WRR

WETENSCHAPPELIJKE RAAD VOOR HET REGERINGSBELEID

Peter Olsthoorn

Big Data voor Fraude-bestrijding

WORKING PAPER 21

Big Data voor Fraudebestrijding

De serie 'Working Papers' omvat studies die in het kader van de werkzaamheden van de WRR tot stand zijn gekomen. De verantwoordelijkheid voor de inhoud berust bij de auteurs. Een overzicht van alle webpublicaties is te vinden op www.wrr.nl.

Wetenschappelijke Raad voor het Regeringsbeleid
Buitenhof 34
Postbus 20004
2500 EA Den Haag
Telefoon 070-356 46 00
E-mail info@wrr.nl
Website www.wrr.nl

WRR

WETENSCHAPPELIJKE RAAD VOOR HET REGERINGSBELEID

Big Data voor Fraudebestrijding

Peter Olsthoorn

Alle *Rapporten aan de Regering* en publicaties in de reeksen *Verkenningen*, *Policy Briefs* en *Working Papers* zijn beschikbaar via www.wrr.nl.

Vormgeving binnenwerk: Textcetera, Den Haag
Omslagafbeelding: Textcetera, Den Haag

Working Paper nummer 21

ISBN 978-94-90186-30-2

WRR, Den Haag 2016

INHOUD

Ten geleide 9

1 Inleiding 11
1.1 Wetsovertreder of brave burger 11
1.2 Politieke wens en controle 12

2 Omvang van de fraude en beleid 19
Inleiding 19
2.1 De ruwe bedragen 20
2.2 Ministeriële commissie-Aanpak Fraude 23
2.3 Slim voorkomen, vlot herstellen 26
2.4 'Vernetwerking' als doel en middel 26

3 Zorg 29
Inleiding 29
3.1 Beleid en mislukkingen 29
3.2 Gemengde resultaten 33
3.3 Nadruk op data-analyse 39
3.4 Toekomst: spanning met medische privacy 48

4 Belastingdienst 57
Inleiding 57
4.1 Innovatie in data-analyse in de 'broedkamer' 57
4.2 Samenwerkingsverbanden met belastingdata 62
4.3 Privacyvraagstukken en privacykritiek 72
4.4 Beleid en toekomst 78

5 Inlichtingenbureau 87
Inleiding 87
5.1 Doel 87
5.2 Opzet van systemen 88
5.3 Uitvoering 91
5.4 Resultaten 93
5.5 Hinderpalen en vraagtekens 94
5.6 Toekomst 96

6 SyRI en LSI 99
Inleiding 99
6.1 Wettelijke basis 99
6.2 Uitvoering SyRI 102

6.3	Toepassing in de praktijk	105
6.4	Privacy	108
7	**Inspectie SZW**	111
	Inleiding	111
7.1	Beleid en werkwijze	111
7.2	Externe samenwerking	115
7.3	Toekomst	117
7.4	Privacyproblemen	119
8	**UWV**	121
	Inleiding	121
8.1	Doel en verwachtingen	121
8.2	Totstandkoming van systemen en projecten	121
8.3	Uitvoering (en resultaten)	122
8.4	Hinderpalen en vraagtekens	125
8.5	Toekomstige voornemens	125
9	**SVB**	129
	Inleiding	129
9.1	Doel	129
9.2	Uitvoering	131
9.3	Resultaten	132
9.4	Hinderpalen en vraagtekens	134
9.5	Toekomst	136
10	**Gemeenten**	139
	Inleiding	139
10.1	Doelen	139
10.2	Opzet systemen	141
10.3	Uitvoering	143
10.4	Resultaten	146
10.5	Privacykwesties	149
10.6	Toekomst	152
11	**BZK**	159
	Inleiding	159
11.1	Doel en uitgangspunten	159
11.2	Risicogestuurd onderzoek naar adresfraude	160
11.3	Landelijke aanpak adreskwaliteit met risico-analyse	162
11.4	Toekomst: vervolg LAA	167
11.5	Project Aanpak Fraude bij ICTU	168
11.6	Basisregistraties: Heel veel data	170

11.7	Relatie Big Data en frauderegistratie	172
11.8	Privacykwesties	174
12	**Veiligheid en justitie, en iCOV**	177
	Inleiding	177
12.1	iCOV: doel en opzet	177
12.2	Opbouw en uitvoering van het systeem	179
12.3	Data-analyse in de praktijk	181
12.4	Research & Development	183
12.5	Resultaten	184
12.6	Hinderpalen en vraagtekens	186
12.7	Toekomstige opties met Big Data	191
12.8	Risicomeldingen malafide bedrijven en Justis	193
12.9	Slot: naar een nieuwe wet	195
13	**Conclusie**	201
	Inleiding	201
13.1	Politieke wens	202
13.2	Zoveel mogelijk data	203
13.3	Beperkte politieke invloed	204
13.4	Transparantie en verantwoording	204
13.5	Privacybotsing	205
13.6	Kaderwet voor minder grenzen	207
Bijlage 1	**21 interventieteamprojecten waarvoor met behulp van de techniek van SyRI bestanden zijn gekoppeld en vervolgens een risicoanalyse is gemaakt**	211
Bijlage 2	**Financiële resultaten uit 21 interventieteamprojecten waarvoor met behulp van de voorloper van 'SyRI' bestanden zijn gekoppeld en vervolgens een risicoanalyse is gemaakt**	213

TEN GELEIDE

WRR Working Paper 21 is geschreven als achtergrondstudie voor het project 'Big Data, privacy en veiligheid'. In dit project verkent de WRR de implicaties van het gebruik van Big Data binnen het veiligheidsdomein.
Deze achtergrondstudie *Big Data en fraudebestrijding* is uitgevoerd door onderzoeksjournalist Peter Olsthoorn. Hij beschrijft in deze studie wat zich in Nederland afspeelt op het terrein van dataverzameling, bestandskoppeling en gegevensanalyse om fraude te voorkomen en/of detecteren. De studie omvat verschillende overheidsdomeinen als gemeentelijke uitkeringen, sociale verzekeringen, belastingen en toeslagen, en criminaliteitsbestrijding. De in deze studie beschreven vormen van data-analyses zijn onder meer het product van de politieke en maatschappelijke wens om door bestandskoppeling effectiever tegen fraude te kunnen optreden. Veel van deze praktijken zijn tot op heden niet of nauwelijks gedocumenteerd. De studie *Big Data en fraudebestrijding* brengt hierin verandering met een uniek en gedetailleerd overzicht van de data-analyses die verschillende overheidsorganisaties en samenwerkingsverbanden van overheidsorganisaties voor fraudebestrijding uitvoeren.

De serie 'Working Papers' omvat studies die in het kader van de werkzaamheden van de WRR tot stand zijn gekomen. De verantwoordelijkheid voor de inhoud berust bij de auteur.

Prof. dr. J. A. Knottnerus
Voorzitter WRR

Dr. F. W. A. Brom
Directeur WRR

1 INLEIDING

iCov? Het Inlichtingenbureau? De meeste Nederlanders, en wellicht ook de meeste parlementariërs en media, zijn onbekend met deze namen. Het zijn onze grootste verzamelaars van persoonlijke 'Big Data', met als belangrijkste doel fraudebestrijding. Helpen ze criminaliteit daadwerkelijk aan te pakken en loopt de privacy van burgers daarbij gevaar?

Vanaf juni 2013 stonden de media bol van onthullingen van Edward Snowden. De Amerikaanse spionagedienst National Security Agency (NSA) blijkt op grote schaal 'data' te verzamelen uit communicatie via telefonie en internet met Google en Facebook.
'Ongeëvenaard', heette het. Maar is dat ook echt zo? Enige invloed van de NSA op het leven van Nederlandse burgers is nauwelijks vastgesteld, er zijn slechts aanwijzingen dat er een (beperkte) uitwisseling van telefoniegegevens is geweest met Defensie.
Terwijl aan de ophef over de Snowden-affaire geen eind leek te komen, werd over onze 'eigen' Big Data-toepassingen nauwelijks iets bericht. Deze toepassingen zijn voor de Nederlandse samenleving – tot op heden – echter van veel grotere en concretere betekenis dan die van de NSA.
De omvang en vooral de invloed van dit onthulde Amerikaanse datagebruik op de Nederlandse burgers staan waarschijnlijk in geen enkele verhouding tot de omvang en invloed van het datagebruik door de Nederlandse overheden, die in tal van samenwerkingsverbanden informatie vergaren, combineren en analyseren ten behoeve van misdaadbestrijding. Daarmee is vooral in de afgelopen jaren een start gemaakt.

1.1 WETSOVERTREDER OF BRAVE BURGER

Selecteer uit het bestand van het Justitieel Incassobureau (CJIB) personen met jaarlijks meer dan drie boetes wegens rijden door rood licht. Is het te rechtvaardigen om specifiek van hen de belastingaangifte extra te controleren?
Hoeveel jaar CJIB-data mag je daarvoor gebruiken? Welke andere data zijn daarbij nog meer nuttig, welke bestanden kun je gecombineerd inzetten?
Of de kernvraag met analyse van data, al dan niet 'big': kun je van elke Nederlander een gedetailleerd frauderisicoprofiel opstellen? Van gezinnen, van families?
Of meer geografisch: fraudeprofielen van wijken, straten of van postcodes? Brabantse wijken met een pakkans op hennepteelt die vijftien keer zo groot is als in een gemiddelde wijk, zouden zo geoormerkt kunnen worden. Net zo goed overigens als bepaalde wijken in Wassenaar, Blaricum en Amsterdam-Zuid zo het stempel brandhaarden van belastingontwijking of zelfs witte boordencriminaliteit opgedrukt zouden kunnen krijgen.

Dit alles is geen science fiction. De Belastingdienst blijkt daadwerkelijk de intentie te hebben om aan de hand van data op naam een 'geïntegreerd beeld' van het historisch gedrag van iedere belastingplichtige samen te stellen om fraudegevoeligheid op te sporen.
Bestanden van de Belastingdienst zijn in gebruik in andere domeinen van fraudebestrijding, met name bij het ministerie van Veiligheid en Justitie (VenJ) (witwassen, zware criminaliteit) en het ministerie Sociale Zaken (SZW) (uitkeringen).
In een toenemend aantal samenwerkingsverbanden delen overheidsinstanties steeds grotere hoeveelheden informatie met elkaar. Dat maakt effectievere fraudebestrijding mogelijk. Bundeling van bestanden en de daaropvolgende data-analyse dienen concreet om risico's op fraude in te schatten, zowel preventief om deze te voorkomen als achteraf om gepleegde fraude aan het licht te brengen.

1.2 POLITIEKE WENS EN CONTROLE

De snelle toename van informatiebundeling ten behoeve van fraudebestrijding komt voort uit een uitdrukkelijke politieke en maatschappelijke wens; misbruik van voorzieningen moest prioriteit krijgen.
Het parlement verwoordde deze eis, aangevuld met bestuurlijke containerbegrippen als de noodzaak tot 'integrale inspanningen' en het 'tegengaan van versnippering'. De ambtelijke vertaling van deze politieke eis was fraudebestrijding vooral door krachtenbundeling; met onder meer letterlijk een bundeling van bestanden om daarin door analyse fraudepatronen en -risico's te kunnen blootleggen.
Is er ook ministeriële en parlementaire controle op de uitkomsten in de praktijk? Is er iets bekend over de effecten van de inzet van middelen en van organisaties die zijn opgetuigd om fraude te beteugelen? Hebben media en het publiek zicht op datagebruik in Nederland voor bestrijding van misdaad? En last but not least, is er voldoende kennis over de ingezette methoden om het maatschappelijk debat te voeren over de grote vraag in deze kwesties, die ongeveer gelijk is als in de NSA-discussie en momenteel in eigen land over de herziening van de Wet op de Inlichtingen- en veiligheidsdiensten (Wiv): welke balans treffen we tussen het voorkomen van terrorisme en de eerbiediging van de privacy?
Of in geval van fraude: welk evenwicht bereiken we tussen noodzakelijke bestrijding van groeiende criminaliteit en het ontzien van 'onschuldige burgers'. Ook in deze discussie lopen gemoederen, al dan niet onder invloed van lobbyisten en door 'framing', gemakkelijk op in (sociale) media tussen personen die bij het woord 'bestandskoppeling' alleen al de noodklok luiden over privacyschending en personen die de termen 'verloedering' en 'criminalisering' in de mond bestorven hebben liggen.
Voor beantwoording van deze kernvraag moet de onderliggende 'casestudy fraudebestrijding' handvatten bieden. De bevindingen zijn vervat in een grote hoeveelheid feiten over toepassing van data-analyse in fraudebestrijding.

De vragen die speelden voor dit onderzoek waren onder meer:
– Welke dataverzameling en -analyse zetten overheden en zelfstandige bestuursorganen in om fraude te voorkomen en/of te detecteren?
– Wat speelt zich op dit terrein van dataverzameling, het combineren van bestanden en gezamenlijke analyse van data in Nederland af, met welke doelstelling en middelen?

Het onderzoek zal zich richten op:
– de doelstellingen en motivaties van datatoepassingen voor fraudebestrijding;
– de weerslag hiervan bij de opzet van systemen;
– de uitvoering van data-analyse van grote bestanden en systemen;
– resultaten van deze uitvoering;
– hindernissen bij de toepassingen en vraagtekens omtrent grenzen, met de nadruk op privacy;
– toekomstige wensen en verwachtingen.

Op onderdelen spelen verder de volgende vragen:
– Vanuit welke interne en externe open en besloten bestanden en domeinen worden de data verzameld?
– Hoe fungeren organisaties en systemen rond data-analyse?
– Waar liggen de grenzen voor gebruik van persoonsgegevens op naam en anoniem – zijn die al dan niet alsnog tot personen te herleiden?
– Welke controle vindt er plaats op de toepassing van de systemen?
– Is er uiteindelijk ook politiek inzicht in en controle op het gebruik van systemen en de eventuele effecten?
– Welke expertise en ondersteuning zijn voorhanden voor controle op de uitvoering?
– Hoe verhouden de datatoepassingen zich tot de privacywetgeving en wat vindt de Autoriteit Persoonsgegevens (AP) ervan?
– Of samenvattend: hoe komen keuzes tot stand en hoe werkt de data-analyse vervolgens en waar willen organisaties heen?

Dat alles concentreert zich rond de kernvraag van dit onderzoek: waar ligt de balans tussen de verwachte adequatere bestrijding van fraude met data-analyse en een afdoende bescherming van de privacy van burgers?

