. In de andere gevallen binnen de bestuurlijke sfeer kwam het eigen

145 Deze problematiek komt naar voren In de conclusie van de AG bij HR 9 juli 2010, *LJN* BM2311, *NJ* 2010, 416.

1912170 01165

belang van de ontvangende organisatie in de plaats van de privacy. In het geval dat gegevens werden geleverd oversteeg het organisatiebelang het belang van geheimhouding.

Bij de geënquêteerden in opsporingsorganisaties werd het belang van doelbinding en geheimhouding hoog ingeschat. Daarnaast werden de baten voor de ontvanger van groot belang gevonden, zowel bij de leverancier als bij de ontvanger zelf.

Opvallend was verder dat bij de overheidsorganisaties kosten als exponent van de stuwende beginselen over de hele linie laag scoorden als belang.

Een uitgebreidere samenvatting van de resultaten vindt u in paragraaf 3.4. De gehele enquête vindt u in paragraaf 7.2.

5.4.2 Het organisatiebelang als overkoepelend belang

Uit ons onderzoek blijkt dat juist bij de uitwisseling van toezichtgegevens het belang van de bescherming van persoonsgegevens, de eis van doelbinding en de geheimhouding van grote waarde worden geacht. De stuwende en procesmatige beginselen in de sfeer van baten voor de organisatie en kosten van de gegevensuitwisseling scoren lager, kosten zelfs uitgesproken laag. Hieruit zou kunnen worden afgeleid dat de verankerende beginselen ook werkelijk goed verankerd zijn in onze handhavingsorganisaties. Bij het streven naar succes bij toezicht en handhaving worden deze beginselen immers nooit uit het oog verloren. De stuwende beginselen kregen in ons onderzoek niet de overhand.

Een aandachtspunt is dat de procesmatige beginselen zoals transparantie en accountability niet expliciet lijken te leven. Denkbaar is dat deze principes intrinsiek worden meegewogen bij de besluitvorming over het al of niet vragen of verstrekken van gegevens, maar de uitkomsten van ons onderzoek geven daarvoor geen basis. Eerder moet worden geconcludeerd dat deze beginselen geen rol spelen.

Als een rangorde van de hoogst gewaardeerde belangen moet worden aangegeven dan valt op dat doelbinding de hoogste score haalt, daarna volgen geheimhouding en privacy, en bij de overheid baten voor de ontvangende of leverende organisatie. De reden voor deze eenduidige keuze zou kunnen worden gezocht in de diepe worteling van de grondrechten in de overheidsorganisatie. Deze beginselen bieden immers tegenwicht aan de voortdurende roep om veiligheid, effectief optreden en efficiency van de overheidsdiensten. In het onderzoek is echter gemeten hoe de belangen werden gewaardeerd, niet hoe deze in concrete gevallen werden afgewogen. In het rapport iOverheid wordt melding gemaakt van de spanningsvolle relatie tussen grondrechten en dagelijkse realiteit en het feit dat privacy een afweging is tussen individuele en gepercipieerde collectieve belangen, waarbij de individuele niet zelden het onderspit delven.[146]

De bevinding dat toezichthouders en opsporingsdiensten de verankerende beginselen zo hoog in het vaandel hebben vanwege de grote waarde die zij toekennen aan de grondrechten van burgers behoeft daarom nuancering. Bescherming van de privacy en doelbinding zijn weliswaar verankerende beginselen, maar voor de overheidsinstanties dienen zij het verder gelegen doel van het waarborgen van de betrouwbaarheid van de overheid en daarmee de effectiviteit en de efficiency van het overheidsoptreden. De bescherming van de belangen van de burger wordt daarbij ook als het belang van de eigen organisatie gezien, omdat daarmee de informatiestroom open wordt gehouden. Zoals uit

146 *iOverheid* (*supra* noot 3), p. 81.

1912170 01165

de MCA blijkt, hechten de vertegenwoordiger van burgers en bedrijven zeer aan de bescherming van de positie van hun cliënt. Bescherming van de privacy, doelbinding en geheimhouding zijn hier de sleutelbegrippen ter omschrijving van deze belangen. Overheidsorganisaties zullen dus om hun informatiepositie te behouden en om hun imago als betrouwbare overheid te beschermen noodzakelijkerwijze een goede bescherming van deze belangen moeten bieden. Hiervoor werd al gerefereerd aan de positie van de ontvangers van gegevens. Bij de ontvangers ontbreekt de directe relatie tot het subject, en leven de noties geheimhouding, bescherming van de privacy en doelbinding minder sterk bij de verwerking van gegevens. Voor de ontvanger nemen juist de resultaten die met de verkregen gegevens kunnen worden gerealiseerd een prominente plaats in.

5.4.3 Het strategische belang van de geheimhoudingsplicht

Het belang bij geheimhouding verdient in dit verband nadere aandacht. Geheimhoudingsplichten strekken zich niet alleen uit over de hiervoor besproken vertrouwelijke gegevens (persoonsgegevens en bedrijfs- en fabricagegegevens) maar over alle soorten toezichtgegevens. Zoals in paragraaf 2.6 is aangegeven heeft de wetgever geheimhoudingsplichten in het leven geroepen ter bevordering van de goede werking van het openbaar bestuur, daaronder begrepen de belangen bij toezicht, controle en opsporing. Geheimhouding, zeker zoals het op de werkvloer wordt geïnterpreteerd, is daarmee vooral ook een organisatiebelang: het openhouden van de inkomende informatiestroom en het niet weggeven van de informatiepositie in een onderzoek.

Het openhouden van de inkomende informatiestroom staat of valt met het vertrouwen dat burgers en bedrijven hebben in de mate waarin de overheid de daartoe in aanmerking komende gegevens vertrouwelijk zullen behandelen. Dit verklaart ook waarom onze respondenten melding maken van terughoudendheid bij de verstrekking van gegevens aan andere toezichthouders of opsporingsinstanties: vertrouwen komt immers te voet en gaat te paard. Het verklaart ook de wens bij gegevensverstrekkers om zicht te hebben op het gebruik dat de ontvanger van de gegevens gaat maken, inclusief de doorverstrekking aan weer een derde partij (zie paragraaf 3.2.1.4, 3.2.3.7, 3.3.2, 3.3.3, 3.5.3.5). De zorg dat gegevens die uiteindelijk opsporingsinstanties of het OM bereiken zijn verkregen zonder noodzakelijke strafvorderlijke waarborgen in acht te nemen kan eveneens hieruit worden verklaard (zie paragraaf 3.2.3.7, 3.3.3, 3.5.3.5).

Ook het belang van het niet weggeven van een informatiepositie in het onderzoek, wordt door de eigen organisatie gepercipieerd als een belang dat aansluit bij dat van de goede werking van het openbaar bestuur c.q. de opsporing. De opsporingsinstantie zal bijvoorbeeld in veel gevallen informatie in het strafdossier niet geven om te voorkomen dat daardoor het onderzoek in gevaar komt. De toezichthouders of uitvoeringsorganisaties die om die reden geen gegevens ontvangen kijken daar anders tegenaan. Zij begrijpen niet altijd goed waarom de geheimhoudingsplicht wordt ingezet en zien dit juist als een belemmering van de goede werking van het openbaar bestuur (zie paragraaf 3.5.3.1 en 3.5.3.2).

5.4.4 Convenanten zijn geen panacee

In paragraaf 2.5.4 is besproken dat zowel de Wbp als de Wpg structurele gegevensuitwisseling toestaat, als sprake is van een samenwerkingsverband. In paragraaf 2.5.5 is vervolgens besproken dat samenwerkende partijen in een convenant hun respectievelijke posities vastleggen en afspreken tot gegevensuitwisseling over te gaan. Daarbij werd opgemerkt dat deze convenanten over het algemeen meer intentieverklaringen zijn en weinig verheldering bieden over de verschillende posities en bevoegdheden, aangezien enkel wordt verwezen naar de voor iedere partner geldende 'wettelijke

1912170 01165

beperkingen'. In sommige gevallen wordt in een convenant slechts herhaald wat al in de wet staat, zonder nadere verheldering of verklaring hoe deze wettelijke bevoegdheden in het concrete samenwerkingsverband zullen worden uitgeoefend. In paragraaf 3.2 kwam meer specifiek aan de orde dat dergelijke convenanten soms worden gezien als verzekering voor de uitwisseling van gegevens, maar dat zij bij nadere bestudering niet helder blijken te maken wanneer gegevensuitwisseling nu wel of niet toelaatbaar is.

Convenanten zijn nodig om vast te kunnen stellen dat er een structureel samenwerkingsverband bestaat, waarbinnen op grond van de Wbp of de Wpg gegevens mogen worden uitgewisseld. Een convenant kan echter geen bevoegdheidsgrondslag bieden: deze moet worden ontleend aan de wet. Iedere convenantspartner moet zijn bevoegdheid baseren op de voor hem toepasselijke wettelijke bepalingen en vervolgens vaststellen welke gegevens in het samenwerkingsverband kunnen worden ingebracht. De omstandigheid dat de verschillende wettelijke kaders verschillende kanten uitwijzen helpt daarbij niet.

Het convenant is ook niet de plaats om de bevoegdheden vast te leggen, maar wel de plaats om vast te leggen hoe deze bevoegdheden in procedurele zin zullen worden uitgeoefend. Zo zou een convenant moeten bepalen voor welke doeleinden de samenwerking dient, welke gegevens of gegevenssets daarvoor zullen worden aangemaakt of aangeleverd, wie bewaakt dat wordt voldaan aan de Wbp (melding aan het CBP), via welke media zal worden uitgewisseld (databank, cloud) en hoe de veiligheid van deze media wordt bewaakt.

5.4.5 Ruimte voor afweging?

In het onderzoek is veel aandacht uitgegaan naar de bescherming van persoonsgegevens, het is een kernpunt bij de afweging of tot uitwisseling kan worden overgegaan. In paragraaf 2.3.2 werd het EU kader voor privacybescherming besproken, dat is uitgewerkt in artikel 7, 8 en 9 Wbp (paragraaf 2.4). Dit kader biedt ruime mogelijkheden om gegevens uit te wisselen, als maar is voldaan aan de randvoorwaarden dat duidelijk vaststaat waarvoor gegevens worden verzameld en verwerkt. Met name de optie van artikel 8, dat gegevensverwerking plaats kan vinden wegens de goede vervulling van een publiekrechtelijke taak door bestuursorganen biedt veel ruimte. Wanneer bestuurlijke toezichthouders en uitvoeringsorganisaties onderling willen uitwisselen, kan dat op grond van de Wbp dus ook. Het Europese recht, noch de Wbp staan daaraan in de weg. De problematiek van de doelbinding, die in het onderzoek in paragraaf 2.4.3 en 4.6 werd besproken, is niet onoverkomelijk. Hierover gaat paragraaf 5.5.2.

Op de strafrechtelijke persoonsgegevens is de Wbp niet van toepassing. De Wpg en de Wjsg geven een kader voor de uitwisseling met benoemde partijen c.q. in een samenwerkingsverband. Beide wetten kennen daarnaast de bevoegdheid om in incidentele gevallen gegevens te verstrekken aan niet benoemde partijen, als dat een zwaarwegend belang dient (artikel 19 Wpg en 39f Wjsg). De wet biedt aldus ruimte voor afweging, zij het dat de normconditie 'zwaarwegend belang' tot terughoudendheid noopt. Uit ons onderzoek blijkt dat vragende partijen de politie en het OM soms te terughoudend vinden bij het maken van die afweging (zie paragraaf 3.2.1.4 en 3.2.3.7). Het organisatiebelang bij het krijgen en behouden van de eigen informatiepositie en bij het beschermen van het eigen onderzoek weegt daarbij volgens de vragende partijen te zwaar. Niet zelden wordt ook de doelbinding, die ook in de Wpg en de Wjsg beperkingen stelt, als argument naar voren gebracht om verstrekking te weigeren. Het eigen belang van de organisatie weegt aldus zwaarder dan het belang van de goede werking van de overheid in den brede. Bij concrete afwegingen zouden OM en de

1912170 01165

opsporingsinstanties meer aandacht moeten besteden aan de belangen van andere overheidsorganisaties.

Een vergelijkbaar punt speelt in het kader van de geheimhoudingsplicht. Hiervoor in paragraaf 5.3.1.3 werd al ingegaan op het strategische belang van de geheimhoudingsplicht. Ook al staat de wet of de uitvoeringsregeling ruime uitzonderingen toe, zoals bij de in paragraaf 2.6.1 besproken Uitvoeringsregeling Awr, dan nog komt het aan op de afweging in concreto. De geheimhoudingsplicht biedt de mogelijkheid om zich in gevallen van twijfel over de wenselijkheid of toelaatbaarheid van de gegevensverstrekking daarachter te verschuilen. Dit uit zich in het adagium 'bij twijfel niet inhalen'. In de expertmeeting bracht de Belastingdienst naar voren dat ieder verzoek om gegevensverstrekking welwillend wordt bekeken en dat het zo mogelijk wordt gehonoreerd. Van de kant van het OM werd juist aangegeven dat geheimhouders (niet enkel de Belastingdienst) naar de inschatting van het OM te snel naar hun geheimhoudingsplicht grijpen. In paragraaf 5.4.3 werd al een verklaring gezocht voor dit fenomeen. De oplossing dat dan maar de uitzonderingen op de geheimhoudingsplicht moeten worden verruimd, leidt naar ons oordeel enkel tot verplaatsing van het probleem. Ook dan zullen er grensgevallen zijn die tot een arbitraire afweging leiden, die door de vragende partij niet begrepen wordt.

Hiervoor werd al opgemerkt dat de procesmatige beginselen van transparantie en accountability niet lijken te leven bij de afwegingsprocessen. Om de acceptatie van de uitkomst bij vragende instanties te vergroten, verdient het aanbeveling de afwegingsprocessen beter inzichtelijk en toetsbaar te maken. Dit kan voorkomen dat overheidsinstanties uitgaan van tegengestelde belangen en daarmee hun eigen organisatiebelang als belangrijkste ijkpunt zien. Het kan ook voorkomen dat overregulering ontstaat, waarbij de lijst van instanties aan wie wel bepaalde gegevens moeten worden verstrekt steeds langer wordt. Een andere oplossing kan zijn dat een verplichting tot het gegevensverstrekking wordt opgenomen (bij twijfel wel inhalen) met de mogelijkheid tot het maken van een uitzondering, waarvoor dan wel een zware motiveringsplicht geldt. Deze laatste optie is door respondenten in het onderzoek als wenselijk naar voren gebracht (zie paragraaf 3.2.3.7 en hierna ook paragraaf 5.5.2).