Hoewel een flink aantal terreinen is verkend, is deze casestudy fraudebestrijding niet uitputtend. Het terrein is nog breder dan hier beschreven en een totaal overzicht ontbreekt. Ook voor de politiek.
Het was in het licht van de beperkte opdracht onmogelijk om het hele veld van data-analyse voor fraudebestrijding in kaart te brengen. Een selectie was nodig. De belangrijkste partijen hebben hun medewerking verleend. Het onderzoek strekt zich uit over de domeinen die hiervoor in de inhoudsopgave zijn genoemd,

samen te vatten als de domeinen zorg, criminaliteitsbestrijding, belastingen, uitkeringen/toelagen en arbeidsmarkt.

Een eerste probleem dreigde op te treden bij de te gebruiken terminologie, te beginnen met de term 'Big Data'. Die wordt gehanteerd door grote volumes data, veelal ongestructureerd, die met een hoge snelheid en betrouwbare verwerking leiden tot nieuwe inzichten die beslissingen ondersteunen.
In het zakelijk domein wordt al decennia de Business Intelligence als Business Analytics, oftewel analyses gericht op toekomstig profijt uit voorspellingen. In fraudebestrijding betekent 'Big Data' vooral het voorspellen welke subjecten en objecten naar verwachting het vaakst tot fraude leiden. Dit kan samengaan met profilering van situaties en personen.

Deze nauwe definitie is uiteindelijk verlaten voor dit onderzoek. Ten eerste gaat Big Data uit van een compleet nieuwe wereld. Ten tweede speelt data-analyse al jaren een grote rol bij fraudeopsporing, is zij eerder evolutionair dan revolutionair. Bovendien lopen analyse van verleden en heden en het voorspellen van toekomst door elkaar. Dat is niet uniek voor de datawereld. Ook personen wegen in het dagelijks leven af of in het verleden behaalde resultaten (g)een garantie voor de toekomst inhouden.
Betrokkenen spraken ook wel over *little data*: daarmee wezen ze behalve op een beperkte omvang, ook op zaak- en persoonsgerichte data, veelal met een min of meer concrete verdenking.
Dit impliceert direct de kern van dit onderzoek: waar de term 'Big Data' vooral van toepassing is op patroonherkenning in grote hoeveelheden, doorgaans geanonimiseerde en ongestructureerde data, richten speurders naar fraude zich op het zo snel mogelijk in beeld brengen van fraudeurs op naam.
Ze zijn dus voorstander van het toepassen van Big Data, van grote hoeveelheden gegevens, maar daarbij vooral gericht op het schakelen naar concrete frauderisico's en naar pakkansen van fraudeurs en uiteindelijk het duiden op naam, opdat verdachten 'in de kraag gevat' kunnen worden.
De huidige werkwijze van fraudebestrijders bestaat vaak uit het combineren van (Big) Databestanden en 'little data' voor het oplossen van concrete zaken. Het uiteindelijke doel van de uitdijende data-exercities is niet louter het ontwaren van generieke patronen die tot fraude leiden – dat is een tussenstap – maar ook van patronen van fraude en kenmerken van zogenoemde recidivisten, oftewel 'beroepsfraudeurs'.
Bij de patronen passen subjecten: organisaties en personen op naam. Van belang is daarbij wel in hoeverre patronen voorspellende waarde hebben, en verder of ze tot profilering of zelfs stigmatisering leiden. Door de weerstand die dit oproept, rees gedurende dit onderzoek de vraag of het mogelijk en goed is om deze ongewenste effecten compleet te verbieden of uit te bannen.

Net zoals wij in ons persoonlijke leven beelden van verwachtingen van personen en situaties laten meewegen in onze besluiten, is dit echter ook bij data-exercities van organisaties altijd het geval. Verwachtingen en verdenkingen zijn 'natuurlijke bondgenoten' van data-analyse.

Een tweede theoretisch probleem betrof de terminologie die hier het gevolg van is. Afwisselend worden de begrippen data-analyse, risicoanalyse, datamining, risicoprofielen en bestandsvergelijking gehanteerd. Ze betekenen ongeveer hetzelfde: het analyseren van data(bestanden), teneinde risico's op fraude (anomalieën of zelf verdenkingen) te kunnen vaststellen.

De precieze betekenissen zijn:
- Datamining is zoeken naar opvallende zaken en verbanden in (grote) databestanden.
- Data-analyse is het analyseren van de bestanden als zodanig.
- Risicoanalyse is het onderzoeken en vaststellen welke risico's er zijn, of dat nu in het uitvoeringsproces (handmatig en geautomatiseerd) of in klant- en uitkeringskenmerken is.
- Risicoprofielen zijn risicovolle klantkenmerken of verzamelingen klantkenmerken die uiteindelijk leiden tot het oormerken (profileren) van groepen personen met dezelfde kenmerken of zelfs individuele klanten.
- Bestandsvergelijking: vergelijken van data uit het ene bestand met dat uit een of meer andere bestanden, teneinde afwijkingen vast te stellen.

In deze casestudy fraudebestrijding is de voorkeur gegeven aan de meest algemene term 'data-analyse', omdat die het eenvoudigst de gemene deler weergeeft van verschillende handelingen met data die keuzes ondersteunen, in dit geval ter voorkoming van fraude en de opsporing daarvan.
Woordvoerders spreken zelf over zowel 'informatiegestuurd handhaven' (IGH) als 'analysegestuurd handhaven' en bedoelen daar hetzelfde mee: fraude bestrijden en voorkomen, met behulp van risicoprofielen en/of indicatoren, of dat in alledaags taalgebruik ook wel genoemd wordt: verdenkingen scoren. En dat met behulp van datagebruik.

Een derde euvel, en niet het geringste, betreft de structuur van dit onderzoek. In de onderzoeksjournalistiek die ik dagelijks bedrijf, zijn selectie en weergave voortdurend mede gericht op het boeien van lezers. Dat is onmogelijk met behoud van alle nuances.
Dat werd door de bronnen in dit onderzoek niet gewaardeerd, uiteraard terecht. Vaak gaat het juist bij dataverzameling en –gebruik voor fraudebestrijding door overheden om zwaar bevochten nuances en details.

Dit heeft mede geleid tot een veel grotere omvang van het onderzoek dan aanvankelijk was beoogd. De keuze is gemaakt voor een uitputtende weergave in een logische samenhang en niet voor een journalistieke selectie.

Na deze inleiding volgt in hoofdstuk 2 een uiteenzetting over de geschatte omvang van het fraudeprobleem. Hoofdstuk 3 heeft het onjuist declareren in de zorg tot onderwerp, het terrein waar de invloed van het verantwoordelijke departement en de politiek relatief gering is.
Vervolgens komen vooral overheden en bestuursorganen aan bod. Te beginnen in hoofdstuk 4 met de Belastingdienst, de voorloper in data-analyse en de meest gewilde partij in samenwerkingen vanwege zijn hoeveelheid relevante data.
Deze gaan onder meer naar het Inlichtingenbureau (IB), besproken in hoofdstuk 5, dat vele tientallen bestanden kan koppelen en analyseren, en aan overheden signalen doorgeeft die op fraude kunnen duiden. Klant zijn bijvoorbeeld de interventieteams van overheden die samen fraude bestrijden in bijvoorbeeld risicovol geachte wijken, op basis van het met wetswijzigingen gelegitimeerde systeem SyRI voor bestandskoppeling (hoofdstuk 6).
De leiding berust bij de Inspectie SZW, besproken in hoofdstuk 7, die nog meer data-analyse opzet. Deze heeft een nauwe samenwerking met het UWV, dat verregaande plannen en wensen met data-analyse openbaart (hoofdstuk 8), gevolgd door 'zuster' Sociale Verzekeringsbank (SVB), die zich na de nodige tegenslag bescheiden opstelt (hoofdstuk 9).
Net als het UWV en de SVB pogen gemeenten misbruik van voorzieningen krachtiger aan te pakken met inzet van data, na aanvankelijke mislukkingen (hoofdstuk 10). Ze werken samen met het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK), besproken in hoofdstuk 11, aan betere adresbestanden waarmee veel fraude en data-analyse samenhangen.
Tot slot komt in hoofdstuk 12 het ministerie van Veiligheid en Justitie aan bod (VenJ), met het samenwerkingsverband ICOV dat grote hoeveelheden data verwerkt voor de opsporing van vooral financiële fraude. De casestudy eindigt met conclusies en de beoogde Kaderwet Gegevensuitwisseling, waar veel instanties die fraude bestrijden, hun hoop op gevestigd hebben voor ruimere bevoegdheden.

Dan rest me nu dank te zeggen aan de voortreffelijke woordvoerders van de organisaties die aan dit onderzoek hun bereidwillige medewerking verleenden, vaak met aanzienlijke inspanningen en uiteindelijk ook de nodige flexibiliteit om zich te plooien naar de onderzoeksopdracht.
Transparantie en fraudebestrijding zijn immers geen natuurlijke bondgenoten. De woordvoerders hechtten niet slechts aan een hoge kwaliteit van informatie over hun werkterrein die tot een nog niet eerder diepgaand overzicht van de fraudebestrijding heeft geleid. Bovenal konden ze een kritische instelling en verslaglegging waarderen en besloten ook hun onzekerheden te delen, zoals de spanningsvelden tussen opsporing en privacy bij de pogingen om fraude te bestrijden.

Ook de Wetenschappelijke Raad voor het Regeringsbeleid – opdrachtgever van deze achtergrondstudie - ben ik veel dank verschuldigd, zowel voor zijn betrokkenheid tijdens het onderzoek als bij de productie daarvan. De hulp van met name WRR-medewerkers Erik Schrijvers en Dennis Broeders heeft me behoed voor het vallen in de nodige valkuilen.

Peter Olsthoorn

2 OMVANG VAN DE FRAUDE EN BELEID

INLEIDING

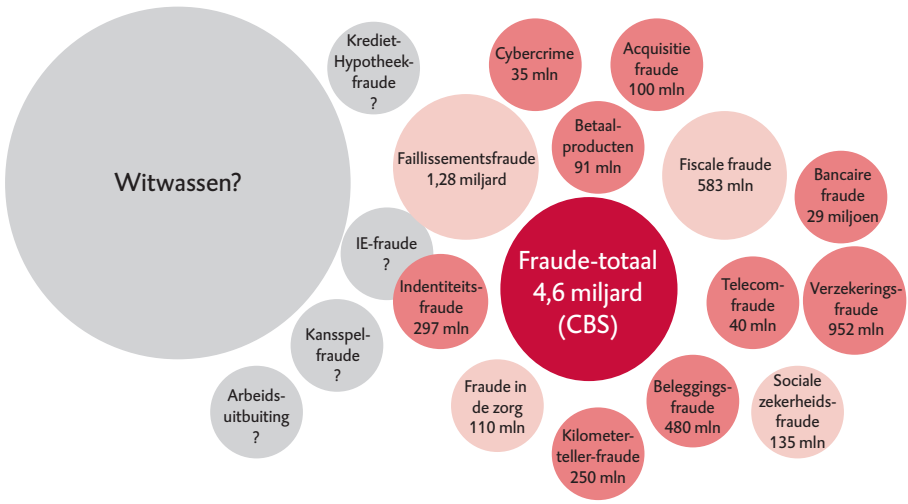
Fraude is bedrog. Dat is de kortste definitie. Van de opgesomde definities op Encyclo.nl is deze verreweg het helderst: 'Het misleiden, bedriegen of schenden van vertrouwen met als doel een oneerlijk of onrechtvaardig voordeel of materialistische winst te verkrijgen.' Hoe omvangrijk is het fraudeprobleem in Nederland? En hoe is dat verdeeld over de verschillende (beleids)terreinen? Daarover zijn geen eenduidige cijfers bekend, onder meer omdat de overheid daarnaar, voor zover bekend, geen onderzoek heeft laten doen. Dit heeft in elk geval tot gevolg dat de verschillende overheden, zelfstandige organen en samenwerkingsverbanden niet van dezelfde cijfers uitgaan. Ook ontbreekt historisch inzicht.
Soms wordt daarvan gebruikgemaakt in de lobby vanuit opsporingsinstanties: er circuleert altijd wel ergens een hoog bedrag dat een eigen leven kan gaan leiden. Aan de ene kant is die onwetendheid logisch: van niet-opgespoorde misdaad is de omvang onbekend. Fraude is veelal administratief, en daardoor niet zo zichtbaar. Maar ten minste zou de overheid een opsomming kunnen maken van jaarlijks vastgestelde fraude. Ook dat stuit echter op problemen: ontdekte onregelmatigheden duiden niet altijd op opzet. Vooral in de zorg (hoofdstuk 3) is er een enorm verschil in omvang van vastgesteld onjuist declareren en fraude.
Deze voorzichtigheid om gedrag als 'frauduleus' te bezoekstaven betreft vooral artsen. Bij uitkeringsgerechtigden heeft deze voorzichtigheid jarenlang ontbroken. Daar zijn te veel geïnde bedragen wel standaard als 'fraude' geoormerkt.

In de jongste projecten voor fraudebestrijding hanteren overheden steeds vaker de term 'businesscase': de investering in een maatregel moet rendabel zijn, dus ten minste het terugverdienen van die investering tot doel hebben. Dat leidt wellicht tot nauwkeuriger rekenen. Heel ruw: ten minste een kleine 10 miljard euro aan opgespoorde plus niet-getraceerde, geschatte, fraude. Naar wat je niet weet, mag je raden.
Dit past bij de ontwikkeling van fraudebestrijding. Een hoog geschatte fraude rechtvaardigt – en noodzaakt tot – daadkracht. Er kwam een ministeriële commissie-Aanpak Fraude, waarvan nauwelijks meer iets is vernomen.
Ondertussen 'vernetwerkte' de overheid in hoog tempo, teneinde de gewenste intensievere samenwerking in fraudebestrijding tot stand te brengen. En om de veelvuldig geëiste vermindering van 'versnippering' van inspanningen – een mantra van het parlement – in praktijk te brengen.

2.1 DE RUWE BEDRAGEN

Het Centraal Bureau voor de Statistiek (CBS) becijferde fraude in Nederland op 4,6 miljard euro, exclusief witwassen (zie figuur 2.1).

Figuur 2.1 Maatschappelijke schade van verschillende vormen fraude



Bron: NVVB Congres –14 & 15 mei 2014. Judy Moester en Michel Savelkoul. Agentschap BPR workshop fraudeprofielen.

Het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC), de Raad voor de rechtspraak en het CBS ramen de totale schade voor de overheid door criminaliteit elders echter op ruim 660 miljoen euro op jaarbasis, waarvan een groot deel belastingontduiking of andere fraude, die in de meeste gevallen wordt opgespoord door de bijzondere opsporingsdiensten.
'Met middelzware en lichte fraudegevallen is naar schatting een bedrag van ongeveer 130 miljoen euro op jaarbasis gemoeid. Gemiddeld wordt er 34 miljoen euro aan zware socialeverzekeringsfraude opgespoord.'[1]

Uitkeringsfraude is een terugkerend onderwerp in de media. Zo liet Het Landelijk Contact Sociaal Rechercheurs optekenen dat 10 à 20 procent van de mensen in de bijstand fraudeert, wat zou neerkomen op bijna 1 miljard euro aan fraude per jaar.[2]

1 Uit Criminaliteit en Rechtshandhaving over 2014, CBS, oktober 2015, http://www.cbs.nl/nl-NL/menu/themas/veiligheid-recht/publicaties/publicaties/archief/2015/2015-criminaliteit-rechtshandhaving-2014-pub.htm (laatst geraadpleegd 19 april 2016).

2 http://www.telegraaf.nl/dft/geld/20053976/__Bijstandsfraudeurs_hebben_vrij_spel__.html (laatst geraadpleegd 19 april 2016).

Nadruk op fraudebestrijding keert periodiek als thema terug in de politiek. In antwoord op Kamervragen antwoordde staatssecretaris van het ministerie Sociale Zaken en Werkgelegenheid (SZW) Paul de Krom dat in 2010 in de sociale zekerheid voor 119 miljoen euro aan fraude met uitkeringen is aangetoond, waarvan 53 miljoen euro in de bijstand: 'Het werkelijke fraudebedrag zal ongetwijfeld hoger zijn. Van de niet-geconstateerde fraude kan echter geen betrouwbare schatting gemaakt worden.'[3]

De Rekenkamer rapporteerde in 2013 dat de omvang van fraude met publieke middelen niet precies is vast te stellen, omdat ministeries geen betrouwbare schattingen publiceren. Dus nam de Rekenkamer haar toevlucht tot de bron 'Burgerinitiatief 1 overheid', die een grove inventarisatie maakte. Volgens de Rekenkamer biedt deze niettemin 'een beeld' waar fraude het meest voorkomt:[4]

- belastingfraude: minimaal 4 miljard euro;
- zorgfraude: 2 à 3 miljard euro;
- sociale uitkeringsfraude ongeveer 1 miljard euro.

De cijfers van de Rekenkamer zijn opvallend, omdat het laatste bedrag zeer afwijkt van dat aan socialeverzekeringsfraude becijferd in Criminaliteit en Rechtshandhaving.
Ook adviesbureau PricewaterhouseCoopers (PwC) becijferde de socialeverzekeringsfraude veel lager dan de Rekenkamer: zo'n 150 miljoen euro per jaar. De eerste twee bedragen van de Rekenkamer komen wel grofweg overeen met de schattingen door PwC, die de belastingfraude op 4,2 miljard schatte en de zorgfraude op 3 miljard. Overigens is fraude een juridisch vergrijp, dat echter zelden tot vervolging, en daarmee een definitieve vaststelling van de wetsovertreding, leidt. Zie daarvoor vooral het hoofdstuk over de zorg in deze rapportage.

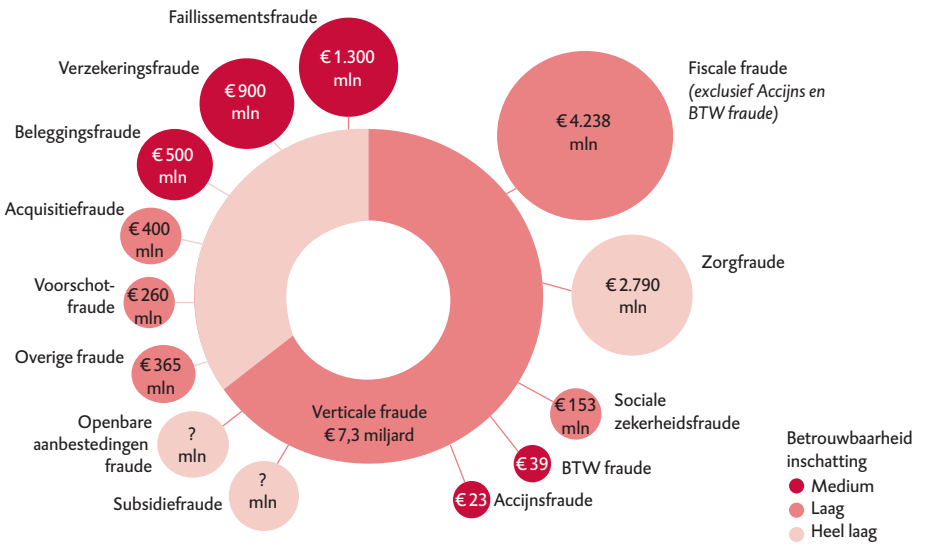
PwC berekende een totale 'minimale' jaarlijkse fraude van 11 miljard euro. Het zou gaan om een schatting, 'niet meer dan een eerste vingeroefening van het in kaart brengen van de fraudeomvang' (figuur 2.2). Bij gebrek aan eigen cijfers namen diverse overheden, waaronder het ministerie van BZK, deze cijfers over in hun presentaties. Het zijn om die reden gangbare bedragen geworden.

---

3 Antwoord vragen Tweede Kamerlid L.E.W. de Jong over het bericht "Bijstandsfraudeurs hebben vrij spel" https://www.tweedekamer.nl/kamerstukken/kamervragen/detail?id=2012Z10119&did=2012D 24640

4 http://verantwoordingsonderzoek.rekenkamer.nl/2013/rijksbreed/themas/fraude/geen-harde-cijfers-over-omvang-fraude-wel-schattingen (laatst geraadpleegd 19 april 2016).

Figuur 2.2 Omvang van de fraude, per soort



Bron: PwC, Naar een fraudebeeld, Nederland Amsterdam, 19 december 2013, http://www.pwc.nl/nl/publicaties/naar-een-fraudebeeld-van-nederland.html (geraadpleegd 19 april 2016)

PwC verbond er suggesties voor bestrijding aan, waarvan data-analyse een belangrijke is: informatie en expertise combineren, waardoor nieuwe inzichten en signalen ontstaan en handhavers over meer kennis kunnen beschikken om fraude te bestrijden.
Dit vereist, aldus PwC, investeringen in IT en in mankracht voor nader onderzoek van de signalen uit data-analyse. Volgens PwC is een Brits programma hiertoe opgezet succesvol: voor elke geïnvesteerde pond is 10 pond fraude vermeden dankzij 'slimme technieken' waarmee fraudepatronen worden herkend. Behalve voor opsporing is dit programma ook te gebruiken voor preventie, 'en dit zou daar mogelijk zelfs veel effectiever kunnen zijn'.
Gewezen werd daarbij op de oprichting van een National Fraud Authority, alsmede een ministeriële taskforce, die acht pilots met data-analyse in gang zette. De Britse regering doekte deze NFA weer op, maar volgens adviesbureaus zouden Nederlandse overheden hoe dan ook miljarden kunnen verdienen met nieuwe methoden voor data-analyse.
PwC waarschuwt tegen '*pennywise and pound foolish*' handelen en noemt de Bulgarenfraude met toeslagen daarbij als voorbeeld. Deze zaak kreeg veel aandacht, maar de omvang was relatief gering en de opsporing vergde veel inzet.

Schadeschattingen belopen soms nog meer dan 11 miljard euro, als onderbouwing en legitimatie van inspanningen om fraude te voorkomen c.q. te bestrijden. Bijvoorbeeld door Infobox Crimineel en Onverklaarbaar Vermogen (ICOV), gericht op

het ontdekken en vorderen van crimineel vermogen. iCOV noemt in dit onderzoek een bedrag aan fraude bij de Nederlandse overheid van 16,5 miljard euro, 55 procent van de in totaal 30 miljard euro geschatte fraude in Nederland.
Dit fraaie ronde bedrag is echter een ruwe schatting van een adviesbureau, dat publiciteit genereerde met een nattevingeronderzoek: uitkeringsfraude per jaar 3 miljard euro en belastingfraude 10 miljard euro (maar wellicht 23 miljard euro).[5]
Hoe dan ook: het bedrag aan uitkeringsfraude van 135 miljoen (CBS-cijfers) of 3 miljard euro, waarvan circa de helft met Wet Werk en Bijstand (WWB)-uitkeringen, vormt minder dan 10 procent van de totale bedragen die met fraude gemoeid zijn. Ofschoon bijstandsfraude een relatief gering deel uitmaakt van de totale fraude, is de aandacht hiervoor het grootst.
Zo ligt het zwaartepunt in de eerste resultaten van het zoeken op het woord 'fraude' bij zowel via Google.nl als op CBS.nl op bijstandsfraude. (Ook dat is overigens een gevolg van toepassing van Big Data en algoritmes).
Wel werd in het voorjaar van 2015 bekend dat er bij gemeenten voor 1,4 miljard euro aan bijstandsvorderingen openstaat, waarop sociaal rechercheurs 'alarm sloegen'. Dit wierp een licht op de grote verschillen in aanpak van vermeende en vastgestelde fraude door gemeenten.[6]

2.2 MINISTERIËLE COMMISSIE-AANPAK FRAUDE

In 2013 werd besloten tot de oprichting van een ministeriële commissie-Aanpak Fraude, onder voorzitterschap van de premier en de minister van VenJ als coördinator. Ook de ministers van SZW, Economische Zaken (EZ), Volksgezondheid, Welzijn en Sport (VWS), BZK, Onderwijs, Cultuur en Wetenschap (OCW), Wonen en Rijksdienst en de staatssecretaris van Financiën zijn vaste deelnemers aan de ministeriële commissie-Aanpak Fraude.
De oprichting van deze commissie was het antwoord van het kabinet op een voorstel en motie vanuit de Tweede Kamer, van de leden Gesthuizen (SP) en Berndsen (D66) voor de oprichting van een nationale fraudeautoriteit en het aanstellen van een nationale fraudecommissaris zoals in Engeland de eerder genoemde – inmiddels opgeheven – National Fraud Authority.
Het kabinet verkoos daarbij de weg van coördinatie boven de oprichting van een fraudeautoriteit en/of de aanstelling van een nationale fraudecommissaris. De toenmalige minister Opstelten van VenJ kenschetste daarbij de verdeling van ver-

5 'Fraude kost Nederland jaarlijks 30 miljard. Aanpak loont', Schalke & Partners, zonder datum http://www.schalke.nl/pdf/FRAUDE-totaaloverzicht%202014.pdf (Geraadpleegd 17 februari 2016).

6 http://www.trouw.nl/tr/nl/4492/Nederland/article/detail/3992203/2015/05/01/1-4-miljard-aan-bijstands fraude-nog-niet-geind.dhtml (Geraadpleegd 19 april 2016).

antwoordelijkheden tussen bewindspersonen als helder.[7] De commissie leidt de uitvoering van een Rijksbreed actieplan, dat eind december 2013 werd gepresenteerd.[8]

De oprichting van een commissie leek een nieuwe benadering, maar in de praktijk wordt fraudebestrijding periodiek met een maatregel opnieuw in de schijnwerper gezet. Zo werd al in 1979 de Interdepartementale Stuurgroep Misbruik en Oneigenlijk Gebruik (ISMO) ingesteld, gericht op indamming van de groeiende uitgaven voor collectieve voorzieningen.
En kwamen er in 1993 onder premier Lubbers een 'task-force fraudebestrijding' en een 'ministeriële commissie-fraudebestrijding'. Behalve Lubbers namen ook de ministers Hirsch Ballin (Justitie), De Vries (SZ) en Kok (Financiën) zitting in de commissie-fraudebestrijding, die tot taak kreeg om het fiscale en sociale fraudebeleid te coördineren. En daarin werd gesteund door een ambtelijke stuurgroep onder leiding van Winnie Sorgdrager, toen nog procureur-generaal te Arnhem. Voor Lubbers was de aandacht voor fraude 'een speerpunt van beleid' als gevolg van een veranderd maatschappelijk klimaat, waarin de behoefte bestond fraude daadwerkelijk aan te pakken: 'De burger vraagt aan de overheid iets te doen.'[9]
In 1994 werd dit speerpunt vertaald in een 'Regeling taak en samenstelling Stuurgroep fraudebestrijding' van, inmiddels, minister Winnie Sorgdrager van Justitie.[10] Doel: versterking van de fraudebestrijding en de coördinatie daarvan.

Een van de vier speerpunten van het rijksbrede actieplan luidt: goed functionerende basisregistraties en een verbeterde informatiepositie. Overheden zouden veel intensiever moeten samenwerken, ook in hun uitwisseling van informatie. Gezamenlijke risicoanalyse van bestanden, te beginnen bij adresregistraties, is van groeiend belang.

---

7 'Stand van zaken inzake coördinatie fraudebestrijding'. Kamerbrief 'Misbruik en oneigenlijk gebruik op het gebied van belastingen, sociale zekerheid en subsidies', minister Opstelten van Veiligheid en Justitie aan de Voortouwcommissie-Veiligheid en Justitie, Nummer 17050-491, 21 november 2014. http://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2014Z21410&did=2014D43220 (geraadpleegd 19 april 2016).

8 'Misbruik en oneigenlijk gebruik op het gebied van belastingen, sociale zekerheid en subsidies – Bestrijding georganiseerde criminaliteit', Brief van De Minister van Veiligheid en Justitie aan de Tweede Kamer, 20 december 2013 http://www.tweedekamer.nl/downloads/document?id=51cc8d05-5108-456b-aac4-4a12f5cb33ff&title=Rijksbrede%20aanpak%20van%20fraude.pdf (geraadpleegd 19 april 2016).

9 http://www.nrc.nl/handelsblad/1992/09/15/ministeriele-commissie-leidt-aanpak-fraude-7156006. (geraadpleegd 19 april 2016).