5.5 Deelvragen 7 en 8: naar een algemene regeling?

De tweede hoofdvraag is erop gericht te achterhalen of het, in het licht van de onderzoeksresultaten met betrekking tot de betrokken belangen en de afweging ervan, gewenst is om voor het verstrekken van toezichtgegevens tussen toezichthouders onderling en tussen toezichthouders enerzijds en het OM, de politie en de buitengewoon opsporingsambtenaren anderzijds, een algemene regeling te treffen in de Algemene wet bestuursrecht en/of eventuele andere wetten. Omdat de uitkomsten van het onderzoek op dit punt diffuus zijn is eveneens onderzocht of een algemene voorziening in de Awb of in andere wetten mogelijk is, en welke effecten een algemene voorziening zou kunnen hebben.

5.5.1 Geen grote behoefte aan een algemene regeling

De behoefte aan een algemene regeling is gepeild via de oriënterende gesprekken over de drie casus en de expertmeeting. Uit deze gesprekken is geen eenduidig beeld gekomen. Het is de onderzoekers gebleken dat er op het niveau van de werkvloer, waar daadwerkelijk beslissingen over doorverstrekking c.q. verzoeken om gegevens worden genomen, wel behoefte bestaat aan een algemene regeling, met name vanuit de verwachting dat meer duidelijkheid zou ontstaan over de juridische basis bij het uitwisselen van gegevens. Een uitzondering vormen de respondenten van de Belastingdienst: zij hebben in de regeling in de Awr en de Uitvoeringsregeling Awr een afdoende

1912170 01165

helder juridisch kader, dat bij de toepassing niet tot veel vragen of problemen aanleiding geeft. Dit valt te verklaren uit de homogeniteit van het beleidsveld waarin de Belastingdienst opereert enerzijds, en de heldere structuur van de toepasselijke regelgeving anderzijds. Het uitgangspunt is dat alle gegevens die de Belastingdienst vergaart geheim zijn. Uitzonderingen hierop vormen gegevens die krachtens wettelijk voorschrift moeten worden verstrekt, dan wel gegevens die worden verstrekt aan bestuursorganen die deze nodig hebben voor de uitoefening van de publiekrechtelijke taak en die zijn opgesomd in de Uitvoeringsregeling Awr.

Ter ondersteuning van de invoering van een algemene regeling werd naar voren gebracht dat daarmee een legitimering voor de uitwisseling wordt gegeven vanuit de meer verankerde beginselen van de doelbinding en de waarborgen die horen bij de sfeerovergang tussen bestuursrechtelijke en strafrechtelijke handhaving. Verder zou met een wettelijke regeling kunnen worden voorzien in de lacune dat er geen mogelijkheid is om het verstrekken van gevraagde informatie af te dwingen. Een (geclausuleerde) verplichting zou daarbij uitkomst kunnen bieden. Een derde argument is dat daarmee een beter zicht ontstaat op 'doorverstrekking' en het naleven van de regels met betrekking tot doelbinding. Als laatste argument is opgeworpen dat daarmee ook een beter zicht op de kwaliteit van de ontvangen gegevens kan worden verkregen.

In de expertmeeting kwamen meer beleidsmatige aspecten aan de orde. De experts waren van oordeel dat de bestaande wettelijke regels veel mogelijk maken, ook al is het ingewikkeld. De inschatting van de experts was, dat er op de werkvloer meer behoefte is aan verduidelijking dan aan een nadere wettelijke regeling. Benadrukt werd dat de Wbp in artikel 8 al een algemeen afwegingskader biedt voor afweging in ad hoc gevallen, dat wil zeggen gevallen die niet in bijzondere wetgeving zijn geregeld. Een andere algemene regeling zou daaraan niet veel kunnen toevoegen.

Omdat hieruit geen eenduidige conclusies zijn te trekken ten aanzien van de vraag of een algemene wettelijke regeling überhaupt gewenst is, hebben de onderzoekers zich gebogen over de vraag hoe een wettelijke regeling, zo die er moest komen, eruit zou kunnen zien.

5.5.2 Opties voor een regeling

In de eerste plaats is onderzocht of een regeling voor uitwisseling van toezichtgegevens een plaats zou kunnen krijgen in de Awb. De Awb is om verschillende redenen een minder geschikte plek. Naast bestuursorganen zijn ook natuurlijke personen en privaatrechtelijke organisaties betrokken bij gegevensuitwisseling. Dat blijkt ook uit de Wbp, die zich tot al deze mogelijke actoren richt. Een (uitputtende) regeling in de Awb, die nu juist gericht is op het handelen van bestuursorganen, ligt daarom niet voor de hand. Wel zou er voor gekozen kunnen worden om in de Awb alleen die regels op te nemen die gelden voor bestuursorganen en toezichthouders. Het nadeel daarvan is dat daarmee slechts een deel van de betrokken actoren wordt bediend en daardoor verdere versnippering van regelgeving zou ontstaan. Bovendien is de problematiek ook zo veelvormig, dat een wettelijke regeling waarschijnlijk voor een belangrijk deel in bijzondere wetgeving en daarop gebaseerde regelingen moet worden uitgewerkt. Een dergelijke regeling past niet goed bij de doelstellingen van de Awb, die primair is gericht op regeling van leerstukken en onderwerpen die geen nadere uitwerking in bijzondere wetgeving behoeven.

Vervolgens is onderzocht of een kaderwet een geschikt medium zou kunnen zijn. Een kaderwet heeft het voordeel dat daarin de zaken geregeld kunnen worden die momenteel als belemmerend worden gezien voor de gegevensuitwisseling in het algemeen, zoals een duidelijke regeling inzake de bevoegdheid om gegevens uit te wisselen en verduidelijking van de wijze waarop verschillende verstrekkings-

1912170 01165

regimes met elkaar te verenigen zijn. Tegelijkertijd laat een kaderwet ruimte om onderwerpen die specifiek voor een bepaald beleidsterrein gelden, in bijzondere wetgeving en daarop gebaseerde (lagere) regelingen te regelen.

Bedacht moet worden dat het naast elkaar bestaan van een kaderwet en de Wbp weer nieuwe vragen kan oproepen. De Wbp kan echter als uitgangspunt dienen en worden omgebouwd tot een brede wet inzake de gegevensverstrekking. Daarbij moet dan ook de verhouding tot de Wpg en de Wjsg worden geregeld. Denkbaar is dat ook de uitwisseling van strafrechtelijke persoonsgegevens in een brede kaderwet wordt geregeld.

De eis van doelbinding zorgt voor veel vragen. De vraag of het doel waarmee de gegevens zijn verzameld (als dit al duidelijk is) past bij het doel waarvoor ze door een volgende toezichthouder worden gebruikt is vaak moeilijk te beantwoorden. Dit leidt er toe dat veel partijen die over persoonsgegevens beschikken bij twijfel – en die ontstaat dus al heel snel – over de vraag of uitwisseling toegestaan is, dan maar afzien van uitwisseling. In Hoofdstuk 4 zijn drie oplossingen voor dit probleem aangedragen. De eerste mogelijkheid zou zijn het criterium van artikel 9 Wbp (voldoende verwantschap) helderder en concreter te formuleren, zodat een maatstaf bestaat die voor de praktijk beter hanteerbaar is. De tweede mogelijkheid is het laten vallen van de eis van de dubbele doelbinding zoals die nu in de wet geformuleerd is. De derde mogelijkheid is in een nadere regeling specifiek voor een bepaald beleidsterrein op te sommen welke gegevens aan welke toezichthouders verstrekt mogen worden.

Tot nu toe probeert men problemen met betrekking tot de afbakening tussen of de verenigbaarheid van uitwisselingsregimes te voorkomen door in de convenanten die bij het aangaan van een vast samenwerkingsverband worden gesloten afspraken te maken. Deze afspraken zijn meestal dusdanig algemeen dat over de hamvraag – in welke gevallen is het verstrekken van gegevens mogelijk en toelaatbaar – geen duidelijkheid ontstaat, terwijl wel de indruk wordt gewekt dat het convenant de juridische legitimering vormt voor uitwisseling. Verwezen wordt naar paragraaf 5.4.4, waarin is besproken dat in een convenant enkel afspraken kunnen worden gemaakt over bestaande wettelijke bevoegdheden tot uitwisseling.

Sommige problemen, zoals gebrekkige kwaliteit van de verstrekte gegevens, zijn inherent aan de gegevensuitwisseling. Ze betreffen vooral de zorgvuldigheid van het verzamelen en verwerken van gegevens. Regeling in een kaderwet zal daarover weinig meer kunnen bepalen dan wat op grond van de bestaande zorgvuldigheidsnormen geldt.

Al met al concluderen wij dat een algemene wettelijke regeling weliswaar mogelijk is, maar slechts voor een beperkt aantal van de in dit rapport gesignaleerde problemen een oplossing biedt.

1912170 01165

5.6 Aanbevelingen

1. Het verdient aanbeveling de bepalingen uit de Wbp over de voor gegevensverwerking vereiste doelbinding - die nu een belemmering vormen bij de gegevensuitwisseling - te verduidelijken in een kaderwet, eventueel met nadere uitwerking in sectorale wetgeving. Deze bepalingen zouden samen met de bepalingen die thans in de Wbp zijn opgenomen, tot een brede kaderwet omgevormd kunnen worden.

2. Met betrekking tot de eis van doelbinding bij doorverstrekking is het aan te bevelen het criterium van voldoende verwantschap te schrappen. De vraag of twee doelen onverenigbaar zijn, is in de meeste gevallen makkelijker te beantwoorden dan de vraag of er tussen twee doelen voldoende verwantschap bestaat. Als het in artikel 9, tweede lid, Wbp genoemde element van verwantschap van doelen voor toezichthouders zou komen te vervallen, zou dat de eisen die de Wbp op dit punt stelt, voor de praktijk beter hanteerbaar maken.

3. Convenanten zouden niet opgesteld moeten worden met als primair doel te regelen welke gegevens uitgewisseld kunnen worden en tussen welke partijen dat kan. Het centrale probleem bij de gegevensuitwisseling is dat de wettelijke normen die momenteel vaak onduidelijkheid veroorzaken, eerst verduidelijkt moeten worden. Als het al mogelijk zou zijn deze normen in convenanten zodanig te concretiseren dat ermee gewerkt kan worden, is nog niet duidelijk of ze in overeenstemming zijn met de wettelijke normen. Wel kunnen convenanten worden afgesloten ter nadere uitvoering van de wettelijke normen uit een kaderwet of sectorale wetgeving, die al wel concreet genoeg zijn. Het verdient aanbeveling om in een convenant louter praktische en procedurele afspraken te maken tussen de gegevensverstrekker en ontvanger.

4. In het geval dat onwil een factor is bij het uitwisselen van gegevens, zou een wettelijke verplichting tot gegevensuitwisseling overwogen kunnen worden. Een algemene verplichting in een kaderwet lijkt echter niet doelmatig en schiet wellicht over het doel heen. Voldoende is dat in een kaderwet wordt opgenomen dat 'bij of krachtens de wet' een verplichting in het leven kan worden geroepen. Deze verplichting zou uitzondering moeten kunnen lijden om zwaarwegende redenen, die worden geëxpliciteerd in de motivering van de weigeringsbeslissing.

5. In die gevallen waarin niet wordt gekozen voor het invoeren van een wettelijke verplichting tot gegevensverstrekking als in Aanbeveling 4 genoemd, verdient het aanbeveling de afwegingsprocessen die leiden tot weigering van gegevensverstrekking beter inzichtelijk en toetsbaar te maken. Dit kan voorkomen dat overheidsinstanties uitgaan van tegengestelde belangen en daarmee hun eigen organisatiebelang als belangrijkste ijkpunt zien. Verder kan het leiden tot een betere acceptatie van een weigering bij de vragende partij.

6. Aanpassing van wettelijke regels kan helpen bij het oplossen van de hier besproken problemen. Los daarvan verdient het aanbeveling om voor degenen die moeten beslissen over gegevensverstrekking praktische handvatten te ontwikkelen op basis waarvan zij verantwoorde en transparante beslissingen kunnen nemen.

1912170 01165

6. Geraadpleegde bronnen

6.1 Convenanten

Concept- Convenant Ketendossier Vuurwerk (2009).

Convenant gegevensuitwisseling Stichting Naleving CAO voor Uitzendkrachten, (SNCU)/Expertisecentrum Mensenhandel en Mensensmokkel (EMM), 7 juli 2011.

Convenant van 31 mei 2011 tussen de Stichting Autoriteit Financiële Markten en De Nederlandsche Bank N.V. inzake samenwerking en coördinatie op het gebied van toezicht, regelgeving en beleid, (inter)nationaal overleg en andere taken met een gemeenschappelijk belang met betrekking tot de uitvoering van de Wta, Wft, Pw, Wvb en Verordening ratingbureaus, *Stcrt.* 2011, 10 191.

Convenant informatie-uitwisseling integrale aanpak van hennepkwekerijen, Regio Haaglanden (ongedateerd).

Convenant houdende afspraken over de samenwerking in het kader van het Financieel Expertise Centrum van 15 april 2009, *Stcrt.* 2009, nr. 71.

Convenant integrale overheidshandhaving Leeuwarden, december 2008.

G4 Taxiconvenant: Convenant inzake de aanpak van de problematiek met betrekking tot het taxivervoer inde vier grote steden: Amsterdam, Rotterdam, Den Haag en Utrecht, 20 maart 2008, *Kamerstukken II* 2007/08, 25 910, nr. 84.

Informatie-uitwisselingsprotocol OPTA – KLPD/DNR, 30 augustus 2007.

Regionaal convenant RIEC Rotterdam-Rijnmond ten behoeve van de geïntegreerde aanpak van georganiseerde criminaliteit in de regio Rotterdam-Rijnmond, april 2010. [Dit convenant is een regionale uitwerking van het Bestuurlijk Akkoord Geïntegreerde Decentrale Aanpak Georganiseerde Criminaliteit van september 2008, op zijn beurt weer een uitwerking van pijler twee van Bestuurlijke Aanpak Georganiseerde criminaliteit, *Kamerstukken II* 2007/08, 29 911, nr. 11, afkomstig uit het Programma Versterking Aanpak Georganiseerde criminaliteit, *Kamerstukken II* 2007/08, 29 911, nr. 10].

Samenwerkingsprotocol Commissariaat voor de Media - OPTA, december 2008.

1912170 01165

Voorstel voor een nieuw 'Vuurwerkconvenant Overijssel 2007-2012', Bijlage brief SMO/2007-05, 22 mei 2007.

6.2 Literatuur

Boeken, dissertaties, oraties

Braak, S. van den, *Visualiseren van Argumentatie, Informatieverwerking en Leersystemen*, Department of Information and Computing Sciences, Intelligent Systems Group, Utrecht University, The Netherlands, November 28, 2006.

Hildebrandt, M., *De rechtsstaat in cyberspace?* (oratie Nijmegen), Radboud Universiteit Nijmegen, 22 december 2011.

Holvast, J., J.W. Sentrop, P.H. Blok, S.J. Zwenne, J. Nouwt, *Handboek privacy*. Online naslagwerk. Alphen a/d Rijn: Kluwer 2001.

Koelewijn, W.I., *Privacy en politiegegevens. Over geautomatiseerde normatieve informatieuitwisseling*. Leiden: Leiden University Press 2009.

Kranenborg, H.R., L.F.M. Verhey, *Wet bescherming persoonsgegevens in Europees perspectief*. Deventer: Kluwer 2011.

Luchtman, M.J.J.P., *Grensoverschrijdende sfeercumulatie. Over de handhavingssamenwerking tussen financiële toezichthouders, fiscale autoriteiten en justitiële autoriteiten in EU-verband* (diss. Universiteit Utrecht), Wolf Legal Publishers, 2007.

Muijen, P.J.D.J., *Politie, informatie en privacy: de Wet politiegegevens toegelicht*, 'Zutphen: Uitgeverij Kerckebosch 2012.

Vrie, N.J. van de, *Wet eenmalige gegevensuitvraag werk en inkomen*. Deventer: Kluwer 2008.

Artikelen

Albers, C.L.G.F.H., P.C.M. Heinen, 'Een (verkapte) civielrechtelijke immuniteit voor toezichts- en handhavingsfalen van overheidsorganen?', *De Gemeentestem* 2010, 101.

Biezeveld, G.A., 'Illegaal vuurwerk: biedt Pyrorichtlijn uitzicht op oplossing?' *Tijdschrift voor Omgevingsrecht* 2010, nr. 2, p. 47-51.

Bitter, C.M. , & F.W. Bleichrodt, 'Informatievoorziening in het kader van de bestuursrechtelijke aanpak van criminaliteit en terrorisme', in: *Bestuursrechtelijke aanpak van criminaliteit en terrorisme* (VAR-reeks 138), Den Haag: Boom Juridische Uitgevers 2007.

Boswijk, P., O.J.D.M.L. Jansen & R.J.G.M. Widdershoven, 'De wettelijke implementatie van administratieve samenwerking in de Europese Unie', *RegelMaat* 2009 (24) 6, p. 322-340.

Evelien Brouwer, 'Legality and Data Protection Law: The Forgotten Purpose of Purpose Limitation', Chapter 14 in: Leonard Besselink, Frans Pennings en Sacha Prechal (eds.), *The Eclipse of the Legality Principle in the European Union*, Deventer: Kluwer 2011, p. 273-294.

Buruma, Y., 'Het recht op vergetelheid. Politiële en justitiële gegevens in een digitale wereld', in: D. Broeders, C. M.K.C. Cuijpers & J.E.J. Prins (red.), *De staat van informatie* (WRR-verkenning nr. 25), Amsterdam: Amsterdam University Press 2011, p. 165-222.

Duijkersloot, Ton, en Henk Kummeling, Parlement en geheime toezichtsinformatie, in: H.R.B.M. Kummeling e.a. (red.), *De samengestelde Besselink, Bruggen bouwen tussen nationaal, Europees en internationaal recht*, Oisterwijk: Wolf Legal Publishers 2012, p. 75-82.

Groothuis, M.M., 'De digitale overheid en de Awb. Bestuursrechtelijke aspecten van elektronische communicatie', Preadviezen VAR-reeks nr. 146, *De digitale overheid*, Den Haag: Boom Juridische

1912170 01165

uitgevers 2011, p. 7-70.

Kohnstamm,J., L. Dubbbeld, 'Glazen samenleving in zicht', *NJB* 2007, nr. 37, p. 2369-2375.

Luut, M. L., 'Nieuwe wetgeving - De Wet politiegegevens: herziening van de Wet politieregisters', *Ars aequi*, 2008-4, p. 303-307.

Maanen, G.E. van, 'Overheidsaansprakelijkheid voor gebrekkig Toezicht. Weging van argumenten en juridische technieken naar aanleiding van de Enschedese vuurwerkramp', *Rechtsgeleerd Magazijn THEMIS* 2007-4, p. 127-140.

Ottow, A.T., 'Toezicht en samenwerking', *Samenwerken met de NMa. NMa jaarverslag 2010*, p. 46-50.

Ottow, A.T., 'Het recht op informatie van toezichthouders', annotatie van: CBb 11 februari 2010, Stichting A Ziekenhuis Groep/Nederlandse Zorgautoriteit, LJN BL3730, *M&M*, december 2010, nr. 6, p. 238-240.

Prins, J.E.J., 'Function creep en privacy', *Justitiële verkenningen* 2011, 37, nr. 8, p. 9-21.

Prins, J.E.J. (Corien), 'De eOverheid voorbij. Recht doen aan de digitale werkelijkheid', Preadviezen VAR-reeks nr. 146, *De digitale overheid*, Den Haag: Boom Juridische uitgevers 2011, p. 71-116.

Prins, J.E.J. (Corien) , 'Over privacy and dingen die voorbijgaan', Vooraf in: *NJB* 2008, p. 145.

Prins, J.E.J. (Corien), 'Politiegegevens: laveren tussen wet en praktijk', Vooraf in: *NJB* 2005, p. 725.

Rossum, A.A. van, 'Civielrechtelijke aansprakelijkheid voor overheidstoezicht', in: A.A. van Rossum, L.F.M. Verhey, N. Verheij, *Toezicht*. Preadviezen. Handelingen Nederlandse Juristenvereniging, 135, 2005-1, p. 37 e.v.

Schillemans, C.E., 'Informatie-uitwisseling en het mededingingsrecht', M&M, oktober 2010, nr. 5, p. 176-183.

Schuyt, C.J.M., 'Overheid en burger in het digitale tijdperk: een vergelijking met vele onbekenden', Preadviezen VAR reeks nr. 146, *De digitale overheid*, Den Haag: Boom Juridische uitgevers 2011, p. 117-162.

Sickinghe, F., 'Fusie NMa, OPTA en Consumentenautoriteit. Kwaliteitsoffer voor kostenbesparingen?', *Mediaforum* 2011-7/8, Themanummer 'De nieuwe marktautoriteit', p. 203-204.

Steyger, E., 'Een cocktail van NMa, OPTA en Consumentenautoriteit: stirred or seriously shaken?', *Mediaforum* 2011-7/8, Themanummer 'De nieuwe marktautoriteit', p. 205-209.

Zwenne, G.J. , 'Over persoonsgegevens en IP-adressen, en de toekomst van privacywetgeving', in: L. Mommers (red.), *Het binnenste buiten. Liber amicorum ter gelegenheid van het emeritaat van prof. dr. Aernout H.J. Schmidt, hoogleraar Recht en Informatica te Leiden*, Leiden: eLaw 2010, p. 321-342.

Rapporten en adviezen

Adviescommissie Veiligheid en persoonlijke levenssfeer (Commissie Brouwer-Korf), *Gewoon doen, beschermen van veiligheid en persoonlijke levenssfeer*, Evaluatie Wet bescherming persoonsgegevens, *Kamerstukken II*, 2009/10, 31 051, nr. 5.

Advies van de Commissie Mans, onderzoeksteam herziening handhavingsstelsel VROM-regelgeving, *De tijd is rijp*, juli 2008. Zie: *Kamerstukken II* 2007/08, 22 343, nr. 201.

Advies Raad van State nr. W06.11.0053/III, inzake 'de spanning die is gesignaleerd tussen de mogelijke verstrekking van vertrouwelijke toezichtinformatie door de Minister van Financiën, De Nederlandsche Bank (DNB) en de Autoriteit Financiële Markten (AFM) aan de Parlementaire Enquêtecommissie Financieel Stelsel (PEFS) en de geheimhoudingsverplichtingen op grond van het op Europese richtlijnen gebaseerde stelsel van geheimhouding, neergelegd in artikel 1:89 en verder van de Wet op het financieel toezicht (Wft)', 11 maart 2011, *Stcrt.* 2011, 5695.

Berenschot, *Burgers beter bediend?* Eindrapportage beleidsdoorlichting artikel 33 [van de begroting 2010 van

1912170 01165

het Ministerie van BZK], 27 april 2011.

Berkelaar, Tim, Marc Gerrard, Peter Nooteboom, *Naar een gezamenlijke Inspectieview Milieu. Eindrapportage verkenning verbetering informatie-uitwisseling Milieuhandhaving*, ICTU 22 augustus 2010.

Boswijk, P., O.J.D.M.L. Jansen, R.J.G.M. Widdershoven, *Transnationale samenwerking tussen toezichthouders in Europa*, WODC 2008.

Eindrapport Commissie Oosting (Commissie Onderzoek Vuurwerkramp), *De vuurwerkramp*. Enschede-Den Haag, 28 februari 2001.

Eindrapport van de projectgroep Integratie en vereenvoudiging toezicht op (publieke) uitvoering, *Beter bestuurlijk toezicht. Hoe departementent de governance ten aanzien van zelfstandige organisaties met een publieke taak kunnen verbeteren*. Deel I, Den Haag, 15 december 2004.

Kwink groep, TNO, Berenschot, *Evaluatie OPTA*, 31 augustus 2009. Bijlage 3: 'Nadere beschouwing samenwerkingsrelaties'.

Lulofs, Kris, Hans Bressers, Annemieke Boeren, *Meta-evaluatie van veranderingen in beleid en praktijk rond de Nederlandse vuurwerksector*, Enschede: Universiteit Twente, 4 mei 2005.

Projectgroep Emergo, *De gezamenlijke aanpak van de zware (georganiseerde) misdaad in het hart van Amsterdam*, Uitgeverij Boom, Amsterdam 2011. Bijlage bij *Kamerstukken II* 2011/12, 29 911, nr. 55.

Raad voor Verkeer en Waterstaat en de VROM-raad, *Verantwoorde risico's, veilige ruimte*, Advies 037, juni 2003.

Rapport bevindingen College bescherming persoonsgegevens (Cbp), *Verwerking van persoonsgegevens door Fraude Interventieteams Onderzoek bij interventieteam "Vakantietijd; integrale controles bij recreatiebedrijven en campings"*, juli 2009.

Rapport van de werkgroep herijking toezichtregelgeving, 20 augustus 2008, bij brief van 29 oktober 2008 aan de kamer aangeboden, *Kamerstukken II* 2008/09, 31 700 VI, nr. 70.

Rapport van de Taskforce Toekomstvisie Taxi, onder voorzitterschap van Hugo B. Roos, *Toekomst voor de taxi*, Amsterdam, juni 2008.

Rapport Samenwerking UWV en Belastingdienst, *Eindrapportage werking van de loonaangifteketen in 2010*, 24 mei 2011.

Rapport BZK *Overheidsbrede implementatieagenda voor dienstverlening en e-overheid*, Bijlage bij *Kamerstukken II* 2010/11, 26 643, nr. 182.

Stuurgroep Kruispuntbank, *Uitwisseling van handhavingsinformatie. Conclusies en aanbevelingen van de LOM (Landelijk Overleg Milieuhandhaving)*, Eindversie Den Haag, 16 juni 2010.

TNO, Tilburg Institute for Law, Technology and Society (Tilt), *Trusted technology. Een onderzoek naar de toepassingsvoorwaarden voor Privacy by Design in de elektronische dienstverlening van de overheid*, 5 december 2011.

Veiligheidshuis Fryslân. Onderzoek naar de verwerking van persoonsgegevens in het kader van het Justitieel Casusoverleg en JCO-Support, Rapportage van definitieve bevindingen (CBP z2010-00827).

Voortgangsrapportage over de maatregelen op de Amsterdamse taximarkt. Dienst Infrastructuur Verkeer en Vervoer, *Voortgang "Naar een gezonde taximarkt"*. Gemeente Amsterdam, 18 november 2009.

Voortgangsrapportage *Programma Vernieuwing Toezicht*, Inspectieraad, januari 2009.

Wetenschappelijke Raad voor het Regeringsbeleid, *iOverheid*, WRR-rapport 86, Amsterdam: University Press 2011.

Winter, H.B., *Wat niet weet, wat niet deert: een evaluatieonderzoek naar de werking van de Wet bescherming persoonsgegevens in de praktijk*, Rapport uitgebracht door Pro Facto RuG en de Vakgroep Bestuursrecht en Bestuurskunde van de RuG in opdracht van het WODC, Den Haag: Boom Juridische uitgevers, 2009.

1912170 01165

Zenc (Noor Huijboom, Marco Meesters, Roeland de Graaf), Concept-Eindrapportage *LOM Kruisppunt in Milieuhandhaving*, in opdracht van LOM, juli 2005.

Zwenne, Gerrit-Jan, Anne-Wil Duthler, Marga Groothuis, Hugo Kielman, Wouter Koelewijn, Laurens Mommers, Rapport *Eerste fase evaluatie Wet bescherming persoonsgegevens, Literatuuronderzoek en knelpuntenanalyse*, december 2007. Zie: *Kamerstukken II*, 2007/08, 31 051, nr. 1 en 2.

Zeeuw, J. de, *Informatieverstrekking door de fiscus. Ontheffing van de fiscale geheimhoudingsplicht in het licht van privacywetgeving*, Registratiekamer, december 1999.

6.3 Regelgeving en beleidstukken

EU

Besluit 2008/615/JBZ inzake de intensivering van de grensoverschrijdende samenwerking, in het bijzonder ter bestrijding van terrorisme en grensoverschrijdende criminaliteit, *PbEU* 2008, L 210.

Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie), *PbEG* 2002, L 201/37.

Richtlijn 2011/16/EU betreffende de administratieve samenwerking op het gebied van de belastingen en tot intrekking van Richtlijn 77/799/EEG, *PbEU* 2011, L 64.

Verordening (EU) nr. 904/2010 betreffende de administratieve samenwerking en de bestrijding van fraude op het gebied van de belasting over de toegevoegde waarde, *PbEU* 2010, L 268.

'Een integrale aanpak van de bescherming van persoonsgegevens in de Europese Unie'. Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's, 4 november 2010, COM(2010) 609 def.

Voorstel voor een richtlijn van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens, Brussel, 25 januari 2012, COM(2012) 10 final.

Voorstel voor een Verordening van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (algemene verordening gegevensbescherming), Brussel, 25 januari 2012, COM(2012) 11 final.

'Privacywaarborging in het online tijdperk. Een Europees gegevensbeschermingskader voor de 21e eeuw', Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's, Brussel, 25 januari 2012, COM(2012) 9 final.