10 Regeling taak en samenstelling Stuurgroep fraudebestrijding http://wetten.overheid.nl/BWBR0007235/geldigheidsdatum_02-01-2016

Het kabinet heeft in vele toonaarden fraudebestrijding als 'prioriteit' genoemd. Onderstaand nog enkele duidingen, met tot slot een uiteenzetting van nieuwe wetgeving op dit terrein:
'Een belangrijke manier om fraude te voorkomen, te ontdekken en te bestraffen is het delen van gegevens of indicatoren voor mogelijke fraude die de overheid of andere organisaties beschikbaar hebben. Het is cruciaal om (realtime) informatie te kunnen uitwisselen en in te kunnen grijpen […] Het is daarom zaak de mogelijkheden van gegevensuitwisseling en daarmee controle vooraf optimaal te benutten', aldus minister Opstelten in een brief aan de Tweede Kamer eind 2013.[11] Daarin benadrukt hij de preventieve functie van data-analyse; het voorkomen van overtredingen 'aan de digitale poort'.
Hij zegde toe om in een viertal casussen te inventariseren aan welke gegevensuitwisseling behoefte is, inclusief 'best practices', ook in de vorm van mogelijk bestaande 'privacyprotocollen' voor 'samenwerkingsverbanden':
– gefingeerde dienstverbanden;
– faillissementsfraude;
– identiteitsfraude;
– notoire fraudeurs ('subjectgerichte fraudebestrijding').

Ook kondigde hij een 'verkenning' aan naar de noodzaak van de invoering van een 'kaderwet voor de gegevensuitwisseling op het bredere terrein van fraudebestrijding'. Ervaringen met de wet-SUWI zouden daarin meegenomen kunnen worden. Daarover meer in het slothoofdstuk.
Tevens versterkte de minister het systeem van Toezicht op Rechtspersonen (TRACK) van de dienst Justis van zijn ministerie met een 'vroegtijdige signaleringsfunctie', gecombineerd met meer 'verfijnde risicoprofielen van beroepsfraudeurs': personen die met verschillende regelingen fraude plegen.
De laatstgenoemde analyse en profilering betreffen niet de vormen van fraude, maar verdachte personen. Ook hier gaat het, aldus de minister, om een verkenning van de mogelijkheden voor analyses van gecombineerde databestanden om verdachten te oormerken. Daartoe werd ook een 'combiteam aanpak facilitators' binnen de Belastingdienst ingericht.
Voor het onderhouden van TRACK hebben Belastingdienst en Justis een convenant ondertekend voor intensieve uitwisseling. De onderliggende wet is de Wet controle op rechtspersonen. Volgens de minister zou de Nationale Politie een capaciteit voor financieel-economische criminaliteit (FinEC) krijgen van 1150 fte. De Dienst Regionale Recherche zou ook 'FinEC / fraudeteams' krijgen.

11 'Rijksbrede aanpak van fraude' Brief van de regering, , Nummer 17050-450, 20 december 2013, I.W. Opstelten, minister van Veiligheid en Justitie aan de Voortouwcommissie Veiligheid en Justitie. (geraadpleegd 19 april 2016)
http://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2013Z25369&did=2013D51734 (geraadpleegd 1 februari 2016).

2.3 SLIM VOORKOMEN, VLOT HERSTELLEN

Op verschillende terreinen zou intensieve samenwerking fraude moeten terugdringen, bijvoorbeeld identiteitsfraude. Verschillende kabinetsleden uitten de boodschap van data delen op uniforme wijze. Al eerder is de minister van SZ uitgebreid geciteerd.
Eind december 2013 stuurde minister Plasterk van BZK de kabinetsvisie op de aanpak van identiteitsfraude, 'Slim voorkomen, vlot herstellen' getiteld, aan de Kamer. Dit beoogde een modus operandi te zijn bij onder meer illegale grenspassage, illegale arbeid, mensensmokkel, drugshandel, terrorisme, witwassen en vele soorten fraude.
Daarmee wordt de kiem gelegd voor een brede uitwisseling van data van overheden onderling, van publieke en private databestanden over de landsgrenzen heen, waarvoor ook Europol, de Europese opsporingsinstantie, al een warm pleidooi hield.
Minister Plasterk: 'Voorkomen en herstellen van identiteitsfraude vraagt om een integrale, informatiegestuurde aanpak waarin partners in publieke en private sector de krachten samenballen. Grote organisaties en zware ketens zijn kwetsbaar tegenover de kleine, creatieve, wendbare dadergroepen die hen bestoken en die makkelijk van aanvalsstrategie kunnen veranderen.'[12]
Dit was conform de wens van de Tweede Kamer voor een 'integrale visie' en het tegengaan van versnippering van overheidstaken. 'Het antwoord op identiteitsfraude komt van moderne netwerken die snel en adequaat reageren. Van bolwerken naar netwerken. De sterk toegenomen aandacht voor fraude stimuleert betrokken partijen tot samenwerken: zowel op regionaal, als landelijk niveau. Met succes: door gebruik te maken van elkaars kennis en informatie worden fraudeurs gesignaleerd en nieuwe maatregelen tegen fraude snel geïmplementeerd', aldus de minister.

2.4 'VERNETWERKING' ALS DOEL EN MIDDEL

Minister Plasterk verwees daarbij onder meer naar de Manifestgroep, die een structureel samenwerkingsverband had opgezet voor de operationele aanpak van fraude. Dit resulteerde in de oprichting van een Expertisecentrum Fraude bij de Belastingdienst, met deelname van het UWV, de Belastingdienst, het CAK, het CBS, het Centrum Indicatiestelling Zorg (CIZ), het Centraal Justitieel Incassobureau (CJIB), Zorginstituut Nederland, Dienst Justis, de Rijksdienst voor Ondernemend Nederland (RVO), Dienst Uitvoering Onderwijs (DUO), de Immigratie- en Naturalisatiedienst (IND), het Kadaster, de Kamer van Koophandel (KvK), de Rijksdienst

12 Kabinetsvisie aanpak identiteitsfraude - 'Slim voorkomen, vlot herstellen', minister Plasterk van BZK, 20 december 2013 http://www.tweedekamer.nl/kamerstukken/detail?id=2013D51829&did=2013D51829 (geraadpleegd 1 februari 2016).

voor het Wegverkeer (RDW) en de Sociale Verzekeringsbank (SVB) samen (zie onderdeel Belastingdienst samenwerkingen).
Ook de partijen in de 'vreemdelingenketen' gingen intensiever data uitwisselen, te weten de IND, de Nationale Politie, de Koninklijke Marechaussee (KMar), het Centraal Orgaan Opvang Asielzoekers (COA) en de Dienst Terugkeer & Vertrek (DT&V).
Een 'brede community Identiteitsfraude' werd aangekondigd, op te bouwen in samenwerking met het Centrum voor Informatiebeveiliging en Privacybescherming (CIP). Met deelname van de partijen in de Manifestgroep, de Nationale Politie, de KMar en de Vereniging van Nederlandse Gemeenten (VNG).
Dit zou aanvullend zijn op de reeds bestaande samenwerkingen in de Regionale Informatie- en Expertisecentra (RIEC), bij de Regionale Coördinatiepunten Fraude (RCF's) en de Landelijke Stuurgroep Interventieteams (LSI), de samenwerking in bestrijding van zorgfraude en een convenant dat 81 gemeenten in Oost-Nederland hebben getekend om de identiteitsfraude bij de afdeling Burgerzaken harder aan te pakken.
Kortom: de verschillende partners zouden in meerdere samenwerkingen leiden tot meerdere dwarsverbanden waardoor informatie-uitwisseling niet meer begrensd of versnipperd zou zijn. Dit was conform de wens van de Tweede Kamer. Plasterk: 'Deze vernetwerking van de overheid maakt een informatiegestuurde, integrale aanpak van identiteitsfraude mogelijk, zoals beoogd in de visie.'[13]
Dit sluit ook aan bij de afspraken voor samenwerking tussen publieke en private sector van het Nationaal Platform Criminaliteitsbeheersing. De aanpak van fraude noodzaakt tot 'het ontwikkelen van een informatiepositie […] alsmede om het beter benutten van communicatiemogelijkheden […]'[14]

13 Kamerbrief Aanpak Identiteitsfraude, 11 juli 2014 https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2014/07/11/kamerbrief-over-aanpak-identiteitsfraude/kamerbrief-over-aanpak-identiteitsfraude.pdf (geraadpleegd 1 februari 2016).

14 Idem.

3 ZORG

INLEIDING

De invoering van het nieuwe zorgstelsel begin 2006 leidde tot hernieuwde aandacht voor bestrijding van fraude. Deze faalde in de eerste jaren. Op aandrang van het parlement is vervolgens een uitgebreide samenwerking opgetuigd tussen partijen in de zorg.
Een serie initiatieven voor bestrijding van zorgfraude zag het licht, met centraal een 'Expertisecentrum', dat met onder meer intensieve dataverwerking fraude en andere 'onregelmatigheden' hielp bestrijden. Eind 2015 is dit centrum in stilte opgeheven. Het was een mislukking, een teken van de problematische samenwerking in de zorgfraudebestrijding.
Wel werd er overigens jaarlijks voor miljarden aan 'onregelmatigheden' van medisch declareren getraceerd dankzij individuele verzekeraars.
Behalve samenwerking is de inzage in patiëntdossiers een heikel punt in de zorg. Om zorgfraude beter te kunnen aantonen willen verzekeraars eenvoudiger inzage, maar dit stuit op privacyzorgen. Als oplossingen worden gezien de medewerking van patiënten en het mogelijk toekomstige beheer van hun zorgdossier, inclusief inzage in declaraties.
Privacyafwegingen komen daarmee bij het individu te liggen, zeker indien er financiële prikkels bij zullen komen. Deze spanningsvelden maken het de zorg tot een uiterst interessant terrein in de fraudebestrijding met behulp van grootschalige data-analyse. Dat openbaart zich ook in de vele details van de onderstaande beschrijvingen.

3.1 BELEID EN MISLUKKINGEN

Valse start

Fraudebestrijding in de zorg kwam jarenlang moeilijk van de grond. In de media werd gesproken over een falen van het kabinet-Rutte I op dit punt. Zelfs de beoogde inning van een relatief bescheiden bedrag van jaarlijks 47 miljoen euro aan onterechte declaraties mislukte aanvankelijk, ofschoon de omvang ervan groot werd geacht: in een (concept)rapport van 2012, dat gedetailleerd ingaat op wijzen van frauderen, staat bijvoorbeeld dat ziekenhuizen en privéklinieken alleen al jaarlijks voor 50 tot 180 miljoen euro aan behandelingen declareren zonder medische noodzaak.
Het betrof een conceptrapport PInCet (Project Intensivering Controle en Toezicht), dat Rtl in zijn bezit kreeg, maar dat de minister van VWS niet naar de

Tweede Kamer had gestuurd. Volgens haar was het gebrek aan eensgezindheid bij de deelnemende partijen over de eindversie reden geweest om het niet te sturen.[15] De Kamer eiste daarop maatregelen voor zorgfraudebestrijding, wijzend op 'sjoemelende zorginstellingen, frauderende ziekenhuizen en malafide pgb-bemiddelingsbureaus'.
De Kamer drong aan op intensieve samenwerking tussen alle partijen betrokken bij de financiering van de zorg en in een motie op een 'samenhangend werkprogramma' voor de aanpak van fraude in de zorg. De samenwerking en samenhang die het parlement eiste, vormden de opmaat naar verder gezamenlijk gebruik van databestanden voor fraudebestrijding. Zowel ingeval van verdenkingen als voor het analyseren van risico's vanuit grote hoeveelheden data.[16]

Collectief initiatief

Dit culmineerde in een gezamenlijke inspanning van de zorgsector. In maart 2013 tekenden negen partijen onder leiding van het ministerie van VWS een breed convenant tegen zorgfraude. De belangrijkste motivatie daarvoor was dat fraude zowel de betaalbaarheid als de solidariteit van de zorg onder druk zet en dus bestreden dient te worden. Onder leiding van VWS tekenden ook de volgende partijen:

- Nederlandse Zorgautoriteit (NZa);
- Inspectie voor de Gezondheidszorg (IGZ);
- Zorgverzekeraars Nederland (ZN);
- Centrum Indicatiestelling Zorg (CIZ);
- Inspectie Sociale Zaken en Werkgelegenheid (Inspectie SZW);
- Fiscale Inlichtingen en Opsporingsdienst (FIOD);
- Belastingdienst;
- Openbaar Ministerie (OM).

15 Rapport PInCeT: Project Intensivering Controle en Toezicht op de rechtmatige uitvoering van de Zorgverzekeringswet (versie 25-06-2012): procesbeschrijving en verbeteringen http://www.tweedekamer.nl/kamerstukken/detail?id=2013D20160&did=2013D20160 (geraadpleegd 19 april 2016).
'Fraude in de zorg veel groter dan gedacht', RTL Nieuws, 16 mei 2013. http://www.rtlnieuws.nl/nieuws/fraude-de-zorg-veel-groter-dan-gedacht (geraadpleegd 19 april 2016).
'Tijdlijn: waarom aanpak zorgfraude mislukte', RTL Nieuws, 23 mei 2013 http://www.rtlnieuws.nl/nieuws/binnenland/tijdlijn-waarom-aanpak-zorgfraude-mislukte (geraadpleegd 19 april 2016).

16 Debat over Fraudebestrijding in de zorg, Tweede Kamer 28 828 Nr. 40, Nummer 2013D21131, 24 mei 2013 http://www.tweedekamer.nl/kamerstukken/detail?id=2013D21131&did=2013D21131 (geraadpleegd 3 februari 2016).

Verschillende activiteiten kwamen voort uit een Plan van Aanpak:
- oprichting Taskforce Integriteit Zorgsector (TIZ) – zonder rechtspersoon – met als doel verbetering van de preventie, detectie en repressie van zorgfraude;
- aanpalend de oprichting van het Bestuurlijk Overleg Integriteit Zorgsector (later ook: Bestuurlijk Overleg TIZ) om het overleg van de convenantpartners structureel voort te zetten;
- met als doel: preventieve, civiel-, bestuurs-, tucht- en strafrechtelijke aanpak van bedreigingen van de integriteit van de zorgsector. Dit behelst opsporing van fraude met declaraties, fraude in het publieke domein (AWBZ, pgb's) en met belastingen;
- belangrijkste middel: delen van informatie over ernstige zorgfraudes, en ook daartoe benodigde persoonsgegevens. En tevens de mogelijke oprichting van een projectorganisatie en werkgroepen, zoals voor 'specifieke risicoanalyses';
- aanscherping van de afspraken in 2015. Zo wordt expliciet de informatie-uitwisseling als belangrijkste middel genoemd, ook ten behoeve van 'het ontwikkelen van nieuwe werkwijzen of maatregelen die kunnen bijdragen aan de versterking van de integriteit van de zorgsector'.[17]

De Taskforce stichtte in 2013 een Expertisecentrum Zorgfraudebestrijding (EZb), gericht op het verzamelen en verwerken van data om onregelmatigheden en fraude te traceren. Tevens zag een Stuurgroep Intensivering Ketenaanpak Correct Declaratieproces (IKCD) het licht. Ook deze had tot doel onterecht uitbetalen van declaraties tegen te gaan.
Het Plan van Aanpak ging ook uit van het uitwisselen van controlesignalen en versterking van risicomanagement systemen bij partijen in de zorgketen: 'Om te weten waarop het risicobeheer […] zich moet richten dienen aan de hand van betrouwbare data de potentiële risico's in kaart te worden gebracht, die na analyse en weging leiden tot aandachtsgebieden voor versterkte controle.'[18]

In een brief aan de Tweede Kamer enkele dagen daarna motiveerden minister Edith Schippers en staatssecretaris Martin van Rijn van VWS hun maatregelen om de naleving van de wet- en regelgeving, zoals de Zorgverzekeringswet (Zvw), de Algemene Wet Bijzondere Ziektekosten (AWBZ), de Wet Maatschappelijke Onder-

17 Convenant verbetering van bestrijding zorgfraude, ministerie van VWS, maart 2013 http://www.rijksoverheid.nl/documenten-en-publicaties/convenanten/2013/03/07/convenant-verbete ring-van-bestrijding-zorgfraude.html (geraadpleegd 3 februari 2016). 'Convenant houdende afspraken over de samenwerking in het kader van de verbetering van de bestrijding van zorgfraude: Voortzetting Bestuurlijk Overleg Integriteit Zorgsector', 11 maart 2015 https://www.nza.nl/96810/20527/Convenant-verbetering-bestrijding-zorg fraude-2015.pdf (geraadpleegd 3 februari 2016).

18 Plan van aanpak 'Intensiveren Ketenaanpak Correct Declaratieproces', 12 september 2013 https://zoek.officielebekendmakingen.nl/blg-252419.pdf (geraadpleegd 3 februari 2016).

steuning (Wmo) en de Wet Marktordening Gezondheidszorg (WMG) te ondersteunen.
Zo stelden ze onder meer: 'Waar veel geld is en veel indirect wordt gefinancierd, zijn ook mensen die daarvan oneigenlijk willen profiteren. Daarom willen wij een forse extra inzet tegen fraude en oneigenlijk gebruik […] vermoedens bestaan dat het van een substantiële omvang kan zijn.'[19]

De opsporingsfunctie in de zorg werd verstevigd en legde VWS grotendeels bij de Inspectie SZW, die daartoe een budget kreeg voor investeringen in een nieuwe eenheid opsporing van zorgfraude, met name pgb- en declaratiefraude.
Door de intensiveringen in het toezicht van de NZa en de opsporing bij de Inspectie SZW zou ook het Openbaar Ministerie (OM) te maken krijgen met een groeiend aantal fraudezaken, zo was het vermoeden. Het OM kreeg dus vanaf 2015 'intensiveringsgelden' voor capaciteitsuitbreiding voor vervolging van fraude in de zorg. VWS stelde extra geld en menskracht beschikbaar voor opsporing en bestrijding van zorgfraude: voor 2014 5 miljoen en vanaf 2015 10 miljoen euro. Behoud van solidariteit noemden beide bewindslieden wederom als een van de onderliggende doelen. Met dit geld is onder meer de Inspectie SZW versterkt met extra inspecteurs, die zich volledig gingen richten op zorgfraude met de focus op pgb-fraude. Vermoedens van grote omvang van fraude baseren zich op signalen, vooral nieuwsberichten.[20]
Zorgverzekeraars kenden vanaf 2012 al een Kenniscentrum Fraudebeheersing in de Zorg. Ook is vanuit genoemd Convenant vanaf 2013 een Verzamelpunt Zorgfraude actief, dat het Expertisecentrum Zorgfraudebestrijding (EZb) van fraudesignalen ging voorzien.

Bij elkaar ontstond – voor de buitenwereld – een ondoorzichtig web van samenwerkingsverbanden om de omvangrijk geachte zorgfraude te bestrijden. Met weinig effectiviteit. Het commentaar daarop luidde: 'Wij vinden het geen ondoorzichtig web, maar er zijn veel partijen betrokken bij de fraudebestrijding, zoals verzekeraars, de Inspectie voor de Gezondheidszorg (IGZ) en de Nederlandse Zorg-

19 'Schippers en Van Rijn: extra geld en speciale inspecteurs voor aanpak zorgfraude', Nieuwsbericht VWS, 16 september 2013 https://www.rijksoverheid.nl/actueel/nieuws/2013/09/16/schippers-en-van-rijn-extra-geld-en-speciale-inspecteurs-voor-aanpak-zorgfraude (geraadpleegd 20 januari 2016).

20 'Fraudebestrijding in de zorg', Brief van de minister en staatssecretaris van VWS aan de Tweede Kamer, 28 828 nr. 89, 27 maart 2015 http://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2015Z05568&did=2015D11299 (geraadpleegd 20 januari 2016). 'Programmaplan Rechtmatige Zorg- Aanpak van Fouten en Fraude 2015-2018', 27 maart 2015 http://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2015Z05568&did=2015D11299 (geraadpleegd 20 januari 2016).

autoriteit (NZa) als respectievelijk de kwalitatieve inhoudelijke en de economische, bestuursrechtelijke toezichthouder.'[21]
Daarnaast functioneert de strafrechtelijke lijn, met twee opsporingsinstanties, Inspectie SZW en FIOD. 'Dat is extra ingewikkeld. Vandaar ook zo veel plannen en rapportages op dit vlak', zo bevestigt de NZa de indruk van complexiteit. Dit is volgens de NZa inherent aan het Nederlandse systeem of model, dat zich ook op andere domeinen manifesteert:
'Niet één partij heeft de leiding, maar elke partij brengt expertise en bevoegdheden mee. In de zorg is dat extra ingewikkeld, omdat een belangrijk deel van de controle- en bestrijding ligt bij private verzekeraars. Zij moeten optreden, terugvorderen of stoppen met een contract.'[22]

3.2 GEMENGDE RESULTATEN

Miljarden getraceerd

Zorgverzekeraars kenden vanaf 2012 al een Kenniscentrum Fraudebeheersing in de Zorg, dat jaarlijks rapporteert over de fraudemeldingen die het ontvangt. Zo leverde fraudebestrijding door de afzonderlijke zorgverzekeraars in 2013 het volgende op:[23]

- vooraf aan betaling uitgevoerde controles: 2,3 miljard euro;
- totaal achteraf: 356 miljoen euro, waarvan:
  controle betaalde declaraties; 329 miljoen;
- onjuistheden na fraudeonderzoek: 27 miljoen, waarvan
  daadwerkelijk aan fraude vastgesteld: 9 miljoen;
  vermoeden, onvoldoende bewijs: 8 miljoen;
  administratieve fouten: 10 miljoen;
- gemiddeld fraudebedrag: 36.000 euro.

In 2014 was het bedrag aan fraudebestrijding (controle achteraf) aanzienlijk gestegen, maar vooraf aanzienlijk toegenomen:

- vooraf aan betaling uitgevoerde controles: 2 miljard euro;
- totaal achteraf: 449 miljoen euro, waarvan:
  controle betaalde declaraties; 329 miljoen;

---

21 Interview met Daan Molenaar, hoofd toezicht zorgaanbieders, bij de NZa.

22 Idem.

23 'Zorgverzekeraars besparen 356 miljoen euro door controles', nieuwsbericht ZN, 15 juli 2014 https://www.zn.nl/338067458/Nieuwsbericht?newsitemid=2654211 (geraadpleegd 20 januari 2016).
'Fraudecijfers 2013, toelichting persbericht juli 2014', nieuwsbericht ZN, 15 juli 2014 https://assets.zn.nl/p/32768/None/Fraudecijfers%202013%2C%20toelichting%20persbericht%20juli%202014.pdf (geraadpleegd 20 januari 2016).

– onjuistheden na fraudeonderzoek: 53 miljoen, waarvan:
  daadwerkelijk aan fraude vastgesteld: 19 miljoen;
  vermoeden, onvoldoende bewijs: 7,5 miljoen;
  administratieve fouten: 26 miljoen;
– gemiddeld fraudebedrag: 77.000 euro.

Opvallend is de relatief hoge afwijzing van declaraties in de categorieën 'Mondzorg' en 'Hulpmiddelen' vooraf en het zeer hoge percentage van de specialistische zorg in de bestrijding van onjuist geachte declaraties achteraf: 81 procent (van die 449 miljoen euro) tegen een aandeel van 59 procent in het totaal gedeclareerde zorgbedrag (van de 37,7 miljard euro).
Van de daadwerkelijke fraudes vond 70 procent plaats in de AWBZ (nu Wlz), en dan nog voornamelijk in de Geestelijke Gezondheidszorg (GGZ) en met persoonsgebonden budgets (pgb's). Ruim 60 procent van het fraudebedrag betrof pgb-fraude.
Daarvan betrof het weer voor 80 procent onjuistheden van de zorgaanbieder. Van het bedrag van 7,5 miljoen euro van vermoede fraude zonder afdoende bewijs was juist ruim 60 procent gevonden in de GGZ. Het hoge bedrag van de administratieve fouten was voornamelijk op conto van één ziekenhuis te schrijven. Details daarvan ontbreken.
Er is 69 keer een 'verzoek' gedaan om een fraude via het bestuursrecht, strafrecht of tuchtrecht te sanctioneren. Zorgverzekeraars zijn hiermee terughoudend, aangezien de dossiervorming en tijdinvestering omvangrijk zijn.[24]

Totaal gedeclareerd voor de basisverzekering in de Zvw in 2013:
40 miljard euro, met 2,6 miljard euro aan correcties is 6,5 procent.
Totaal gedeclareerd voor de basisverzekering in de Zvw in 2014:
37,7 miljard euro, met bijna 2,5 miljard euro aan correcties is ook 6,5 procent.

Uiteindelijk betalen de burgers deze kosten. Het percentage aan onjuiste declaraties is bijvoorbeeld hoger dan van de premieverschillen tussen ziektekostenverzekeringen waarvoor aan het einde van het jaar zoveel wordt geadverteerd. Deze miljarden en hoge percentages aan niet geaccepteerde zorgdeclaraties druppelden echter niet of nauwelijks door in de algemene media.

24 Rapportage Controle en Fraude 2014, ZN, zonder datum
https://www.zn.nl/336986126/Document?parenttitle=Controle+%26+Fraudebeheersing&parent id=33914880 0&title=Fraudebeheersing&dossierids=33914880 8&folder id=342097936&documentregis trationid=401735681 (Geraadpleegd 19 januari 2016).
Toelichting 'Feiten en cijfers Controle & Fraudebeheersing'
https://www.zn.nl/337149960/Algemene-tekst?generictextid=404750339 (geraadpleegd 19 april 2016).

Zorgverzekeraars Nederland (ZN) verklaart de 'materiële controle' als volgt. De zorgverzekeraar gaat na of:
– de door de zorgverlener in rekening gebrachte prestatie is geleverd ('rechtmatigheid');
– en die geleverde prestatie het meest was aangewezen gezien de gezondheidstoestand van de verzekerde ('doelmatigheid').

Dit kan plaatsgrijpen aan de hand van statistische analyses, steekproeven, enquêtes en eventueel dossiercontroles. Volgens de woordvoerder van ZN speelt analyse van bestanden nog geen rol:
'Ons Kenniscentrum Fraudebeheersing in de Zorg (onderdeel van Zorgverzekeraars Nederland) doet geen data-analyse, simpelweg omdat wij hier (behalve de fraudemeldingen van zorgverzekeraars) geen data hebben. Het Kenniscentrum Fraudebeheersing verzamelt fraudemeldingen van de zorgverzekeraars ten behoeve van de coördinerende rol van ZN richting zorgverzekeraars.'[25]

Weinig fraude vastgesteld

Het bedrag aan fraude bedraagt minder dan 1 procent van het totale bedrag aan onjuiste geachte declaraties. De NZa beaamt dat dit een discutabele verhouding is:
'De presentatie van deze cijfers komt wel ongelukkig. Fraude is een heftige beschuldiging, die niet snel wordt geuit. Dat is een gevolg van de vereiste zorgvuldigheid in het hele, langdurige proces, al snel 1,5 jaar per bestuursrechtelijk onderzoek en wel drie tot soms vier jaar ingeval van strafrechtelijke vervolging.'
Verzekeraars, aldus de NZa, willen hun geld terug en beëindigen eventueel het contract met de zorgverlener. De juridische weg is lang en kostbaar. Alleen flagrante gevallen worden naar het OM doorgeschoven.
'We zien dat er veel fouten worden gemaakt en als er voor een miljoen euro incorrect is gedeclareerd, kunnen we veelal niet achterhalen of er sprake is van de boel bewust flessen. We leggen dan wel een bestuursrechtelijke boete op, maar strafrechtelijke vervolging is dan heel moeilijk.'[26]

Genoemd Verzamelpunt Zorgfraude rapporteerde in juni 2015 over het jaar 2014:
'Er waren in dat jaar "668 unieke signalen" bij het verzamelpunt aangemeld door de verschillende partners, van wie twee derde patiënten.' De grote meerderheid betrof tips over '*upcoding*' en 'spookfacturen'. Dit aantal resulteerde in een kleine tweehonderd afgeronde vooronderzoeken met mogelijk een maatregel. Daarover werd inhoudelijk niet gerapporteerd. Ook betrof dit geen data-analyse, wel gedeelde data in vooronderzoeken.[27]

---

25 Woordvoering ZN, schriftelijke antwoorden 25 januari 2016.
26 Interview met Daan Molenaar van de NZa.
27 Rapportage Verzamelpunt Zorgfraude 2014, NZA, 30 juni 2015 http://www.tweedekamer.nl/kamerstuk ken/detail?id=2015D26263&did=2015D26263

Dit lijken vrij geringe cijfers, in vergelijking met de eerder genoemde jaarlijks tot 6,5 miljard oplopende declaratiecorrecties. 'Dit vinden wij zelf ook weinig, maar we verwachten dat het aantal tips de komende jaren zal toenemen als bij consumenten de bekendheid toeneemt van de mogelijkheid om verdenkingen van incorrect declareren te melden.'[28]

Ook de cijfers over resultaten van de Inspectie SZW vormden geen indicatie van een eclatant succes in bestrijding van zorgfraude. In heel 2013 zijn elf opsporingsonderzoeken en twee ontnemingsonderzoeken met pgb's afgerond en ingeleverd voor strafrechtelijke vervolging.
Het ging bij elkaar om een kleine 5 miljoen euro. Daartoe zijn bijna 25.000 opsporingsuren besteed. Er waren, in samenwerking met de zorgkantoren, NZa, IGZ, Belastingdienst en FIOD zo'n tweehonderd zaken bij de eenheid gemeld, waarvan dus 10 procent met succes is afgerond. Zaken zijn tijdrovend, zo werd gemeld.[29]
Op een totaal van 2,75 miljard aan pgb-toekenningen is dit een gering resultaat. Volgens de Rekenkamer was het speuren naar pgb-fraude zodoende inefficiënt.[30]
De teams voor pgb-fraude en declaratiefraude van de Inspectie SZW gingen samenwerken met de FIOD vanwege de daar aanwezige kennis en expertise. Ook de mogelijke samenhang tussen zorgfraude en andere vormen van fraude, zoals faillissementsfraude of fiscale fraude, speelde hierbij een rol.[31]
Tot verbetering leidde dit echter nauwelijks: in de eerste tien maanden van 2014 rondde de Inspectie SWZ vijf strafrechtelijke onderzoeken en vijf ontnemingsonderzoeken van pgb-fraude af. Er werd verbetering voorzien: 'Doordat de SVB nu op een centraal punt de pgb-bestanden beheert, nemen de mogelijkheden voor analyse en controle van deze bestanden op fraude over de pgb-domeinen heen toe. Fraude kan eerder en beter worden opgespoord en de resultaten kunnen gedeeld worden tussen zorgkantoren, gemeenten en zorgverzekeraars.'
De NZa erkent dat deze fraudebestrijding met twee sporen, via de FIOD en de Inspectie SZW, niet effectief genoeg was: 'We werken uiteraard nauw samen. De samenwerking is niet altijd goed gegaan afgelopen jaren. Dat is nogal een uitdaging.'[32]

---

28 Interview met eerdergenoemde.

29 Signaleringsbrief van de Inspectie SZW gericht aan ministerie van VWS, 7 april 2014 http://www.rijksover heid.nl/documenten-en-publicaties/brieven/2014/04/07/singaleringsbrief-van-de-inspectie-szw.html (laatst geraadpleegd 19 april 2016).