Duitsland

Artikel 35 Grundgesetz, Rechts- und Amtshilfe, Kompetenzüberschreitendes Zusammenwirken bei Notfällen, in: Dr. Michael Sachs, *Grundgesetz, Kommentar*, 3. Auflage, Verlag C.H. Beck, München 2003, p. 1194-1205.

Nederland

Kamerstukken

Kamerstukken II 2011/12, 22 112, nr. 1239, Nieuwe Commissievoorstellen en initiatieven van de lidstaten van de Europese Unie. Brief van de Staatssecretaris van Buitenlandse Zaken, Fiche: Verordening Interne Markt Informatiesysteem (IMI), 10 oktober 2011.

1912170 01165

Kamerstukken II, 2010/11, 26 643, nr. 177, Informatie- en communicatietechnologie (ICT), Verslag van een algemeen overleg, 17 maart 2011.

Kamerstukken II 2011/12, 26 643, nr. 211, Kabinetsreactie op WRR-rapport *iOverheid*: de rol van de overheid in de iSamenleving).

Kamerstukken II 2005/06, 27 831, nr. 15. Kaderstellende Visie op Toezicht (KVOT), *Minder last, meer effect; zes principes van goed toezicht.*

Kamerstukken II 2003/04, 29 362, nr. 1. Modernisering van de overheid. Kabinetsvisie *Actieprogramma 'Andere Overheid'.*

Kamerstukken II 2009/10, 29362, nr. 176. *Uitvoeringsagenda Stelsel van Basisregistraties 2010-2015.*

Kamerstukken II 2007/08, 31 051. *Evaluatie Wet bescherming persoonsgegevens.*

Kamerstukken II 2007/08, 31 201, nr. 3 (Trendnota Arbeidszaken Overheidspersoneel 2008), *Nota Vernieuwing Rijksdienst.*

Kamerstukken II 2007/08, 31 201, nr. 25, *Programma Vernieuwing Toezicht.*

Kamerstukken II 2007/08, 31 490, nr. 1. *Programma Vernieuwing Rijksdienst.*

Kamerstukken II 2010/11, 31 490, nr. 54. *Compacte Rijksdienst: Uitvoeringsprogramma.*

Kamerstukken II 2008/09, 31 700 VI, nr. 70. Bijlage: Rapport van de werkgroep herijking toezichtregelgeving.

Kamerstukken II 2010/11, 32 255, nrs. 6, 8 en 9. Het systeem van toezicht op de stabiliteit van financiële markten (inzake de juridische aspecten van het verkrijgen van toegang door de Algemene Rekenkamer tot bedrijfsdossiers bij DNB), februari – juni 2011.

Kamerstukken II 2010-11, 32 500 XI, nr. 10 Lijst van vragen en antwoorden over het Ontwerpbesluit tot wijziging van het Vuurwerkbesluit en enkele algemene maatregelen van bestuur (verbetering uitvoerbaarheid en handhaafbaarheid Vuurwerkbesluit, *Kamerstukken II* 32 500 XI, nr. 4).

Kamerstukken II 2010/11, 32 676, nr. 3 MvT (de Evaluatie- en Uitbreidingswet Bibob).

Kamerstukken II 2010/11, 32 761, nr. 1. Verwerking en bescherming persoonsgegevens. Brief van de Staatssecretaris van Veiligheid en Justitie en de Minister van Binnenlandse Zaken en Koninkrijksrelaties, 29 april 2011.

Kamerstukken II 2010/11, 32 761, nr. 1. Reactie op schriftelijke vragen Eerste Kamer ter voorbereiding van het debat digitale dataverwerking.

Kamerstukken II 2011/12, 32 761, nr. 2. Verwerking en bescherming persoonsgegevens. Verslag van een algemeen overleg.

Kamerstukken II 2011/12, 33 186, Regels omtrent de instelling van de Autoriteit Consument en Markt (Instellingswet Autoriteit Consument en Markt), nr. 3, memorie van toelichting.

Kamerstukken II 2011/12, 33 186, Regels omtrent de instelling van de Autoriteit Consument en Markt (Instellingswet Autoriteit Consument en Markt), nr. 5, Verslag vaste commissie voor Economische Zaken, Landbouw en Innovatie.

Beleid lagere overheden

Toelating en toezicht op de Amsterdamse Taximarkt: nieuw samenspel tussen klanten, branche, gemeente en partners, Uitwerking Hoofdlijnenplan Taxi, 11e versie, 8 december 2011.

Gemeente Amsterdam, *Hoofdlijnennotitie taxibeleid*, 2009.

Dienst Infrastructuur Verkeer en Vervoer (dIVV), *Naar een gezonde taximarkt in Amsterdam*, Gemeente Amsterdam, 6 mei 2009.

1912170 01165

6.4 Jurisprudentie

Europees Hof voor de Rechten van de Mens

EHRM 28 april 2009, nr. 32881/04 (*K.H. e.a./Slowakije*).

EHRM 4 december 2008, nr. 30562/04 en 30566/04 (*S. en Marper/Verenigd Koninkrijk*).

EHRM 17 juli 2008, nr. 20511/03 (*I/Finland*).

EHRM 3 april 2007, *NJ* 2007-50, nr. 617 (*Copland/Verenigd Koninkrijk*).

EHRM 4 januari 2007, nr. 39658/05 (*Smith/Verenigd Koninkrijk*).

EHRM 16 april 2002, nr. 37971/97 (*Société Colas Est e.a./Frankrijk*).

EHRM 3 mei 2001, nr. 31827/96, *NJ* 2003, 354 (*JB/Zwitserland*).

EHRM 4 mei 2000, nr. 28341/95 (*Rotaru/Roemenië*).

EHRM 16 februari 2000, nr. 27798/95 (*Amann/Switzerland*).

EHRM 25 februari 1997, nr. 22009/93 (Z./Finland).

EHRM 17 december 1996, nr. 19187/91, *NJ* 1997, 699 (*Saunders/Verenigd Koninkrijk*).

EHRM 16 december 1992, nr. 13710/88 (*Niemietz/Duitsland*).

EHRM 7 juli 1989, nr. 10454/83 (*Gaskin/Verenigd Koninkrijk*).

EHRM 26 maart 1987, nr. 9248/81 (*Leander/Sweden*).

EHRM 2 augustus 1984, nr. 8691/79, *NJ* 1988, 534 (*Malone/Verenigd Koninkrijk*).

EHRM 6 september 1978, nr. 5029/71 (*Klass e.a./Duitsland*).

Hof van Justitie van de Europese Gemeenschappen / Europese Unie

HvJ EG 24 november 2011, nr. C-468/10 en C-469/10 *(ASNEF en FECEMD)*.

HvJ EG 9 november 2010, nr. C-92/09 en C-93/09 (*Volker und Markus Schecke GbR en Hartmut Eifert*).

HvJ EG 29 juni 2010, nr. C-28/08 P (*Europese Commissie/The Bavarian Lager* Co. Ltd.).

HvJ EG 6 november 2003, nr. C-101/100 (*Lindqvist*).

HvJ EG 12 juni 2003, nr. C-112/00 (*Schmidberger*).

Nederland[147]

Hoge Raad

HR 9 september 2011, LJN BQ8097, *NJ* 2011, 595 (artikel 8, 36, 46 Wbp en artikel 8 EVRM).

HR 9 juli 2010, *LJN* BM2311, *NJ* 2010, 416 *(Begrip politieregister of register in artikel 1, eerste lid, aanhef en onder c, Wet politieregisters)*.

HR 23 maart 2010, LJN BK6331, *NJ* 2010, 355 (*Gevoelige informatie artikel 126nd Sv jo artikel 126nf Sv*).

147 Alle uitspraken zijn te vinden op rechtspraak.nl. Als zij ook elders gepubliceerd zijn, wordt dit vermeld.

1912170 01165

Afdeling Bestuursrechtspraak Raad van State

ABRvS 16 november 2011, *LJN* BU4567 (*artikel 35, tweede lid, Wbp*).

ABRvS 5 oktober 2011, *LJN* BT6640 (artikel 25, 28 en 29 Wpg).

ABRvS 27 april 2011, *LJN* BQ2630 (*'Brummenlijn': beginsel van procesrecht).*

ABRvS 29 september 2010, *LJN* BN8578 (*artikel 10, tweede lid, aanhef en onder d, Wob*).

ABRvS 8 september 2010, *LJN* BN6172, *JB* 2010, 233 (artikel 3, 36 en 45 Wbp).

ABRvS 12 mei 2004, *LJN* AO9207, *JB* 2004, 251.

Centrale Raad van Beroep

CRvB 16 november 2011, *LJN* BU6392, *AB* 2012, 39, *JB* 2012, 18.

CRvB 24 juni 2008, *LJN* BD5289, *AB* 2008, 286.

Gerechtshoven

Gerechtshof Amsterdam

Hof Amsterdam 18 oktober 2010, LJN BO6031 (artikel 359a, eerste lid, Sv; persoonsgegevens gebruikt voor een ander doel dan waarvoor zij waren verzameld).

Gerechtshof Arnhem

Hof Arnhem 16 juni 2010, LJN BM8111, *NJFS* 2010, 279 (bewijsuitsluiting; *onrechtmatig verkregen Automatic Number Plate Recognition (ANPR) gegevens).*

Gerechtshof 's-Gravenhage

Hof 's-Gravenhage 6 februari 2012, LJN BV3488 (Openlijk geweld Ajax-supporters; Wet politieregisters).

Hof 's-Gravenhage 24 augustus 2010, *LJN* BN4316 (*Vuurwerkramp Enschede. Geen aansprakelijkheid overheid).*

Rechtbanken

Rechtbank Amsterdam

Rb. Amsterdam 9 februari 2012, LJN BW0269 (Wbp. Incidentenregister. *Gerechtvaardigd belang bank verwerking persoonsgegevens).*

Rb. Amsterdam 26 januari 2012, LJN BV2297 (*Wbp. Incidentenregister. Gerechtvaardigd belang van de bank verwerking persoonsgegevens).*

Rechtbank Arnhem

Rb. Arnhem 5 april 2011, LJN BQ0140 (Wbp; *Richtlijn 2005/85/EG van de Raad van de Europese Unie van 1 december 2005 (Procedurerichtlijn)).*

Rb. Arnhem 9 maart 2010, LJN BL7288 (*artikel 10, tweede lid, aanhef en onder c, g en e Wob).*

Rechtbank 's-Gravenhage

Rb. 's-Gravenhage 13 april 2012, *LJN* BW2236, *NTFR* 2012, 937.

Rechtbank 's-Hertogenbosch

Rb. 's-Hertogenbosch 30 mei 2011, *LJN* BQ7115 (*artikel 27, eerste lid, aanhef en onder b, Wpg).*

Rechtbank Haarlem

Rb. Haarlem 16 mei 2012, *LJN* BW7578

Rechtbank Leeuwarden

Rb. Leeuwarden 1-07-2011, *LJN* BR4918, AWB 10/2311 (artikel 1, 35, 36 Wbp).

Rb. Leeuwarden 2 september 2010, *LJN* BO9303 (artikel 1, 35, 43 Wbp).

1912170 01165

Rechtbank Middelburg
Rb. Middelburg 22 maart 2012, *LJN* BW0570 (verstrekkingenregiem Wpg).

Rb. Middelburg 15 maart 2012, *LJN* BV8942 (prejudiciële vragen aan HvJEU inzake artikel 2 en 12 Privacyrichtlijn).

Rechtbank Roermond
Rb. Roermond 25 februari 2011, *LJN* BP6001 (artikel 25 Wpg).

Rechtbank Rotterdam
Rb. Rotterdam 5 augustus 2010, *LJN* BN3651 (artikel 28, eerste lid, Wpg).

Rb. Rotterdam 24 maart 2009, *LJN* BH7631 (artikel 49 en 50 Wbp; onrechtmatigheid publicatie op internet van persoonsgegevens zonder toestemming).

Rechtbank Utrecht
Rb. Utrecht 26 augustus 2011, *LJN* BR5924 (*juridische betekenis van het Regionaal Convenant Geïntegreerde Decentrale Aanpak Georganiseerde Misdaad regio Midden-Nederland).*

Rb. Utrecht 13 oktober 2010, LJN BO0351, *NJF* 2010, 450 (*artikel 22, vierde lid, sub c, Wbp*).

Rechtbank Zwolle
Rb. Zwolle 5 december 2011, *LJN* BV2799 (*Promis, vormverzuim ex artikel 359a Sv).*

Rb. Zwolle 17 maart 2009, LJN BH6275 (*verstrekkingenregime Wpg).*

College Bescherming Persoonsgegevens
CBP 12 juli 2006, nr. 2005-1447.

1912170 01165

7. Bijlagen

7.1 CV Onderzoekers

Adrienne de Moor-van Vugt is hoogleraar Staats- en bestuursrecht aan de UvA. Zij geeft leiding aan de onderzoeksgroep Marktordening en is verbonden aan het Centrum voor Energievraagstukken. Tot 2004 was zij verbonden aan de Universiteit van Tilburg, de laatste jaren als hoogleraar Bestuurlijk handhavingrecht en Europees bestuursrecht. Tussen 2004 en 2008 was zij raadsheer bij het College van Beroep voor het bedrijfsleven. Vakinhoudelijk heeft zij zich in haar carrière met een breed scala aan bestuursrechtelijke onderwerpen beziggehouden. Deze omvatten onder meer de relatie tussen Nederlands bestuursrecht en het Europees recht, vraagstukken rond toezicht, de Wet Bibob en de Algemene wet bestuursrecht. Zij is lid van de Kwaliteitscommissie Wet Bibob, was voorzitter van de WODC-begeleidingscommissie *De Europese agenda van de Awb* en onder meer lid van de Commissie Rechts-bescherming van de VAR en van de Commissie Ilsink.

Tom van Engers is hoogleraar Juridisch Kennismanagement aan de Universiteit van Amsterdam en directeur van het Leibniz Center for Law. Van Engers studeerde Cognitieve Kunstmatige Intelligentie aan de Universiteit Utrecht en promoveerde aan de faculteit Wiskunde en Informatica aan de Vrije Universiteit te Amsterdam. Hij werkt sinds 1983 op het terrein van de rechtsinformatica en was gedurende tien jaar hoofd research bij onderzoekafdeling Artificial Intelligence and Audit Automation van het Ministerie van Financiën. Het rechtswetenschappelijk onderzoek van Van Engers is daarnaast met name gericht op effecten van wetgeving. Hij is adviseur voor verschillende overheidsdiensten, zoals de Belastingdienst, Immigratie en Naturalisatie Dienst en Kadaster. Meer informatie over Van Engers of het Leibniz Center for Law is te vinden op <www.LeibnizCenter.org>.