30 Rekenkamer 'Aanpak PGB-fraude: veel maatregelen, nog onvoldoende zicht op effecten' http://verant woordingsonderzoekrekenkamer.nl/2014/vws/bedrijfsvoering/aanpak-pgb-fraude-veel-maatregelen-nog-onvoldoende-zicht-op-effecten (laatst geraadpleegd 19 april 2016).

31 Mededeling regering https://www.rijksoverheid.nl/onderwerpen/fouten-en-fraude-in-de-zorg/inhoud/gerichte-aanpak-over tredingen-bij-declaraties-en-betalingen-in-de-zorg

32 Interview met eerdergenoemde.

Mislukking expertisecentrum

Ook moest de NZa erkennen dat het Expertisecentrum Zorgfraudebestrijding (EZb) als samenwerkingsverband een mislukking werd. Het EZb kreeg een strategische en een operationele functie.

De operationele functie behelsde de centrale aanpak van meervoudige zorgfraudezaken op terreinen waar de grootste risico's liggen, zoals de GGZ en de medisch-specialistische zorg. In de strategische functie speelde intelligence een belangrijke rol bij het verzamelen, verwerken en interpreteren van (digitale) gegevens waarmee (patronen van) fraude in de zorg opgespoord kunnen worden. Deze tak neigde naar grootschalig datagebruik.

Van enig resultaat is echter weinig tot niets vernomen. 'In de vorm van het experiment werkte het niet. Vooral de algemene analyses waren niet goed genoeg om te worden toegepast.' EZb is per eind 2015 opgeheven. Momenteel wordt onder de hoede van VWS overleg gepleegd om een nieuw instituut op te richten om zo de krachten te bundelen in fraudebestrijding. Ook Andersson Elffer Felix (AEF), een adviesbureau voor maatschappelijke vraagstukken, adviseerde om één opsporingsdienst voor de zorg op te richten.

De conclusie luidt dat de bestrijding van onrechtmatige declaraties effect sorteert dankzij inspanningen van de individuele verzekeraars, maar dat het traceren en vervolgen van fraude in de zorg problematisch zijn.

Poging samenwerking verzekeraars

In maart 2015 stuurden de minister en staatssecretaris van VWS de Kamer het programma met plannen 'Rechtmatige Zorg' toe. Daarin stond de opvatting van de NZa, zorgverzekeraars en uitvoerders van de Wet langdurige zorg (Wlz) dat prioriteit noodzakelijk is voor inzet van 'moderne controletechnieken zoals […] datamining'.

Het inzetten van data-analyses, bestands- en systeemvergelijkingen op risicogebieden was voor verbetering vatbaar. Meer fouten en mogelijk bewuste overtredingen zouden daarmee aan het licht komen. De politiek bepleitte dat zorgverzekeraars nauw samenwerken en – waar zinvol en juridisch mogelijk – gebruikmaken van elkaars analyses en resultaten.

Zorgverzekeraars investeerden immers elk apart in controles en aanpak van fraudebeheersing met behulp van eigen data- en ict om (risico's op) onrechtmatigheden te detecteren.

In 2015 verkenden zorgverzekeraars mogelijkheden voor gezamenlijk fraudeonderzoek – inclusief data-uitwisseling en analyse. Eventueel in een gezamenlijke onderzoekseenheid. Ze maken er geen haast mee. In het 'Plan van aanpak fraudebeheersing 2015 – 2017' van ZN staat dat de zorgverzekeraars gaan 'verkennen' of ze met een 'onafhankelijke, gezamenlijke onderzoeksunit' de uitvoering van complex fraudeonderzoek gezamenlijk efficiënter kunnen doen.

Ondertussen beloven ze te overleggen over fenomenen en zorgsoorten die extra aandacht behoeven in de fraudebestrijding, en samen suggesties te doen voor het verbeteren van wet- en regelgeving op grond van fraudesignalen.[33]

In januari 2016 liet ZN op schriftelijke vragen van mij over de uitvoering het volgende weten: 'Onlangs heeft ZN dit plan van aanpak geëvalueerd. Ten aanzien van punt 1 (Thematisch samenwerken in ketens op specifieke fenomenen) is geconstateerd dat dit lastig te stroomlijnen is. Dit punt vervalt daarom. Dat is geen ramp, omdat het ons niet zozeer gaat om data-analyse, maar om risicoanalyse (hoeveel kans is er dat iets plaatsvindt en wat de impact daarvan is).(…)
Voor punt 2 (Onafhankelijke, gezamenlijke onderzoeksunit van zorgverzekeraars) kan dat later aan de orde komen. Eerst wordt nu een pilot voorbereid waarin zorgverzekeraars in fraudeonderzoek meer samenwerken. Bij succes kan data-analyse in definitieve vorm worden uitgewerkt.'[34]
Wel is binnen ZN een proef gestart van het portaal Raadpleging Integriteit Zorgaanbieders (RIZ). Zorgverzekeraars kunnen via het RIZ diverse relevante databronnen (tijdens de pilot AGB, BIG, en Insolventieregister) gelijktijdig raadplegen, waardoor het screenen van zorgaanbieders efficiënter wordt. Vooralsnog blijft data-analyse een zaak van zorgverzekeraars apart.
Details over de proef waren niet beschikbaar. Volgens Capgemini heeft gezamenlijke fraudebestrijding van verzekeraars als Achmea, VGZ, CZ en Menzis geen prioriteit, omdat de kostenverlaging door vermindering van fraude concurrentievoordeel oplevert. Kijken in elkaars keuken ligt niet voor de hand. De kleine verzekeraar DSW, zelf al op streek met pragmatisch opgezette data-analyse voor fraudebestrijding, doet volgens Capgemini pogingen om tot collectieve fraudebestrijding te komen.[35]
De NZa ondernam, onder meer via het EZb, de nodige pogingen om gezamenlijk op te trekken in fraudebestrijding. En ontplooide ook zelfstandig initiatieven; zie onder. Niet helder is waar de grens ligt tussen aanpak van verdenkingen door de NZa en door verzekeraars. Volgens de NZa is dat afhankelijk van de plaats waar het signaal wordt opgepakt. Soms vindt samenwerking plaats tussen NZa en verzekeraars.

Kritiek op de sector

Adviesbureau AEF was in een recente evaluatie van de WMG (marktwet zorg) en NZa kritisch. De nadrukkelijke aandacht voor zorgfraude is volgens AEF met een

33 'Plan van aanpak fraudebeheersing 2015 – 2017', ongedateerd, ZN https://assets.zn.nl/p/32768/None/files/Plan%20van%20aanpak%20fraudebeheersing%202015-2017.pdf (geraadpleegd 19 januari 2016).

34 Rik van Druten, woordvoerder a.i van ZN, 27 januari 2016.

35 Interview Norbert Jansen, adviseur Business Development Fraude and Error, Capgemini Nederland.

bureaucratisering gepaard gegaan. De NZa heeft daarmee meer grip proberen te krijgen op het handelen van de verzekeraars, wat op gespannen voet staat met de beoogde rol van verzekeraars als private spelers.
Of die fraudebestrijding effect sorteert, is volgens AEF niet te duiden, maar de NZa heeft met de nadruk op fraude wel bewustwording bewerkstelligd over onrechtmatig gebruik van zorggelden en controle door verzekeraars.
Blije reacties had dat niet tot gevolg: 'De manier waarop de NZa invulling geeft aan het toezicht kan in het veld op weinig draagvlak rekenen. Er is met name kritiek op de protocollering en de manier waarop de NZa die handhaaft.' Kortom, verzekeraars vinden dat NZa te veel beperkingen oplegt in controlewerk.[36]

3.3 NADRUK OP DATA-ANALYSE

Hoge verwachtingen deskundigen
Fraudebestrijding door individuele verzekeraars werpt wel vruchten af, gezien de genoemde miljardenbedragen. Volgens fraudeadviseurs van Capgemini Nederland lopen de zorgverzekeraars voorop met de patroonherkenning vanuit dataverzamelingen voor fraudebestrijding.
Het risicoprofiel kan per claim worden vastgesteld op grond van data-analyse, zoals vanuit claimgeschiedenis, familie-, demografische - en geografische kenmerken, tekstanalyse en sociale banden zoals die zich online openbaren. De effectiviteit zou kunnen toenemen door meer samenwerking in uitwisseling van methoden en fraudesignalen, maar het eigen belang prevaleert.[37]

In de zorg maken de grootste verzekeraars ook gebruik van de expertise van Deloitte voor data-analyse en fraudedetectie. Deloitte adviseerde om niet langer een ondergrens te hanteren voor bedragen waarbij fraude wordt onderzocht. Niet de hoogte van de claim, maar combinaties van indicatoren in relatie tot een opgebouwd profiel moeten bepalen of er controle op een claim plaatsvindt. Fraude kan ook in kleine bedragen frequent optreden.
Deze fraudeprofielen kunnen naast de geschiedenis van een klant worden gelegd. In de data-analyse van zorgdeclaraties worden patronen vastgesteld: geen tandarts zo bijzonder of geen pgb-aanvraag zo speciaal of er is in het hele grote bestand wel vergelijkingsmateriaal voorhanden. Statistisch gezien is niemand of geen enkele situatie uniek, aldus Deloitte.
Het declareren van 42 getrokken kiezen bij één patiënt valt sowieso op, maar kleinere afwijkingen ook. Als een nota op verscheidene risico-indicatoren afwijkt,

36 Ordening en toezicht in de Zorg – Evaluatie Wet Marktordening Gezondheidszorg en de Nederlandse Zorgautoriteit, Andersson Elffers Felix, in opdracht van het ministerie van VWS, september 2014 https://www.nza.nl/1048076/1048181/Rapport_AEF__Evaluatie_Wet_Marktordening_Gezondheidszorg_ en_de_Nederlandse_Zorgautoriteit.pdf

37 Interview met Norbert Jansen van Capgemini Nederland.

moet de kans op controle toenemen. Deloitte noemt succesratio's tot boven de 90 procent bij het traceren van onregelmatig declaratiegedrag vanuit de analyse van bestanden.
Dit wil zeggen dat van de tien 'hits' die in een risicoanalyse van data naar voren treden als onregelmatig, er bij ten minste negen iets niet in orde is. Los van de oorzaken. De resultaten, zowel de juiste indicaties als onjuist gebleken verdenkingen, moeten 'terug' in het systeem ter verfijning van bestaande indicatoren, zodat de volgende ronde scherper wordt.[38]

Poging tot fraudemonitor

De Twentse hoogleraar Theo de Vries deed een ruwe schatting van de totale fraude met publieke middelen in Nederland van 'minimaal 10 miljard euro per jaar'. Daarvan komt volgens hem maar 2 procent aan het licht.
Hij noemt Big Data-toepassing als een van belangrijkste sleutels naar deze schatkamer. 'De toename in data vraagt om inzet van nieuwe geavanceerde methoden voor *handling* en analyse van data. Met behulp van geavanceerde analyses, zoals neurale netwerken, kunnen inzichten worden verkregen die anders moeilijk te realiseren zijn, bijvoorbeeld voor handhaving of preventie.'
In de Verenigde Staten werd volgens De Vries bijvoorbeeld al in 2012 in één zaak voor 450 miljoen dollar aan zorgfraude ontdekt dankzij analyse van declaraties. Amerikaanse verzekeraars schatten dat 10 procent van de claims (deels) frauduleus zijn, goed voor 30 miljard dollar aan potentiële winst per jaar.
Prof. De Vries is mede initiatiefnemer bij het Dutch Fraud Initiative (DFI) van de Universiteit Twente. De doelen waren:

1. Het ontwikkelen en opzetten van een nationale fraudemonitor, van belang geacht voor een groot aantal beleidsinstanties.
2. Onderzoek en ontwikkeling op het gebied van nieuwe detectie, opsporing en -bestrijdingsmethoden, ten behoeve van zowel publieke als private organisaties.
3. Het verzamelen van kennis op het gebied van fraudebestrijding en deze beschikbaar maken.