1912170 01165

Arnout Klap is gepromoveerd op een onderzoek naar vage normen in het bestuursrecht. Hij werkte als universitair docent in Leiden en Utrecht, voordat hij universitair hoofddocent werd aan de UvA. Hij was lid van de Algemene Bezwaar- en Beroepcommissie Amsterdam Zuid en voorzitter Algemene Bezwaar- en Beroepcommissie Amstelveen. Thans is hij rechter-plaatsvervanger bij de rechtbank Amsterdam. Zijn expertise is gelegen op het gebied van het bestuursprocesrecht, beleidsregels en de bestuursrechtspraak. Hij werkte mee aan de evaluatie van de Awb in 2001 en 2006 en was medeauteur van de rapporten *De burger en de Awb, Ervaringen van repeat players met Awb-procedures* (2001) en *Definitieve geschilbeslechting door de bestuursrechter* (2006).

Taco Groenewegen is universitair docent bestuursrecht aan de UvA. Hij is gepromoveerd op een onderzoek naar wetsinterpretatie en rechtsvorming door de bestuursrechter en de burgerlijke rechter. Hij publiceert op het gebied van het algemene bestuursrecht, bestuursrechtelijke sancties, vreemdelingenrecht en rechtstheorie. Hij werkte mee aan de evaluatie van de Awb in 2006 en was medeauteur van het rapport Definitieve geschilbeslechting door de bestuursrechter (2006).

Wouter van Haaften is promovendus invoering van nieuwe wetgeving door uitvoeringsorganisaties bij de vakgroep Juridisch Kennismanagement (promotor: Tom van Engers). Na een start als wetgevingsjurist op het Ministerie van Financiën was hij binnen het DG Belastingdienst-handhavingsbeleid in de jaren negentig belast met de uitwisseling van zowel fiscale als niet fiscale gegevens (vb Sofinummers) met andere overheidsorganen. Verder was hij voorzitter van de kennisgroep Juridische inbedding van het Elektronisch berichtenverkeer en adviseerde hij namens de Belastingdienst bij de aanpassing van de AWB in dit kader (Wet elektronisch bestuurlijk verkeer). Na 2003 was hij ondermeer programmamanager ICT en administratieve lastenverlichting bij het Ministerie van Economische zaken, programmamanager Basisregistraties (o.m. basisregistratie Inkomen) bij de Belastingdienst en bij ICTU betrokken bij de vormgeving van de elektronische overheid.

Aernout Nieuwenhuis is universitair hoofddocent Staatsrecht van de UvA. Daarnaast is hij verbonden aan het Instituut voor Informatierecht (IViR) en redacteur van het tijdschrift Mediaforum. In 1991 promoveerde hij op Persvrijheid en persbeleid, een rechtsvergelijkend onderzoek naar de verhouding tussen de grondrechtelijke onthoudingsplicht en overheidsingrijpen tegen persconcentratie. Hij verrichtte van 1994 tot 1999 rechtsvergelijkend onderzoek bij de KNAW dat is uitgemond in de studie Over de grens van de uitingsvrijheid (Nijmegen 1997, 2e druk 2006). Verder verscheen van zijn hand een studie naar de reikwijdte van het grondrecht op privacy, Tussen privacy en persoonlijkheidsrecht (Nijmegen 2001) en is hij co-auteur van het boek Uitingsdelicten (2e druk, Deventer 2008). Hij publiceert regelmatig over de (grenzen van de) grondrechten vrijheid van meningsuiting en privacy in de vorm van artikelen, annotaties of preadviezen.

Marleen Wessel is promovenda Financieel Toezicht bij de leerstoelgroep Staats- en bestuursrecht van de UvA (promotor: Adrienne de Moor-van Vugt). In haar onderzoek vergelijkt zij regulering van financieel systeemrisico in de Europese Unie en de Verenigde Staten. Zij heeft tevens onderzoekservaring als historicus.

Lentine Schouten studeerde politicologie aan de UvA en is thans bezig met haar master Staats- en Bestuursrecht. Daarnaast is zij als docent rechtsfilosofie verbonden aan de Faculteit der Rechtsgeleerdheid.

1912170 01165

7.2 Vragen enquête en resultaten

7.2.1 Resultaten

Nadat de interviews waren verwerkt in de vragenlijsten konden de enquêtes worden uitgezet. Ongelukkigerwijs viel het moment van uitzetten samen met het begin van een voorjaarsvakantieperiode van 2 weken. Daardoor verliep het retourneren van de ingevulde formulieren minder snel dan werd verwacht.

Bestuurlijke toezichthouders/uitvoeringsorganisaties

Van de eerste doelgroep, de uitvoeringsorganisaties, werden in totaal 12 formulieren ontvangen. Deze formulieren kwamen met name van de gemeente Amsterdam en de Belastingdienst, de partners in de casus 1 en 2. De belangrijkste resultaten zijn hierna beschreven.

Cluster 1

De eerste vraag betrof het aanbrengen van rangorde in de belangen die spelen bij gegevensuitwisseling met als vertrekpunt bestuursrechtelijk informatievoorziening vanuit het perspectief van de leverancier.

	Aangevulde belangen:			- Algemeen belang - Belang van de juistheid van de gegeven				
Perspectief Leverancier	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Doelbinding	7	2	1	1				
Privacy subject		1	1	6	1	2		
Privacy derde			3	1	3	1	2	1
Geheimhouding	2	4	2		2		1	
Kosten verstrekken		2		0	1	6	2	
Eigen baten, wederkerigheid	1	2	2	0	3		2	1
Baten ontvanger	1		2	3		1	4	
Andere					1	1		9
	11	11	11	11	11	11	11	11

De drie belangen die door de medewerkers van uitvoeringsorganisatie's vanuit het perspectief van de leverancier bovenaan werden gezet zijn in rood aangegeven. Doelbinding wordt zeer belangrijk gevonden, liefst 10 van de 11 deelnemers plaatsen dit belang in de top 3. Daarna volgt geheimhouding met 8 stemmen in de top 3. Het meer 'informele organisatiebelang wederkerigheid' scoort met 5 stemmen de derde plek. Van de gelegenheid om een nog niet genoemd belang in te brengen werd spaarzaam gebruik gemaakt. De twee belangen die genoemd werden waren: het algemeen belang en het belang van de juistheid van de gegevens.

De kosten van de verstrekking speelde voor de respondenten geen grote rol.

Ten aanzien van de kwaliteit van de eigen, geleverde gegevens was men positief zoals uit onderstaand staatje blijkt. De gestelde vraag was:

Is de geleverde informatie:

Tijdig	**47**				
Compleet		**51**			
Betrouwbaar			**56**		
Actueel				**50**	
Passend					**46**
Maximaal	55	55	55	55	55
Gemiddeld	3,9	4,3	4,7	4,2	3,8

De scores waren over het algemeen goed, waarbij opvalt dat de tijdigheid en de passendheid van de informatie wat minder worden gewaardeerd. Vooral de betrouwbaarheid van de eigen gegevens wordt relatief hoog ingeschat.

1912170 01165

Cluster 2

Het tweede cluster vragen moest rangorde aanbrengen in de belangen die spelen bij gegevensuitwisseling met als vertrekpunt bestuursrechtelijk informatievoorziening vanuit het perspectief van de ontvanger.

	Aangevulde belangen:			- Het algemeen belang bij de uitwisseling - Belang van de juistheid van de gegevens				
Perspectief Ontvanger	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Doelbinding	4	5	2	1				
Privacy subject	1		4	3		2	1	
Privacy derde		1	1	3	2	1	2	1
Geheimhouding		3	1	1	5		1	
Kosten verstrekken				1	2	3	4	
Baten leverancier		1	2	1		5	2	1
Baten ontvanger	7	2	1		2			
Andere			1	1			1	9
	12	12	12	11	11	11	11	11

De drie belangen die door de medewerkers van uitvoeringsorganisatie's vanuit het perspectief van de ontvanger bovenaan werden gezet zijn weer in rood aangegeven. Doelbinding wordt ook door de ontvanger zeer belangrijk gevonden, 11 van de 12 deelnemers plaatsen dit belang in de top 3. Daarna volgen de eigen baten van de ontvanger met 10 stemmen. De privacy van het subject komt met 5 stemmen op een derde plaats. Ook hier werd weer van de gelegenheid om een nog niet genoemd belang in te brengen werd spaarzaam gebruik gemaakt. De twee belangen die genoemd werden waren: het algemeen belang en het risico van het niet ontvangen van de gegevens.

Ten aanzien van de kwaliteit van de van de andere organisatie ontvangen gegevens was men positief zoals uit onderstaand staatje blijkt. De gestelde vraag was:

Is de geleverde informatie:

Tijdig	**56**				
Compleet		**54**			
Betrouwbaar			**45**		
Actueel				**54**	
Passend					**45**
Maximaal	60	60	60	60	60
Gemiddeld	4,7	4,5	3,8	4,5	3,8

Ook hier goede scores op tijdigheid, compleetheid en actualiteit. Minder hoog scoorden betrouwbaarheid en passendheid van de ontvangen gegevens. De betrouwbaarheid van de ontvangen gegevens wordt lager ingeschat dan door de leverancier. De tijdigheid wordt hoger ingeschat, terwijl de passendheid van de gegevens opmerkelijk genoeg door leverancier en ontvanger gelijk worden gewaardeerd.

Cluster 3

Bij dit cluster moesten de respondenten vanuit het leveranciers perspectief de rangorde aanbrengen in de belangen die spelen bij gegevensuitwisseling waarbij een opsporingsorganisatie is betrokken.

	Aangevulde belangen: Het risico of het effect van niet leveren							
Perspectief Leverancier aan opsporing	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Doelbinding	6	2	1	2				
Privacy subject	1	1	3	1	2		1	2
Privacy derde		2	2		1	3	1	1
Geheimhouding	3	2	1	2	2		1	
Kosten verstrekken		1	1	1	2	3	2	
Baten leverancier		2	1	3	2	1	2	1
Baten ontvanger	1	1	1	2	1	3	2	
Andere			1		1	1	1	6
	11	11	11	11	11	11	10	10

Wanneer er een opsporingsorganisatie is betrokken en de gegevens dus een strafrechtelijke lading krijgen verandert er niettemin weinig in de beoordeling door de leverancier van de twee meest gewaardeerde belangen. Doelbinding eindigt op 9 en geheimhouding op 6 van de 11, kennelijk spelen deze noties in iets mindere mate als er aan opsporingsorganisaties wordt geleverd. Als derde eindigt de privacy van het subject met 5 stemmen.

Ten aanzien van de kwaliteit van de eigen, geleverde gegevens verschuift de beoordeling iets als deze aan een opsporingsorganisatie moet worden geleverd zoals uit onderstaand staatje blijkt. De gestelde vraag was:

Is de geleverde informatie:

Tijdig	**49**				
Compleet		**44**			
Betrouwbaar			**39**		
Actueel				**44**	
Passend					**39**
Maximaal	50	50	50	50	50
Gemiddeld	4,9	4,4	3,9	4,4	3,9

De scores voor kwaliteit van de eigen levering waren over het hoger dan bij levering aan een andere uitvoeringsorganisatie, waarbij opvalt dat tijdigheid extreem hoog scoort.

Cluster 4

Bij het laatste cluster moesten de respondenten vanuit het perspectief van de ontvanger de rangorde aanbrengen in de belangen die spelen bij gegevensuitwisseling waarbij een opsporingsorganisatie is betrokken.

	Aangevulde belangen:		- Juistheid van de gegevens - Het risico van het niet of niet goed ontvangen van de gegevens					
Perspectief: Ontvanger van opsporingsgegevens	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Doelbinding	5	5	2					
Privacy subject	1	1	1	4	2	2	1	
Privacy derde			2	3	1	2	1	2
Geheimhouding	1	1	5	2	2		1	
Kosten verstrekken				2	3	2	3	1
Baten leverancier			2		1	2	4	1
Baten ontvanger	5	4			1	1		
Andere		1		1	1	2		6
	12	12	12	12	11	11	10	10

Doelbinding wordt ook door de ontvanger van opsporingsgegevens zeer belangrijk gevonden, 12 van de 12 deelnemers plaatsen dit belang in de top 3. Daarna volgen de eigen baten van de ontvanger met 9 stemmen. Geheimhouding komt op 7 stemmen. Dit ging ten koste van de privacy van het subject, die bij de ontvangers in de bestuursrechtelijke sfeer hoger in het vaandel staat. Ook hier werd weer van de gelegenheid om een nog niet genoemd belang in te brengen werd spaarzaam gebruik gemaakt door de juistheid van de gegevens, en het risico van het niet ontvangen van de gegevens te vermelden.

Ten aanzien van de kwaliteit van de van de opsporingsorganisatie ontvangen gegevens was men positief zoals uit onderstaand staatje blijkt. De gestelde vraag was:

Is de geleverde informatie:

Tijdig	**57**				
Compleet		**52**			
Betrouwbaar			**47**		
Actueel				**52**	
Passend					**47**
Maximaal	60	60	60	60	60
Gemiddeld	4,8	4,3	3,9	4,3	3,9

De gegevens uit de opsporingsorganisatie worden kwalitatief hoog ingeschat, met name de tijdigheid. Betrouwbaarheid en passendheid scoren vrijwel hetzelfde als bij de ontvangst van een andere uitvoeringsorganisatie.

1912170 01165

Opsporingsorganisaties

Van de tweede doelgroep, de opsporingsorganisaties, werden in totaal 9 formulieren ontvangen. Deze formulieren kwamen met name van de Politie, het Openbaar Ministerie en de Belastingdienst (FIOD), de partners in de casus 2 en 3. De belangrijkste resultaten zijn hierna beschreven.

Cluster 1

Bij dit cluster moesten de respondenten uit een opsporingsorganisatie vanuit het leveranciers perspectief de rangorde aanbrengen in de belangen die spelen bij het leveren van gegevens.

	Aangevulde belangen:			- Overheidsbreed effectief optreden - Opsporing			
Perspectief Leverancier	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Doelbinding	2	4		1		1	
Privacy subject	2		1	1	2	1	1
Privacy derde		2	1		3	1	1
Geheimhouding	2		2	2		1	1
Kosten verstrekken			1	2			4
Eigen baten wed.	1		1	1	2	2	1
Baten ontvanger		2	2	1	1	2	
Andere	1						
	8	8	8	8	8	8	8

Wanneer er een opsporingsorganisatie is als leverancier van gegevens optreed gaat het om opsporingsgegevens die aan toezichthouders of andere opsporingsinstanties worden geleverd. Wat opvalt is dat de scores in de top drie flink lager zijn dan bij de uitvoeringsorganisaties. Ook hier zijn de twee meest gewaardeerde belangen doelbinding eindigt op 6 en geheimhouding en privacy van het subject beide op 5, bijna de helft van het aantal stemmen dat dezelfde belangen kregen bij de bestuursrechtelijke uitvoerders/toezichthouders. Kosten scoren ook hier laag als belang.