DFI bouwde aan mathematische methoden voor analyse van grote databestanden ten behoeve van fraudedetectie met voorspellende variabelen. Onder meer in de opsporing van faillissements- en (zorg)verzekeringsfraude is dit toegepast, aldus De Vries.
Samenwerking begon DFI met KPMG voor een promotieonderzoek naar faillissementsfraude en aan de Utwente vindt onderzoek plaats naar fraudegevoeligheid van verschillende DBC-categorieën met zorgdeclaraties. Beoogde samenwerking

38 Interview met Gerrie Lenting en Johan ten Houten van Deloitte.

met de National Fraud Authority (NFA) in Engeland liep spaak, omdat de Britse regering deze in 2014 opdoekte om meer ministeriële controle terug te nemen. De Fraudemonitor kwam er nog niet. Die is wel eerder vervaardigd over het jaar 2006, maar door de Universiteit Utrecht en op een beperkt terrein.
Een nieuwe Fraudemonitor staat op stapel volgens De Vries, te vervaardigen met budget van de TU Twente. Wel werkte hij mee aan 'scans' van de Stichting Toekomstbeeld der Techniek (STT) om de omvang van fraude en ICT-belang te schatten.
De Vries constateert te weinig gebundelde inspanning van partijen die baat hebben bij de bestrijding van zorgfraude. Hij verwijt dit vooral de NZa. Vanouds zijn de diverse belangen in de Nederlandse zorg volgens hem echter gefragmenteerd.
De Vries: 'Heel eenvoudig kun je 80 tot 90 procent ontdekken, want verzekeraars hebben uitstekende dataverzamelingen. De zorg als geheel zou een technology assessment moeten doen om de mogelijkheden van data-analyse goed in beeld te krijgen.' Een gezamenlijk expertisecentrum voor data-analyse zou belangrijke resultaten kunnen boeken, aldus De Vries, zelf voorheen werkzaam op leidende posities in de zorg.
Zo zou de zorg de nog schaarse deskundigheid in Big Data volgens De Vries in een gezamenlijk inspanning moeten aantrekken. 'Er zijn veel te weinig topdeskundigen, en die kiezen het eerst voor het bedrijfsleven. Je moet die mensen goed belonen en goede perspectieven bieden in de zorg. Hun werk is goud waard.'
Anderzijds toonde De Vries zich bevreesd dat de groei in koppelingen van bestanden ten koste gaat van privacy. Volgens De Vries is de organisatie van een periodieke technologie-inventarisatie door de Autoriteit Persoonsgegevens noodzakelijk om meer inzicht te krijgen in de dilemma's van de voordelen van voortschrijdende mogelijkheden voor datatoepassingen versus de risico's voor de privacy van individuen. 'Maar de AP is sterk juridisch georiënteerd, en te weinig op technologie.'[39]

---

39 'Wat doen we met de overvloed van data?', presentatie van prof. dr. ir. Theo de Vries, tijdens het seminar 'Fraude en criminaliteit bestrijden met basisregistraties' http://www.digitaleoverheid.nl/images/stories/stip/2013%200122%20presentatie%20fraudeseminar%20theo%20de%20vries%202.pdf (geraadpleegd 20 januari 2016).
Nieuwsbericht idem: http://www.digitaleoverheid.nl/onderwerpen/stelselinformatiepunt/stelsel-van-basisregistraties/1853-presentatie-theo-de-vries
Dutch Fraud Initiative (DFI), Universiteit Twente https://www.utwente.nl/igs/dfi/DFI/ (geraadpleegd 22 januari 2016).
Fraude monitor rapportage 2006, Universiteit Utrecht, Departement Methoden en Technieken http://docplayer.nl/6297616-Fraudemonitor-rapportage.html (geraadpleegd 22 januari 2016).
'Fraude Loont… nog steeds', Redactie Alex van Geldrop en Theo de Vries, 2015, Stichting Toekomstbeeld der Techniek (STT) http://stt.nl/publicatie/quick-scan-fraude-loont-nog-steeds/

Data-analysedeclaratieberg NZa

De NZa heeft zich – ondanks de kritiek van prof. De Vries – wel intensief met bestrijding van zorgfraude ingelaten. Zo is onderzoek gedaan door het Fraude Detectie Expertise Centrum (FDEC), in samenwerking met de Universiteit Leiden. Dat specialiseert zich in datamining en datastream mining, respectievelijk vissen in databestanden en in datastromen.
De NZa vroeg in 2013 aan het FDEC om met behulp van datamining onregelmatigheden in declaratiebestanden op te sporen. Voor de analyse eind 2013 zijn 880 miljoen records van declaraties van huisartsen, 190 miljoen van mondzorg, 620 miljoen van farmacie en 4 miljoen van GGZ gebruikt vanuit de Vektis-databanken. Totaal 1,7 miljard gegevens, die dankzij toegenomen computerkracht en nieuwe analysemodellen nu 'te kraken' waren. Met behulp van datamining zijn onregelmatigheden opgespoord in declaratiebestanden.
Dit was de eerste keer dat een dergelijk grote hoeveelheid declaraties in de gezondheidszorg in Nederland bij elkaar zijn gebracht om 'merkwaardige' transacties op te sporen. Een simpel voorbeeld: huisartsen die vijf kwartalen per jaar de patiëntvergoeding declareren. Dat wil nog niet zeggen dat het fraude is, het kan een menselijke of een systeemfout zijn.

Het detecteren van anomalieën met een breed scala van moderne technieken was ook volgens het FDEC goed mogelijk met de Big Data-exercitie. Deze leverde direct identificeerbare behandelaars en indieners op en het mogelijk te veel betaalde bedrag was eenvoudig te berekenen en relatief zeker. Erg onwaarschijnlijke cases werden snel zichtbaar.
Om het totale bedrag dat gemoeid was met overtredingen van declaratieregels en de anomalieën te bepalen, heeft het FDEC conservatief voor het 99 procent-referentiepunt gekozen om anomalieën en te veel vergoede bedragen door overtreding van declaratieregels bloot te leggen. Voor 2010 is geconcludeerd dat het overtreden van declaratieregels leidde tot een te veel vergoed bedrag van bijna 28 miljoen euro en anomalieën van 7 miljoen: een totaal van 35 miljoen euro.
Voor 2011 kwam dat op bijna 39 miljoen, in dezelfde verhouding. Percentages van discutabele declaraties varieerden van 0,8 bij huisartsen tot 0,1 procent voor de GGZ.[40]

Data-analyse AWBZ

De NZa vroeg verder aan het FDEC om declaraties inzake de Algemene Wet Bijzondere Ziektekosten (AWBZ) te onderzoeken, te weten de Zorg in Natura (ZIN) en het

40 'Onregelmatigheden in declaratiebestanden bij huisartsen, mondzorg, farmacie, GGZ, paramedische zorg en medisch specialistische zorg', Prof. dr. H.M.P. Kersten, Dr. W.J. Kowalczyk en F. Kleyn, FDEC, 8 augustus 2014
https://www.nza.nl/regelgeving/bijlagen/Eindrapport_Onregelmatigheden_in_declaratiebestanden_in_zes_zorgsegmenten_FDEC (geraadpleegd 23 januari 2016).

pgb. Voor het pgb worden veel minder gegevens vastgelegd in systemen, dus is detectie van fraude niet eenvoudig, terwijl juist het pbg fraudegevoelig is volgens de onderzoekers. In sommige gevallen wordt er geen zorg ingekocht of er wordt te weinig zorg ingekocht.
Dit volgende FDEC-onderzoek[41] richtte zich specifiek op de declaratiebestanden waardoor over de zorginkoop bij pbg geen uitspraken gedaan konden worden, louter over Zorg in Natura. Van het CAK en CIZ zijn 29 miljoen declaratierecords over 2012 en deels over 2013 geanalyseerd.
Voor het pbg ontbraken alle gegevens over 2013. Louter goedgekeurde declaraties telden mee, niet de door zorgkantoren reeds afgewezen declaraties. Data waren te beperkt en moeten completer zijn om een goed beeld van onregelmatigheden op te stellen, aldus de onderzoekers. Ze splitsten hun bevindingen in:

1. overtredingen van declaratie- en registratieregels, het gaat hier om harde controles en harde uitkomsten;
2. afwijkingen van wat verwacht mag worden rekening houdend met het declaratiegedrag van andere zorgaanbieders (anomaliedetectie).

Het 'te veel gedeclareerde bedrag' bij de AWBZ-controle hoeft niet daadwerkelijk te zijn uitbetaald. Het aandeel overproductie (in 2012: circa 60 miljoen euro) ten opzichte van het totaal gedeclareerde zorg is relatief klein, circa 20 procent van het totaal te veel gedeclareerde bedrag dat uit deze Big Data-analyse naar voren kwam. Voor ZIN is in 2012 voor circa 300 miljoen euro te veel gedeclareerd op een totaal van ruim 20 miljard euro facturen. In 2013 voor circa 90 miljoen euro op 18,7 miljard omzet. Het lagere bedrag in 2013 kan voor
een groot deel worden verklaard door gebrekkig voorhanden zijnde data.
Het totaal aan te veel gedeclareerde bedragen voor pbg kwam voor 2012 op circa 42 miljoen. De meest voorkomende overtredingen waren het overschrijden van maximum beleidsregelwaarden, niet-valide combinaties van zorg en meer zorgfactureren dan geïndiceerd. Deze uitkomsten vragen om nadere bestudering door domeindeskundigen, vinden de onderzoekers. Data-analyse levert direct identificeerbare zorgaanbieders op. Het te veel gedeclareerde bedrag kan worden berekend en is relatief hard.
Het rapport laat – mede vanwege privacyoverwegingen – niet zien hoeveel en welke zorgaanbieders bij dit onderzoek zijn betrapt. Deze informatie is wel aan de NZa beschikbaar gesteld. Moedwil is niet altijd de oorzaak, maar moeilijk te onderscheiden: 'We hebben waargenomen dat vaak fouten worden gemaakt met de tijdseenheden van declaraties: daar waar in uren gedeclareerd moet worden, vult

41 'Onderzoek naar onregelmatigheden in databestanden van de Zorg in Natura (ZIN) en het persoonsgebonden budget (door FDEC) ',dr. H.M.P. Kersten, Dr. W.J. Kowalczyk e.a., 14 september 2014 https://www.nza.nl/1048076/1048155/Onderzoek_naar_onregelmatigheden_in_databestanden_van_de_ Zorg_in_Natura_ZIN_en_het_persoonsgebonde.pdf

men minuten is. Dit leidt natuurlijk – zonder juiste controle en alerte medewerkers – tot een veel te hoog gedeclareerd bedrag.'[42]

Data-analyse GGZ-declaraties

Vervolgens heeft de NZa zelf aanvullend onderzoek gedaan om meer details te kunnen analyseren over GGZ-declaraties.[43] Het DBC-informatiesysteem (DIS) biedt declaratiegegevens van aanbieders van geestelijke gezondheidszorg, inclusief de daadwerkelijk bestede tijd (althans, de door aanbieders ingevulde tijd, de werkelijke tijd is niet controleerbaar vanuit een systeem).
De NZa heeft op deze DIS-data een aantal toetsen uitgevoerd. Als eerste is de kwaliteit van gegevens gecontroleerd. Zo kwam naar voren van welke geregistreerde behandelingen of activiteiten het aantal geregistreerde minuten groter was dan verwacht mag worden. Dit betreft wellicht administratieve fouten die zijn niet meegenomen in de analyse van afwijkingen. Vervolgens zijn vier toetsen uitgevoerd:

1. Hoe vaak komt het voor dat de totale hoeveelheid tijd die een zorgaanbieder besteedt op een waarde uitkomt die financieel voordelig is? Immers, zodra een zorgaanbieder 800 minuten heeft besteed, levert een extra behandeling financieel niets op, maar leidt dit wel tot kosten. De NZa bekeek hoeveel procent van de DBC's van een zorgaanbieder 800 tot 900 minuten geregistreerde bestede tijd bevatten om in kaart te brengen of er zorgaanbieders zijn die zich hierdoor laten leiden.
2. In hoeverre geven aanbieders patiënten die in 2011 onder behandeling waren met de diagnose 'aanpassingsstoornis', vanaf 2012 een andere behandelcode? Immers, de 'aanpassingsstoornis' behoorde niet langer tot het verzekerde pakket. De NZa constateerde dat het aantal patiënten met deze diagnose in 2012 sterk terugliep.
3. Verder een 'anomaliedetectie' op de totale tijd die zorgaanbieders hebben besteed aan patiënten per dag; hoeveel kan er bespaard worden als de meest extreme gevallen op een lager niveau uitkomen. 'Op basis van deze analyse hebben we vastgesteld dat voor 2011 54,6 miljoen euro en in 2012 voor 50,8 miljoen euro te veel is uitbetaald.'
4. Hoe vaak komt het voor dat er voor één patiënt op één datum meer dan één deelprestatie 'verblijf' is geregistreerd, terwijl hij per dag maar op één afdeling tegelijk kan verblijven? Dit leverde onterechte dubbele vergoedingen op voor een totaal van 155 miljoen euro.

Dit rapport biedt inzicht in de mogelijkheden van fraudedetectie met behulp van grote databestanden. Het gaat hier overigens nog om vrij basale en voor de hand

42 Idem.

43 Tijdschrijven verblijfsdagen en diagnoses in GGZ, NZA, 12 december 2014 https://www.nza.nl/publicaties/1048188/Tijdschrijven_verblijfsdagen_en_diagnoses_in_GGZ

liggende indicatoren. Naar verwachting spelen zorgaanbieders daar ook op in. In bepaalde opzichten is het ook bijna hilarisch: een dag telt 1440 minuten. Maar bij één aanbieder kwam NZa tot registraties van gemiddeld 2174 minuten per dag per patiënt. Dat is 36 uur en 13 minuten. Dit gemiddelde was ook nog eens gebaseerd op 2490 waarnemingen. Het declaratiesysteem kan op hol geslagen zijn of de patiënt kan er geestelijk buitengewoon ernstig aan toe zijn. Maar het ook zijn dat de behandelaar in kwestie ernstig de weg is kwijtgeraakt.