Ten aanzien van de kwaliteit van de eigen, geleverde gegevens verschuift de beoordeling iets als deze aan een opsporingsorganisatie moet worden geleverd zoals uit onderstaand staatje blijkt. De gestelde vraag was:

Is de geleverde informatie:

Tijdig	**31**				
Compleet		**36**			
Betrouwbaar			**35**		
Actueel				**37**	
Passend					**31**
Maximaal	40	45	40	45	40
Gemiddeld	3,9	4,0	4,4	4,1	3,9

De gegevens uit de opsporingsorganisatie worden door hun medewerkers kwalitatief hoog ingeschat op compleetheid en actualiteit. De tijdigheid wordt kennelijk als iets minder goed ervaren. Betrouwbaarheid en passendheid scoren vrijwel hetzelfde als bij de levering door een uitvoeringsorganisatie een de opsporing.

1912170 01165

Cluster 2

Bij dit cluster moesten de respondenten uit een opsporingsorganisatie vanuit het ontvangers perspectief de rangorde aanbrengen in de belangen die spelen bij het ontvangen van gegevens.

	Aangevulde belangen:			- Gemeenschappelijk overheidsbelang, organisatie-overstijgend - Opsporing				
Persepctief Ontvanger	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Doelbinding	1	4	2		1		1	
Privacy subject	2	1		4		1	1	
Privacy derde			2	1	3	1	2	
Geheimhouding		3	2	2	1	1		
Kosten verstrekken				1	3		4	1
Baten leverancier		1	1	1		6		
Baten ontvanger	6		2		1			
Andere							1	6
	9	9	9	9	9	9	9	7

Wanneer er een opsporingsorganisatie is als ontvanger van gegevens optreed kan het zowel gaan om opsporingsgegevens als om toezichtgegevens van niet-opsporingsdiensten. Hier blijken de eigen baten bij de gegevens het hoogst te scoren bij de eerste 3, namelijk 8. Op de tweede en derde plaats eindigen doelbinding en geheimhouding met resp. 7 en 5 stemmen. Niet een wezenlijk andere score dan bij de bestuursrechtelijke uitvoerders/toezichthouders, hoewel de 'verankerende beginselen ' in absolute zin lager scoren.

Ook de kwaliteit van de ontvangen gegevens door een opsporingsorganisatie wordt goed beoordeeld zoals uit onderstaand staatje blijkt. De gestelde vraag was:

Is de geleverde informatie:

Tijdig	**36**				
Compleet		**36**			
Betrouwbaar			**39**		
Actueel				**31**	
Passend					**34**
Maximaal	45	45	40	40	40
Gemiddeld	4,0	4,0	4,9	3,9	4,3

Wat opvalt is de hoge score van betrouwbaarheid van de gegevens. Deze hoge score zou verband kunnen houden met de herkomst van uitvoeringsinstantie die doorgaans over betrekkelijk harde informatie beschikken.

Vertegenwoordigers

Van de derde doelgroep, de vertegenwoordigers, werden in totaal 10 formulieren ontvangen. Deze formulieren kwamen met name van advocaten, accountants en belastingadviseurs waar de enquête was uitgezet. Ook werd een formulier ingevuld door een respondent van het College Bescherming Persoonsgegevens. De belangrijkste resultaten zijn hierna beschreven. De vertegenwoordigers kregen de vragen te beantwoorden vanuit twee perspectieven: die van de vertegenwoordigde en die van henzelf als vertegenwoordiger. Verder werd een onderscheid gemaakt tussen de gegevensuitwisseling in de bestuursrechtelijke sfeer en in de strafrechtelijke sfeer.

Cluster 1

Bij dit cluster moesten de respondenten vanuit het perspectief van de vertegenwoordigde een rangorde aanbrengen in de belangen die spelen bij het leveren van gegevens in de bestuursrechtelijke sfeer.

	Aangevulde belangen:				Transparantie			
Perspectief Vertegenwoordigde	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Doelbinding	2	1	3	2		1	1	
Privacy subject	5		2	2				
Privacy derde		2	1	2	2	2	1	1
Geheimhouding	1	7	1				1	
Kosten verstrekken			1	2		3	2	2
Baten subject			1	2	6	1		
Baten vertegenwoordiger	1				2	2	5	
Andere	1		1			1		6
	10	10	10	10	10	10	10	9

Het wekt geen verbazing dat de privacy van de vertegenwoordigde en de geheimhouding hier het hoogste scoren met respectievelijk 9 en 7 uit 10 bij de top 3. Ook de doelbinding wordt ook door de 'vertegenwoordigde' zeer belangrijk gevonden, 6 van de 10 deelnemers plaatsen dit belang in de top 3. De baten voor de cliënt, vanuit wiens perspectief werd gekeken, scoren opmerkelijk laag. Ook hier werd weer van de gelegenheid om een nog niet genoemd belang in te brengen werd spaarzaam gebruik gemaakt. Transparantie wordt als ontbrekend belang gesignaleerd.

Cluster 2

Bij dit cluster moesten de respondenten vanuit hun eigen perspectief van vertegenwoordiger een rangorde aanbrengen in de belangen die spelen bij het leveren van gegevens in de bestuursrechtelijke sfeer.

	Aangevulde belangen: Transparantie, risico van aansprakelijkheidstelling							
Perspectief Vertegenwoordiger	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Doelbinding	3	1	1	2	1		2	
Privacy subject	3	2	2	1	1			1
Privacy derde		1	1	1	1	5	1	
Geheimhouding	2	5	1		1		1	
Kosten verstrekken		1	2	1	1		4	1
Baten subject			1	3	3	3		
Baten vertegenwoordiger	1		1	2	2	2	2	
Andere	1		1					6
	10	10	10	10	10	10	10	8

Geheimhouding en privacy van de cliënt staan hoog genoteerd vanuit het perspectief van de vertegenwoordiger met respectievelijk 8 en 7 uit 10. Als derde de doelbinding met 5 stemmen, dezelfde volgorde als vanuit het perspectief van de vertegenwoordigde.

1912170 01165

Cluster 3

Bij dit cluster moesten de respondenten vanuit het perspectief van de vertegenwoordigde een rangorde aanbrengen in de belangen die spelen bij het leveren van gegevens in de strafrechtelijke sfeer.

	Aangevulde belangen: Opsporingssfeer							
Perspectief Vertegenwoordigde	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Doelbinding	2	1	2		2	1	1	
Privacy subject	4	2	2			1		
Privacy derde		1	1	4	3			
Geheimhouding	1	5	1	1				1
Kosten verstrekken			1	1	2	2	3	
Baten subject			2	3	2	4		
Baten ontvangende organisatie						1	5	1
Andere	2							6
	9	9	9	9	9	9	9	8

In de strafrechtelijke sfeer wisselen geheimhouding en privacy van de cliënt van plaats, met respectievelijk 8 en 7 uit 9. Als derde de doelbinding met 5 stemmen. Ook hier scoren de baten voor de cliënt niet erg hoog. Andere belangen scoort twee keer op 1. Het betreft het al eerder genoemde belang van transparantie en helaas een niet nader in tekst aangevuld belang.

Cluster 4

Bij dit cluster moesten de respondenten vanuit hun eigen perspectief van vertegenwoordiger een rangorde aanbrengen in de belangen die spelen bij het leveren van gegevens in de strafrechtelijke sfeer.

	Aangevulde belangen:			- Opsporingssfeer - Transparantie - Risico van aansprakelijkheidstelling				
Perspectief Vertegenwoordiger	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Doelbinding	3	1	1	1	1		3	
Privacy subject	2	3	3		2			
Privacy derde		2	1	2	2	3		
Geheimhouding	2	3	2	1			1	1
Kosten verstrekken			3	2		1	4	
Baten ontvangende org.		1		1	2	3	2	1
Baten vertegenwoordiger	1			3	3	3		
Andere	2							7
	10	10	10	10	10	10	10	9

Geheimhouding en privacy van de cliënt staan hoog genoteerd vanuit het perspectief van de vertegenwoordiger met respectievelijk 8 en 7 uit 10. Als derde de doelbinding met 5 stemmen. Deze score verschilt nauwelijks van de score buiten de opsporingssfeer. Ook hier bij twee respondenten een aanvullend belang op 1, het al eerder genoemde belang van transparantie en helaas een niet nader in tekst aangevuld belang.

1912170 01165

7.2.2. Enquêtevragen

MCA Enquête 1

Uitvoeringsorganisatie

Welkom bij de enquête naar de diverse belangen die een rol spelen in het kader van de uitwisseling van toezichtgegevens tussen uitvoeringsorganisaties. Er worden twee categorieën van uitwisseling van toezichtgegevens onderscheiden: in de bestuursrechtelijke sfeer, en in de opsporingssfeer. In de bestuursrechtelijke sfeer gaat het om uitwisseling met bijvoorbeeld:

- Belastingdienst;
- UWV;
- SVB;
- Milieu-inspectie;
- Gemeenten.

In de opsporingssfeer gaat het om uitwisseling met bijvoorbeeld:

- OM;
- Politie;
- SIOD;
- FIOD;
- BOA's.

In deze enquête wordt door middel van het aanbrengen van een rangorde tussen een aantal belangen de waardering van die belangen gepeild. Daarbij kunt u zowel in de rol van leverancier als in de rol van ontvanger van toezichtgegevens deelnemen. Als u kiest voor een van beide, dan kunt u de overige vragen onbeantwoord laten.

Naast vragen over de belangen worden ook vragen gesteld over de kwaliteit van de geleverde gegevens in de vorm van score-vragen.

Voor vragen of problemen met het invullen van de enquête kunt u contact opnemen met Lentine Schouten, l.m.schouten@uva.nl of Wouter van Haaften, vanhaaften@uva.nl, 06 1072 3500.

Er zijn 12 vragen in deze enquête.

Overheidsorganisatie

1 [1.1]

Welke rangorde zou u als **leverancier** van toezichtgegevens toekennen aan de onderstaande belangen? Mocht u kiezen voor een ander belang dan vermeld, dan kunt u dit belang apart weergeven.

Klik de opties uit de lijst aan in de gewenste volgorde van 1 naar 8.

Geef een nummer voor elke optie volgens uw voorkeur van 1 tot 8

- Doelbinding van de uit te wisselen toezichtgegevens
- De privacy van het subject
- De privacy van een eventuele derde
- De geheimhouding van de toezichtgegevens
- Kosten c.q. moeite van het verstrekken van de gegevens
- Baten voor de eigen organisatie (wederkerigheid)
- Baten voor de ontvangende organisatie
- Andere belangen dan zijn vermeld

Toelichting

Doelbinding van de uit te wisselen toezichtgegevens:
De gegevens zijn door het subject zelf met een bepaald doel afgegeven of buiten hem om verzameld.

De privacy van het subject:
Het leveren van toezichtgegevens leidt mogelijk tot aantasting van de privacy van het subject.

De privacy van een eventuele derde:
Het leveren van gegevens leidt mogelijk tot aantasting van de privacy van een derde.

De geheimhouding van de toezichtgegevens:
Er is een organisatiebelang gediend met geheimhouding van de gegevens.

Kosten c.q. moeite van het verstrekken van de gegevens:
De kosten in tijd, geld, personeel en technische en/of organisatorische aanpassingen die moeten worden gemaakt om de gevraagde gegevens te kunnen leveren.

Baten voor de eigen organisatie (wederkerigheid):
Het verlangen van een tegenprestatie in de sfeer van gegevensuitwisseling.

Baten voor de ontvangende organisatie:
Het belang van de ontvangende organisatie bij de levering aan uw organisatie.

Andere belangen dan zijn vermeld:
Hieronder kunt u eventuele belangen invullen, anders dan de hierboven genoemde.

2 [1.1b]

Mist u nog een belang? Dan kunt u dat hier invullen.

Vul uw antwoord hier in:

3 [1.2]

Bij het uitwisselen van toezichtgegevens komt het voor dat dataverzamelingen moeten worden uitgewisseld. De volgende vragen hebben betrekking op de kwaliteit van die uitwisseling vanuit het perspectief van de leverancier van deze data. Welke waardering zou u toekennen aan de hierna genoemde criteria? (geef een score tussen 1-5, 1 = laag 5 = hoog)

Kies het toepasselijk antwoord voor elk onderdeel:

	1	2	3	4	5
De tijdigheid van de gegevens. De gegevens kunnen op redelijke termijn worden verstrekt gelet op het gebruiksdoel en het gewenste gebruiksmoment van de gegevens.	○	○	○	○	○
De compleetheid van de gegevens. De geleverde gegevens zijn voldoende compleet om het gebruiksdoel te kunnen dienen.	○	○	○	○	○
De betrouwbaarheid van de gegevens. De geleverde gegevens zijn voldoende betrouwbaar voor directe aanwending voor het gebruiksdoel.	○	○	○	○	○
De actualiteit van de gegevens. De geleverde gegevens zijn voldoende actueel voor aanwending voor het gebruiksdoel.	○	○	○	○	○
Sluit de gegevens vraag voldoende aan bij uw gegevensverzameling? Zijn de gevraagde gegevens direct leverbaar of vergen zij nog nadere bewerking ten behoeve van de levering?	○	○	○	○	○

4 [1.3]

Als u **ontvanger** bent van gegevens, welke rangorde zou u dan toekennen aan de onderstaande belangen? Mocht u kiezen voor een ander belang dan vermeld, dan kunt u dit belang apart weergeven.

Klik de opties uit de lijst aan in de gewenste volgorde van 1 naar 8.

Geef een nummer voor elke optie volgens uw voorkeur van 1 tot 8

- Doelbinding van de uit te wisselen toezichtgegevens
- De privacy van het subject
- De privacy van een eventuele derde
- De geheimhouding van de toezichtgegevens
- De kosten c.q. moeite van het verstrekken van de gegevens
- De baten voor de ontvangende organisatie
- De baten voor de leverende organisatie
- Andere belangen dan zijn vermeld

Doelbinding van de uit te wisselen toezichtgegevens:
De gegevens zijn door het subject zelf met een bepaald doel afgegeven of buiten hem om verzameld.

De privacy van het subject:
Het leveren van toezichtgegevens leidt mogelijk tot aantasting van de privacy van het subject.

De privacy van een eventuele derde
Het leveren van gegevens leidt mogelijk tot aantasting van de privacy van een derde.

De geheimhouding van de toezichtgegevens
Er is een organisatiebelang gediend met geheimhouding van de gegevens.

Kosten c.q. moeite van het verstrekken van de gegevens
De kosten in tijd, geld, personeel en technische en/of organisatorische aanpassingen die moeten worden gemaakt om de gevraagde gegevens te kunnen uitwisselen.

Baten voor de leverende organisatie (wederkerigheid)
Het verlangen van een tegenprestatie in de sfeer van gegevensuitwisseling.

Baten voor de ontvangende organisatie
Het belang van de ontvangende organisatie bij de levering aan uw organisatie.

Andere belangen dan hiervoor vermeld
Hieronder kunt u eventueel een ander belang invullen dan de hierboven genoemde.

5 [1.3b]

Mist u nog een belang? Dan kunt u dat hier invullen.

Vul uw antwoord hier in:

6 [1.4]

Bij het uitwisselen van toezichtgegevens komt het voor dat dataverzamelingen moeten worden uitgewisseld. De volgende vragen hebben betrekking op de kwaliteit van die uitwisseling vanuit het perspectief van de ontvanger van deze data. Welke waardering zou u toekennen aan de hierna genoemde criteria? (geef een score tussen 1-5, 1 = laag 5 = hoog)

Kies het toepasselijk antwoord voor elk onderdeel:

	1	2	3	4	5
De tijdigheid van de gegevens. De gegevens kunnen op redelijke termijn worden verkregen gelet op het gebruiksdoel en het gewenste gebruiksmoment van de gegevens.	○	○	○	○	○
De compleetheid van de gegevens. De verkregen gegevens zijn voldoende compleet om het gebruiksdoel te kunnen dienen.	○	○	○	○	○
De betrouwbaarheid van de gegevens. De verkregen gegevens zijn voldoende betrouwbaar voor directe aanwending voor het gebruiksdoel.	○	○	○	○	○
De actualiteit van de gegevens. De verkregen gegevens zijn voldoende actueel voor aanwending voor het gebruiksdoel.	○	○	○	○	○
Sluit de gegevens vraag voldoende aan bij uw gegevensverzameling? Zijn de verkregen gegevens direct inzetbaar of vergen zij nog nadere bewerking ten behoeve van het gebruiksdoel?	○	○	○	○	○

7 [1.5]

Opsporingssfeer

Bij de volgende vragen is een van beide overheidsinstanties een opsporingsorganisatie.

Welke rangorde zou u als **leverancier** van toezichtgegevens **aan een opsporingsorganisatie** toekennen aan de onderstaande belangen? Mocht u kiezen voor een ander belang dan vermeld, dan kunt u dit belang apart weergeven.

Klik de opties uit de lijst aan in de gewenste volgorde van 1 naar 8.

Geef een nummer voor elke optie volgens uw voorkeur van 1 tot 8

- Doelbinding van de uit te wisselen toezichtgegevens
- De privacy van het subject
- De privacy van een eventuele derde
- De geheimhouding van de toezichtgegevens
- De kosten c.q. moeite van het verstrekken van de gegevens
- De baten voor de leverende organisatie (wederkerigheid)
- De baten voor de ontvangende organisatie
- Andere belangen dan zijn vermeld

Doelbinding van de uit te wisselen toezichtgegevens
De gegevens zijn door het subject zelf met een bepaald doel afgegeven of buiten hem om verzameld.

De privacy van het subject
Het leveren van toezichtgegevens leidt mogelijk tot aantasting van de privacy van het subject.

De privacy van een eventuele derde
Het leveren van gegevens leidt mogelijk tot aantasting van de privacy van een derde.

De geheimhouding van de toezichtgegevens
Er is een organisatiebelang gediend met geheimhouding van de gegevens.

Kosten c.q. moeite van het verstrekken van de gegevens
De kosten in tijd, geld, personeel en technische en/of organisatorische aanpassingen die moeten worden gemaakt om de gevraagde gegevens te kunnen leveren.

Baten voor de eigen organisatie (wederkerigheid)
Het verlangen van een tegenprestatie in de sfeer van gegevensuitwisseling.

Baten voor de ontvangende organisatie
Het belang van de ontvangende organisatie bij de levering aan uw organisatie.

Andere belangen dan zijn vermeld
Hieronder kunt u eventueel een ander belang invullen dan de hierboven genoemde.

8 [1.5b]

Mist u nog een belang? Dan kunt u dat hier invullen.

Vul uw antwoord hier in:

9 [1.6]

Bij het uitwisselen van toezichtgegevens komt het voor dat dataverzamelingen moeten worden uitgewisseld. De volgende vragen hebben betrekking op de kwaliteit van die uitwisseling vanuit het perspectief van de leverancier van deze data aan de opsporingsinstantie. Welke waardering zou u toekennen aan de hierna genoemde criteria? (geef een score tussen 1-5, 1 = laag 5 = hoog)

Kies het toepasselijk antwoord voor elk onderdeel:

	1	2	3	4	5
De tijdigheid van de gegevens. De gegevens kunnen op redelijke termijn worden verkregen gelet op het gebruiksdoel en het gewenste gebruiksmoment van de gegevens.	○	○	○	○	○
De compleetheid van de gegevens. De verkregen gegevens zijn voldoende compleet om het gebruiksdoel te kunnen dienen.	○	○	○	○	○
De betrouwbaarheid van de gegevens. De verkregen gegevens zijn voldoende betrouwbaar voor directe aanwending voor het gebruiksdoel.	○	○	○	○	○
De actualiteit van de gegevens. De verkregen gegevens zijn voldoende actueel voor aanwending voor het gebruiksdoel.	○	○	○	○	○
Sluit de gegevens vraag voldoende aan bij uw gegevensverzameling? Zijn de verkregen gegevens direct inzetbaar of vergen zij nog nadere bewerking ten behoeve van het gebruiksdoel?	○	○	○	○	○

10 [1.7]

Als u **ontvanger** bent van toezichtgegevens **van een opsporingsorganisatie**, welke rangorde zou u dan toekennen aan de onderstaande belangen? Mocht u kiezen voor een ander belang dan vermeld, dan kunt u dit belang apart weergeven.

Klik de opties uit de lijst aan in de gewenste volgorde van 1 naar 8.

Geef een nummer voor elke optie volgens uw voorkeur van 1 tot 8

- Doelbinding van de uit te wisselen toezichtgegevens
- De privacy van het subject
- De privacy van een eventuele derde
- De geheimhouding van de toezichtgegevens
- De kosten c.q. moeite van het verstrekken van de gegevens
- De baten voor de eigen organisatie
- De baten voor de leverende organisatie
- Andere belangen dan zijn vermeld

Doelbinding van de uit te wisselen toezichtgegevens
De gegevens zijn door het subject zelf met een bepaald doel afgegeven of buiten hem om verzameld.

De privacy van het subject
Het leveren van toezichtgegevens leidt mogelijk tot aantasting van de privacy van het subject.

De privacy van een eventuele derde
Het leveren van gegevens leidt mogelijk tot aantasting van de privacy van een derde.

De geheimhouding van de toezichtgegevens
Er is een organisatiebelang gediend met geheimhouding van de gegevens.

De kosten c.q. moeite van het verstrekken van de gegevens
De kosten in tijd, geld, personeel en technische en/of organisatorische aanpassingen die moeten worden gemaakt om de gevraagde gegevens te kunnen leveren.

De baten voor de leverende organisatie
Het verlangen van een tegenprestatie in de sfeer van gegevensuitwisseling.

De baten voor uw eigen organisatie
Het belang van de ontvangende organisatie bij de levering aan uw organisatie.

Andere belangen dan zijn vermeld
Hier kunt u eventueel andere belangen invullen dan de hierboven genoemde.

11 [1.7b]

Mist u nog een belang? Dan kunt u dat hier invullen.

Vul uw antwoord hier in:

12 [1.8]

Bij het uitwisselen van toezichtgegevens komt het voor dat dataverzamelingen moeten worden uitgewisseld. De volgende vragen hebben betrekking op de kwaliteit van die uitwisseling vanuit het perspectief van de ontvanger van deze data van een opsporingsinstantie. Welke waardering zou u toekennen aan de hierna genoemde criteria? (geef een score tussen 1-5, 1 = laag 5 = hoog)

Kies het toepasselijk antwoord voor elk onderdeel:

	1	2	3	4	5
De tijdigheid van de gegevens. De gegevens kunnen op redelijke termijn worden verkregen gelet op het gebruiksdoel en het gewenste gebruiksmoment van de gegevens.	○	○	○	○	○
De compleetheid van de gegevens. De verkregen gegevens zijn voldoende compleet om het gebruiksdoel te kunnen dienen.	○	○	○	○	○
De betrouwbaarheid van de gegevens. De verkregen gegevens zijn voldoende betrouwbaar voor directe aanwending voor het gebruiksdoel.	○	○	○	○	○
De actualiteit van de gegevens. De verkregen gegevens zijn voldoende actueel voor aanwending voor het gebruiksdoel.	○	○	○	○	○
Sluit de gegevens vraag voldoende aan bij uw gegevens-verzameling? Zijn de verkregen gegevens direct inzetbaar of vergen zij nog nadere bewerking ten behoeve van het gebruiksdoel?	○	○	○	○	○

Dank voor uw bereidheid aan deze enquête te willen meewerken. Wij zullen uw gegevens vertrouwelijk behandelen.
01.01.1970 – 01:00

Verstuur uw enquête
Bedankt voor uw deelname aan deze enquête.

MCA Enquête 2

Opsporingsorganisatie

Welkom bij de enquête naar de diverse belangen die een rol spelen in het kader van de uitwisseling van toezichtgegevens tussen uitvoeringsorganisaties. Er worden twee categorieën van uitwisseling van toezichtgegevens onderscheiden: in de bestuursrechtelijke sfeer, en in de opsporingssfeer. In de bestuursrechtelijke sfeer gaat het om uitwisseling met bijvoorbeeld:

- Belastingdienst;
- UWV;
- SVB;
- Milieu-inspectie;
- Gemeenten.

In de opsporingssfeer gaat het om uitwisseling met bijvoorbeeld:

- OM;
- Politie;
- SIOD;
- FIOD;
- BOA's.

In deze enquête wordt door middel van het aanbrengen van een rangorde tussen een aantal belangen de waardering van die belangen gepeild. Daarbij kunt u zowel in de rol van leverancier als in de rol van ontvanger van toezichtgegevens deelnemen. Als u kiest voor een van beide, dan kunt u de overige vragen onbeantwoord laten.

Naast vragen over de belangen worden ook vragen gesteld over de kwaliteit van de geleverde gegevens in de vorm van score-vragen.

Voor vragen of problemen met het invullen van de enquête kunt u contact opnemen met Lentine Schouten, l.m.schouten@uva.nl of Wouter van Haaften, vanhaaften@uva.nl, 06-10723500.

Er zijn 6 vragen in deze enquête:

1912170 01165

Opsporingsorganisatie

Bij de volgende vragen is een van beide overheidsinstanties een **opsporingsorganisatie.** U kunt de vragen beantwoorden vanuit het perspectief van leverancier, het perspectief van ontvanger of vanuit beide perspectieven. Als u voor een van beide kiest, dan laat u de andere vragen open.

1 [2.1]

Als u **als opsporingsorganisatie leverancier** bent van gegevens aan een andere overheids-organisatie, welke rangorde zou u dan toekennen aan de onderstaande belangen? Mocht u kiezen voor een ander belang dan vermeld, dan kunt u dit belang apart weergeven.

Klik de opties uit de lijst aan in de gewenste volgorde van 1 naar 8.

Geef een nummer voor elke optie volgens uw voorkeur van 1 tot 8

- Doelbinding van de uit te wisselen toezichtgegevens
- De privacy van het subject
- De privacy van een eventuele derde
- De geheimhouding van de toezichtgegevens
- Kosten c.q. moeite van het verstrekken van de gegevens
- Baten voor de eigen organisatie (wederkerigheid)
- Baten voor de ontvangende organisatie
- Andere belangen dan zijn vermeld

Doelbinding van de uit te wisselen toezichtgegevens
De gegevens zijn door het subject zelf met een bepaald doel afgegeven of buiten hem om verzameld.

De privacy van het subject
Het leveren van toezichtgegevens leidt mogelijk tot aantasting van de privacy van het subject.

De privacy van een eventuele derde
Het leveren van gegevens leidt mogelijk tot aantasting van de privacy van een derde.

De geheimhouding van de toezichtgegevens
Er is een organisatiebelang gediend met geheimhouding van de gegevens.

De kosten c.q. moeite van het verstrekken van de gegevens
De kosten in tijd, geld, personeel en technische en/of organisatorische aanpassingen die moeten worden gemaakt om de gevraagde gegevens te kunnen leveren.

De baten voor de eigen organisatie (wederkerigheid)
Het verlangen van een tegenprestatie in de sfeer van gegevensuitwisseling.

1912170 01165

De baten voor de ontvangende organisatie
Het belang van de ontvangende organisatie bij de levering aan uw organisatie.

Andere belangen dan zijn vermeld
Hier kunt u eventuele andere belangen invullen dan de hierboven genoemde.

2 [2.1b]

Mist u nog een belang? Dan kunt u dat hier invullen.

Vul uw antwoord hier in:

3 [2.2]

Bij het uitwisselen van toezichtgegevens komt het voor dat dataverzamelingen moeten worden uitgewisseld. De volgende vragen hebben betrekking op de kwaliteit van die levering van data vanuit het perspectief van de leverende opsporingsinstantie. Welke waardering zou u toekennen aan de hierna genoemde criteria? (geef een score tussen 1-5, 1 = laag 5 = hoog)

Kies het toepasselijk antwoord voor elk onderdeel:

	1	2	3	4	5
De tijdigheid van de gegevens. De gegevens kunnen op redelijke termijn worden verkregen gelet op het gebruiksdoel en het gewenste gebruiksmoment van de gegevens.	○	○	○	○	○
De compleetheid van de gegevens. De verkregen gegevens zijn voldoende compleet om het gebruiksdoel te kunnen dienen.	○	○	○	○	○
De betrouwbaarheid van de gegevens. De verkregen gegevens zijn voldoende betrouwbaar voor directe aanwending voor het gebruiksdoel.	○	○	○	○	○
De actualiteit van de gegevens. De verkregen gegevens zijn voldoende actueel voor aanwending voor het gebruiksdoel.	○	○	○	○	○
Sluit de gegevens vraag voldoende aan bij uw gegevensverzameling? Zijn de verkregen gegevens direct inzetbaar of vergen zij nog nadere bewerking ten behoeve van het gebruiksdoel?	○	○	○	○	○

4 [2.3]

Als u als opsporingsorganisatie ontvanger bent van toezichtgegevens van een andere overheids-organisatie, welke rangorde zou u dan toekennen aan de onderstaande belangen? Mocht u kiezen voor een ander belang dan vermeld, dan kunt u dit belang apart weergeven.

Klik de opties uit de lijst aan in de gewenste volgorde van 1 naar 8.

Geef een nummer voor elke optie volgens uw voorkeur van 1 tot 8

- Doelbinding van de uit te wisselen toezichtgegevens
- De privacy van het subject
- De privacy van een eventuele derde
- De geheimhouding van de toezichtgegevens
- De kosten c.q. moeite van het verstrekken van de gegevens
- De baten voor de eigen organisatie
- De baten voor de leverende organisatie
- Andere belangen dan zijn vermeld

Doelbinding van uit te wisselen toezichtgegevens
De gegevens zijn door het subject zelf met een bepaald doel afgegeven of buiten hem om verzameld.

De privacy van het subject
Het leveren van toezichtgegevens leidt mogelijk tot aantasting van de privacy van het subject.

De privacy van een eventuele derde
Het leveren van gegevens leidt mogelijk tot aantasting van de privacy van een derde.

De geheimhouding van de toezichtgegevens
Er is een organisatiebelang gediend met geheimhouding van de gegevens.

De kosten c.q. moeite van het verstrekken van de gegevens
De kosten in tijd, geld, personeel en technische en/of organisatorische aanpassingen die moeten worden gemaakt om de gevraagde gegevens te kunnen leveren.

De baten voor de leverende organisatie
Het verlangen van een tegenprestatie in de sfeer van gegevensuitwisseling.

De baten voor uw eigen organisatie
Het belang van de ontvangende organisatie bij de levering aan uw organisatie.

Andere belangen dan zijn vermeld
Hieronder kunt u eventuele andere belangen invullen dan de hierboven genoemde.

5 [2.3b]

Mist u nog een belang? Dan kunt u dat hier invullen.
Vul uw antwoord hier in:

6 [2.4]

Bij het uitwisselen van toezichtgegevens komt het voor dat dataverzamelingen moeten worden uitgewisseld. De volgende vragen hebben betrekking op de kwaliteit van die levering van data vanuit het perspectief van de ontvangende opsporingsinstantie. Welke waardering zou u toekennen aan de hierna genoemde criteria? (geef een score tussen 1-5, 1 = laag 5 = hoog).

Kies het toepasselijk antwoord voor elk onderdeel:

	1	2	3	4	5
De tijdigheid van de gegevens. De gegevens kunnen op redelijke termijn worden verkregen gelet op het gebruiksdoel en het gewenste gebruiksmoment van de gegevens.	○	○	○	○	○
De compleetheid van de gegevens. De verkregen gegevens zijn voldoende compleet om het gebruiksdoel te kunnen dienen.	○	○	○	○	○
De betrouwbaarheid van de gegevens. De verkregen gegevens zijn voldoende betrouwbaar voor directe aanwending voor het gebruiksdoel.	○	○	○	○	○
De actualiteit van de gegevens. De verkregen gegevens zijn voldoende actueel voor aanwending voor het gebruiksdoel.	○	○	○	○	○
Sluit de gegevens vraag voldoende aan bij uw gegevensverzameling? Zijn de verkregen gegevens direct inzetbaar of vergen zij nog nadere bewerking ten behoeve van het gebruiksdoel?	○	○	○	○	○

Dank voor uw bereidheid aan deze enquête mee te willen werken. Wij zullen uw gegevens vertrouwelijk behandelen.
01.01.1970 – 01:00

Verstuur uw enquête
Bedankt voor uw deelname aan deze enquête

MCA Enquête 3

Vertegenwoordiger

Welkom bij de enquête naar de diverse belangen die een rol spelen in het kader van de uitwisseling van toezichtgegevens tussen uitvoeringsorganisaties. Er worden twee categorieën van uitwisseling van toezichtgegevens onderscheiden: in de bestuursrechtelijke sfeer, en in de opsporingssfeer. In de bestuursrechtelijke sfeer gaat het om uitwisseling met bijvoorbeeld:

- Belastingdienst;
- UWV;
- SVB;
- Milieu-inspectie;
- Gemeenten.

In de opsporingssfeer gaat het om uitwisseling met bijvoorbeeld:

- OM;
- Politie;
- SIOD;
- FIOD;
- BOA's.

In deze enquête wordt door middel van het aanbrengen van een rangorde tussen een aantal belangen de waardering van die belangen gepeild. Als vertegenwoordiger kunt u de vragen vanuit twee perspectieven beantwoorden, zowel vanuit het perspectief van de vertegenwoordiger, als vanuit het perspectief van de door u vertegenwoordigde.

Voor vragen of problemen met het invullen van de enquête kunt u contact opnemen met Lentine Schouten, l.m.schouten@uva.nl of Wouter van Haaften, vanhaaften@uva.nl, 06-10723500.

Er zijn 8 vragen in deze enquête:

Vertegenwoordiger

1 [3.1]

Als er gegevens over een door u vertegenwoordigd persoon worden uitgewisseld **tussen overheidsorganisaties**, welke rangorde zou u dan toekennen aan de onderstaande belangen vanuit het **perspectief van de vertegenwoordigde?** Mocht u kiezen voor een ander belang dan vermeld, dan kunt u dit belang apart weergeven.

Klik de opties uit de lijst aan in de gewenste volgorde van 1 naar 8.

Geef een nummer voor elke optie volgens uw voorkeur van 1 tot 8

- Doelbinding van de uit te wisselen toezichtgegevens
- De privacy van het subject
- De privacy van een eventuele derde
- De geheimhouding van de toezichtgegevens
- De kosten c.q. moeite van het verstrekken van de gegevens
- De baten voor het subject
- De baten voor de vertegenwoordiger
- Andere belangen dan zijn vermeld

Doelbinding van de uit te wisselen toezichtgegevens
De gegevens zijn door het subject zelf met een bepaald doel afgegeven of buiten hem om verzameld.

De privacy van het subject
Het leveren van toezichtgegevens leidt mogelijk tot aantasting van de privacy van het subject.

De privacy van een eventuele derde
Het leveren van gegevens leidt mogelijk tot aantasting van de privacy van een derde.

De geheimhouding van de toezichtgegevens
De gegevens worden uitsluitend binnen de uitwisselende organisaties gebruikt.

De kosten c.q. moeite van het verstrekken van de gegevens
De kosten in tijd, geld, personeel en technische en/of organisatorische aanpassingen die moeten worden gemaakt om de gevraagde gegevens te kunnen uitwisselen.

De baten voor het subject
Te denken valt aan stroomlijning van controles, minder administratieve lasten.

De baten voor de vertegenwoordiger
Te denken valt aan stroomlijning van controles, minder administratieve lasten.

Andere belangen dan zijn vermeld
Hieronder kunt u eventuele belangen invullen, anders dan de hierboven genoemde.

1912170 01165

2 [3.1b]

Mist u nog een belang? Dan kunt u dat hier invullen.

Vul uw antwoord hier in:

3 [3.2]

Als er gegevens over een door u vertegenwoordigd persoon worden uitgewisseld **tussen overheidsorganisaties**, welke rangorde zou u dan toekennen aan de onderstaande belangen vanuit **uw eigen belang al vertegenwoordiger?** Mocht u kiezen voor een ander belang dan vermeld, dan kunt u dit belang apart weergeven.

Klik de opties uit de lijst aan in de gewenste volgorde van 1 naar 8.

Geef een nummer voor elke optie volgens uw voorkeur van 1 tot 8

- Doelbinding van de uit te wisselen toezichtgegevens
- De privacy van het subject
- De privacy van een eventuele derde
- De geheimhouding van de toezichtgegevens
- De kosten c.q. moeite van het verstrekken van de gegevens
- De baten voor het subject
- De baten voor de vertegenwoordiger
- Andere belangen dan zijn vermeld

Doelbinding van de uit te wisselen toezichtgegevens
De gegevens zijn door het subject zelf met een bepaald doel afgegeven of buiten hem om verzameld.

De privacy van het subject
Het leveren van toezichtgegevens leidt mogelijk tot aantasting van de privacy van het subject.

De privacy van een eventuele derde
Het leveren van gegevens leidt mogelijk tot aantasting van de privacy van een derde.

De geheimhouding van de toezichtgegevens
De gegevens worden uitsluitend binnen de uitwisselende organisaties gebruikt.

De kosten c.q. moeite van het verstrekken van de gegevens
De kosten in tijd, geld, personeel en technische en/of organisatorische aanpassingen die moeten worden gemaakt om de gevraagde gegevens te kunnen uitwisselen.

De baten voor het subject
Te denken valt aan stroomlijning van controles, minder administratieve lasten.

De baten voor de vertegenwoordiger
Te denken valt aan stroomlijning controles, minder administratieve lasten.

Andere belangen dan zijn vermeld
Hieronder kunt u eventuele belangen invullen, anders dan de hierboven genoemde.

4 [3.2b]

Mist u nog een belang? Dan kunt u dat hier invullen.

Vul uw antwoord hier in:

5 [3.3]

Als er gegevens over een door u vertegenwoordigd persoon worden uitgewisseld tussen **een opsporingsorganisatie** en een andere overheidsorganisatie, welke rangorde zou u dan toekennen aan de onderstaande belangen vanuit het **perspectief van de vertegenwoordigde?** Mocht u kiezen voor een ander belang dan vermeld, dan kunt u dit belang apart weergeven.

Klik de opties uit de lijst aan in de gewenste volgorde van 1 naar 8.

Geef een nummer voor elke optie volgens uw voorkeur van 1 tot 8

- Doelbinding van de uit te wisselen toezichtgegevens
- De privacy van de vertegenwoordigde
- De privacy van een eventuele derde
- De geheimhouding van de toezichtgegevens
- De kosten c.q. moeite van het verstrekken van de gegevens
- De baten voor de vertegenwoordigde
- De baten voor de ontvangende organisatie
- Andere belangen dan zijn vermeld

Doelbinding van uit te wisselen toezichtgegevens
De gegevens zijn door het subject zelf met een bepaald doel afgegeven of buiten hem om verzameld.

De privacy van het subject
Het leveren van toezichtgegevens leidt mogelijk tot aantasting van de privacy van het subject.

De privacy van een eventuele derde
Het leveren van gegevens leidt mogelijk tot aantasting van de privacy van een derde.

De geheimhouding van de toezichtgegevens
Er is een organisatiebelang gediend met geheimhouding van de gegevens?

De kosten c.q. moeite van het verstrekken van de gegevens
De kosten in tijd, geld, personeel en technische en/of organisatorische aanpassingen die moeten worden gemaakt om de gevraagde gegevens te kunnen leveren.

De baten voor het subject
Te denken valt aan stroomlijning van controles, minder administratieve lasten.

De baten voor de vertegenwoordiger
Te denken valt aan stroomlijning van controles, minder administratieve lasten.

Andere belangen dan zijn vermeld
Hieronder kunt u eventuele belangen invullen, anders dan de hierboven genoemde.

6 [3.3b]

Mist u nog een belang? Dan kunt u dat hier invullen.

Vul uw antwoord hier in:

7 [3.4]

Als er gegevens over een door u vertegenwoordigd persoon worden uitgewisseld tussen **een opsporingsorganisatie** en een andere overheidsorganisatie, welke rangorde zou u dan toekennen aan de onderstaande belangen vanuit het **perspectief van uzelf als vertegenwoordiger?** Mocht u kiezen voor een ander belang dan vermeld, dan kunt u dit belang apart weergeven.

Klik de opties uit de lijst aan in de gewenste volgorde van 1 naar 8.

Geef een nummer voor elke optie volgens uw voorkeur van 1 tot 8

- Doelbinding van de uit te wisselen toezichtgegevens
- De privacy van het subject
- De privacy van een eventuele derde
- De geheimhouding van de toezichtgegevens
- De kosten c.q. moeite van het verstrekken van de gegevens
- De baten voor de eigen organisatie van de vertegenwoordiger
- De baten voor de ontvangende organisatie
- Andere belangen dan zijn vermeld

Doelbinding van de uit te wisselen toezichtgegevens
De gegevens zijn door het subject zelf met een bepaald doel afgegeven of buiten hem om verzameld.

De privacy van het subject
Het leveren van toezichtgegevens leidt mogelijk tot aantasting van de privacy van het subject.

De privacy van een eventuele derde
Het leveren van gegevens leidt mogelijk tot aantasting van de privacy van een derde.

De geheimhouding van de toezichtgegevens
Er is een organisatiebelang gediend met geheimhouding van de gegevens?

De kosten c.q. moeite van het verstrekken van de gegevens
De kosten in tijd, geld, personeel en technische en/of organisatorische aanpassingen die moeten worden gemaakt om de gevraagde gegevens te kunnen leveren.

De baten voor het subject
Te denken valt aan stroomlijning van controles, minder administratieve lasten.

De baten voor de vertegenwoordiger
Te denken valt aan stroomlijning van controles, minder administratieve lasten.

Andere belangen dan zijn vermeld
Hieronder kunt u eventuele belangen invullen, anders dan de hierboven genoemde.

8 [3.4b]

Mist u nog een belang? Dan kunt u dat hier invullen.

Vul uw antwoord hier in:

Dank voor uw bereidheid aan deze enquête te willen meewerken. Wij zullen uw gegevens vertrouwelijk behandelen.
01.01.1970 – 01:00

Verstuur uw enquête
Bedankt voor uw deelname aan deze enquête.

7.3 Lijst deelnemers Expertmeeting 29 februari 2012

Experts

Jan Been, extern adviseur gemeente Amsterdam

Jacob de Boer, Fort Advocaten

Caroline Coolen, OM, Functioneel Parket

Paul van Dijk, Belastingdienst

Astrid Franke, Gemeente Amsterdam

Hein Kloosterman, Kloosterman Statistical Audit Consulting

Heleen Koning, CBP

Jiska Pot, Juridische Zaken, Gemeente Amsterdam

Roy Wildemors, Dienst Justis

Begeleidingscommissie

Rob van den Hoven van Genderen, Director Center for Law and Internet (VU)

Onderzoeksteam

Adrienne de Moor-van Vugt, hoogleraar Bestuursrecht

Tom van Engers, hoogleraar Legal Knowledge Management

Taco Groenewegen, universitair docent Bestuursrecht

Wouter van Haaften, senior researcher Leibniz Center for Law

Arnout Klap, universitair hoofddocent Bestuursrecht

Lentine Schouten, student-assistent

Marleen Wessel, promovenda Financieel Toezicht (onderzoeksassistentie)

Djaënti Sewdihal (stagiair)

1912170 01165