De vraag is wat er concreet gedaan is met de resultaten van deze onderzoeken. Volgens de NZa waren ze allereerst bedoeld om de verzekeraars te prikkelen om meer onderzoek te doen, gestimuleerd door de minister van VWS. De minister wilde ook de omvang van de zorgfraude weten. Dat kwam er niet van.
Immers, in vergelijking tot veel andere studies, die percentages van 3 tot 12 procent rapporteerden aan fraude met zorgbudgetten, waren de percentages van de FDEC/NZa-onderzoeken vanuit data-analyse veel lager. 'We haalden er dus lang niet alles uit met data-analyse. Een heleboel geavanceerde manieren van frauderen bleven kennelijk onder de radar met deze uitvoering van de data-analyse.'
Dit heeft invloed op de pretenties van fraudeonderzoek aan de hand van data-analyse. Ofschoon vooral de indicatoren en de wisselwerking met daadwerkelijke controles (steekproeven) tot de hogere 'pakkans' moeten
leiden. 'In de pgb-wereld wordt de omvang van fraude groot geacht, maar exact is dat niet vast te stellen, want niemand wil uitgebreide intensieve controle op alle uitkeringen. Toch wil iedereen dat er zinnig en zuinig met zorggeld wordt omgegaan, dus wil je wel een voldoende niveau van controle.'[44]

Megabestanden declaraties voorhanden

De NZa kon voor deze analyse een beroep doen op de declaraties van alle verzekeraars die via Vektis van zorgverleners komen. Vektis publiceert in samenwerking met de ZN vanaf 2014 de Vektis Dataset Zorgverzekeringswet, open data ten behoeve van studie met in eerste instantie het databestand Zorgverzekeringswet 2012, gevolgd door 2013. Dit geeft inzicht in de betaalde kosten van alle zorgsoorten. Deze open data voor analyse moeten andere partijen aantrekken die kennis en inzicht voor data-analyse helpen genereren, met als uiteindelijk doel de betaalbaar-

44 Interview met Daan Molenaar van NZa.

heid en de kwaliteit van zorg te verbeteren. Zo zijn er data op postcode (drie cijfers) en per gemeente voorhanden.[45]
Vektis wil ook zelf een rol spelen in de aanpak van zorgfraude met analyses, als 'het informatiecentrum voor zorgverzekeraars', dat de miljarden data van alle passerende zorgdeclaraties niet enkel doorsluist, maar ook bundelt en analyseert. Vektis kocht daartoe via leveranciers als Imtech ICT, Axians- en IBM-systemen waarmee volgens Vektis de data-analyses worden versneld met een factor tien tot honderd. Dat genereert ook fraudesignalen als onderdeel van trendanalyses. De analyse is beperkt door bescherming van privacy en vanwege concurrentiegevoeligheid. Vektis bundelt geen data op persoonsniveau en de specifieke gegevens van individuele zorgverzekeraars worden afgeschermd.[46]

Er treedt een spanningsveld op. Vektis beschikt weliswaar over alle data, maar verzekeraars vinden analyse op dit niveau niet wenselijk. Volgens Achmea schieten de mogelijkheden voor Vektis te kort om patronen te duiden. NZa is het hiermee niet eens: 'Vektis heeft het grootste bestand aan data van declaraties en behandelingen. Verzekeraars kunnen door Vektis analyses op de eigen bestanden laten uitvoeren. Vektis kan dat zelf over bestanden van verschillende verzekeraars doen. Of een derde partij, zoals het FDEC in Leiden dat voor ons deed.'[47]

Case: Achmea

Met een vraaggesprek is inzicht verkregen in data-analyse van Achmea, de grootste zorgverzekeraar.[48] Ze besteedt toenemende aandacht aan fraudebestrijding door tientallen miljoenen declaraties op afwijkende sporen te analyseren.
In 2011 heeft Achmea een Kenniscentrum voor onderzoek en toepassing van haar databank opgericht. Intern werken er nu zo'n zestig personen bij het centrum, dat input levert aan andere afdelingen voor verbetering van dienstverlening en verlaging van kosten.
Het Achmea Kenniscentrum doet zowel zorginhoudelijk gericht onderzoek met data-analyse om zorginkoop en -verlening te verbeteren, als marktgericht onder-

45 'Data-analyse speelt belangrijke rol bij aanpak zorgfraude', nieuwsbericht Vektis, ongedateerd http://www.vektis.nl/index.php/nieuws/onderzoeken/373-data-analyse-speelt-belangrijke-rol-bij-aanpak-zorg fraude (geraadpleegd 21 januari 2016).
'Eerste stap publicatie Open Data', nieuwbericht Vektis, 4 november 2014 http://www.vektis.nl/index.php/nieuws/algemeen-nieuws/513-eerste-stap-publicatie-open-data (geraadpleegd 21 januari 2016).
Vektis Open Data Databestand Zorgverzekeringswet http://www.vektis.nl/index.php/vektis-open-data (geraadpleegd 21 januari 2016).

46 'Referentie Vektis', Imtech ICT Performance Solutions, ongedateerd http://cdn2.hubspot.net/hub/227033/file-692312180-pdf/docs/Referentie_Big_Data-Vektis-Imtech_ICT.pdf (geraadpleegd 16 juni 2015).

47 Interview met Daan Molenaar van de NZa.

48 Interview met Barry Egberts en Rob Konijn van Achmea.

zoek om de concurrentiepositie te verstevigen. De scheiding tussen beide is niet altijd absoluut. Vanuit de data wordt gezocht naar opvallende relevante correlaties, zowel bewust als met serendipiteit.
Alleen al 13 miljard euro aan zorgdeclaraties verwerkt Achmea/Zilveren Kruis per jaar, de belangrijkste basis voor de datamining vanuit de SAS-software voor databewerking en -analyse. De onderliggende Achmea Health Database wordt steeds vaker door derden gevraagd voor wetenschappelijk onderzoek, voornamelijk om wetenschappelijke redenen.
Toegang tot de bestanden worden geleverd na anonimisering en overige contractafspraken. Uit de data kunnen vele patronen van de zorg naar voren treden, zoals de geestelijke gezondheid per wijk, gemeente of instelling. Geaggregeerde data zijn belangrijk om trends en beelden vast te stellen.

Resultaten
Achmea hanteert twee categorieën:
1. formele controle: toetsing aan wet en polissen;
2. materiële controle: afwijkingen van normaal declaratiegedrag in beeld brengen, met behulp van onder meer data-analyse.

De materiële controles (achteraf) leveren op jaarbasis tussen de 40 en 45 miljoen euro op (2014). Ook Achmea neemt het woord fraude bij voorkeur niet in de mond, omdat zowel de vermeende opzet als strafrechtelijke implicaties een gedegen, verregaande bewijsvoering vereisen.
Zo blijft de categorie 'bewezen fraude' bij Achmea door deze benadering beperkt in omvang: een kleine 6 miljoen euro in 2014, relatief gering op 13 miljard aan verwerkte zorgdeclaraties. De meeste gevallen van onjuist declareren komen nog altijd aan het licht door tips, zeker waar patiënten zelf de facturen inzien en afwijkingen vaststellen in vergelijking met ondergane behandelingen. Patroonanalyse uit dataherkenning neemt toe, ook in combinatie met deze tips. Voorbeelden van onjuist declareren dat is getraceerd met, of ondersteund door, data-analyse volgens genoemde woordvoerders:
– Eerder is gepubliceerd over een casus zorgfacturering binnen een plastisch-chirurgische groep. Verbanden tussen daadwerkelijke zorg en declaraties zijn onderzocht. Van de ruim 30.000 behandelingen waren er duizend niet afgesloten en toch gedeclareerd. Vaak ontbrak de formele afsluiting, maar ook waren er tekenen van fraude.
– Op het raakvlak van tandverzorging en kaakchirurgie vallen vanuit de data-analyse steeds meer onregelmatigheden op. Tandzorg valt vaak onder de aanvullende verzekering zonder eigen risico, kaakchirurgische behandelcodes vallen onder het eigen risico. Artsen gaan daarmee soms in de fout.
– Behandelingen die in één reeks vallen, worden 'geknipt' in verschillende behandelingen over verschillende dagen teneinde de omzet te maximaliseren.

Vooral in enkele veelvoorkomende behandelreeksen van fysiotherapeuten zijn dit soort patronen onderkend, vanuit totaal honderden meldingen.
- Met de verhoging van het eigen risico worden ook meer behandelingen of verstrekking van medicijnen onderhevig aan antedatering bij declareren; overhevelen naar een vorig jaar waarin het eigen risico al verbruikt was, of juist naar een volgend jaar waarin meer kans is op het opsouperen van het eigen risico; ook het juist in of uit de basisverzekering halen van – zoals van de anticonceptiepil – levert opvallende grafieken op over de behoefte aan anticonceptie in Nederland.
- ID-fraude, zorg ontvangen op het pasje van een ander is een grote categorie. Ook buitenlandse familie en kennissen kunnen hiervan gebruik maken. Data-analyse van buitengewone combinaties van kwalen levert verdenkingen op. Die vervolgens wel moeilijk hard te maken zijn.
- Het voorschrijven van medische fitness is een bij patiënten vaak gewilde methode. Patroonherkenning kan aan het licht brengen of bepaalde zorgverleners hiervoor vatbaar zijn.
- De eerder met veel publiciteit omgeven *upcoding* komt nog veelvuldig voor. Met het terugbrengen van het aantal behandelcodes van circa 30.000 naar circa 3000 is de uitdaging geringer, maar het is nog steeds een veelvoorkomende categorie fouten, al dan niet opzettelijk gemaakt.
- Het voorschrijven van opiaten is vanouds fraudegevoelig. Snuivende zorgverleners of cliënten zijn via data-analyse soms op te sporen.
- Verkeerde bankrekeningnummers komen aan het licht, vaak per abuis ingevuld. Gebruik van bankrekeningen van familieleden voor betalingen door zorgverleners kan duiden op een verkeerde bedoeling.
- Te veel nullen in declaratiebedragen of andere 'typefouten' blijken meer voor te komen dan gedacht en er ook vaak doorheen te glippen. Data-analyse bracht dit aan het licht. Zoals een declaratie van 30.000 euro die 300 euro had moeten bedragen (jammer van het extra vakantiegeld).

3.4 TOEKOMST: SPANNING MET MEDISCHE PRIVACY

Rapportage 'succes'

Eind oktober 2015 zijn over Programmaplan Rechtmatige Zorg en Aanpak van Fouten en Fraude 2015-2018 resultaten bekendgemaakt. Deze is echter door het ministerie van VWS zelf geproduceerd en het plan spreekt in vrijwel louter positieve termen over successen van de 'integrale aanpak' op alle terreinen en thema's. Hoe 'integraal' de aanpak van fraude feitelijk is in de praktijk, en op welke manieren het containerbegrip 'integrale aanpak' bijdraagt aan eventuele successen, komt in de verantwoording niet tot uiting.

Wel maakt het rapport uitgebreid melding van de activiteiten van de NZa, die op basis van declaratie- en registratiegegevens data-analyses uitvoert. Ook de nodige tekortkomingen voor de uitbreiding van het gebruik van datamining en het

analyseren van declaratiebestanden worden benoemd. Alsmede de noodzakelijke 'intensivering van onderlinge samenwerking' – wat erop duidt dat de gewenste ideale 'integrale aanpak' nog niet is gerealiseerd.[49]

Toezicht 2.0

De wetenschappelijk onderzoekers van FDEC zien de noodzakelijke innovatie als volgt:

- Toezicht 1.0: toezien op ordentelijke administratieve organisatie, procedures, integriteit, ethiek, deskundigheid, et cetera.
- Toezicht 2.0: in het digitale declaratieverkeer wordt steeds diepgaander data-analyse toegepast. Domein- en expertkennis op het terrein van de zorg wordt gecombineerd met vindingrijkheid van onderzoekers en de rekenkracht van computers om te komen tot anomalieën.

De Vektis-bestanden vinden ze echter onvoldoende toegespitst op analyse om fraude op te sporen.
Zo maken de reeds door zorgverzekeraars geweigerde declaraties er geen deel van uit. Er is in de onderzoeken voor de NZa louter een schatting gegeven van de omvang (frequentie en bedragen) van de onregelmatigheden. Er moet volgens de onderzoekers van FDEC ernstig rekening worden gehouden met vooral *false negatives* (het is mis, maar het alarm gaat niet af), maar ook met de *false positives* (vals alarm).
Om vast te stellen of merkwaardige cases daadwerkelijk frauduleus zijn, vindt het FDEC nader dossieronderzoek noodzakelijk. Dat geldt ook voor de vergelijking met informatie over de werkelijk verleende zorg (zie onder). Ook wijzen ze op het ontstaan van kat-en-muisspel tussen fraudeurs en speurders in data-analyse. Fraudeurs kunnen zich terugtrekken in het niet te controleren gebied achter het 'scherm van de privacy', aldus de FDEC-onderzoekers.
'Het is overduidelijk dat de behandelaar/indiener meer op zijn hoede is. Dat daardoor de anomalieën kunnen verschuiven naar andere behandelingen/verrichtingen/medicijnen is een fact of life. Hiermee is de wedloop tussen overtreders en zij die de detectie doen, geschetst.'

Voor vervolgstappen adviseert FDEC dringend om in het databestand op te nemen: het rekeningnummer van de begunstigde en zijn geboortedag en -maand. Ook de complete postcodes zijn nodig, bijvoorbeeld om de vergoeding per wijk te kunnen beoordelen. Aggregatie van alle bestanden naar verzekerden (via het encrypte BSN) is een slag die de onderzoekers willen maken om een compleet beeld van de behandelingen en kosten per verzekerde. Om na te gaan of zorg conform factuur is gele-

49 Voortgang programma Rechtmatige Zorg 2015, minister van VWS, 29 oktober 2015 http://www.tweede kamer.nl/kamerstukken/detail?id=2015D41067&did=2015D41067 (geraadpleegd 20 januari 2016).

verd, moeten, aldus onderzoekers, verder onderzoek van databestanden, materiële controles en audits uitkomst bieden.
Ze pleiten echter niet voor grootschalige materiële controle en audits, maar selectief bij sterke fraudesignalen en merkwaardige gevallen. De administratieve problemen zijn zowel hinderlijk als behulpzaam. 'Het percentage correctierecords is hoog. Dat wijst niet alleen op een administratief proces dat beter kan, maar het bemoeilijkt ook het opsporen van onregelmatigheden. Het goede nieuws daarbij is dat die zorgaanbieders die veel correctieboekingen indienen als vanzelf de aandacht op zich vestigen.'[50]

NZa: topje van de ijsberg

De NZa is positief over datamining als methode om mogelijke overtredingen en aanbieders die afwijken van het gemiddelde op te sporen. Met de uitkomsten van de data-analyses kunnen verzekeraars hun controles verbeteren. Ook zal de NZa de data-analyse gebruiken voor prioritering in eigen toezicht.
De NZa stelt echter vast dat er nog veel onzekerheden zijn met data-analyse. Zo wordt gekeken naar afwijkingen van het gemiddelde, terwijl wellicht dat gemiddelde al te hoog is. Bovendien glippen er nog vele gevallen doorheen die aandacht waard waren, de 'false positives'. Anderzijds is bij als onregelmatig geselecteerde declaraties op voorhand niet duidelijk of een aanbieder bewust onrechtmatig declareert.
Dit zijn mede redenen dat de NZa zich niet heeft gewaagd aan het produceren van een 'zorgfraudecijfer' (percentaqe), zoals haar was verzocht van verschillende kanten. 'We zien slechts het topje van de ijsberg, want we zien maar een deel van de foute declaraties. Het is niet mogelijk om de uitkomsten van onze analyse op een verantwoorde en betrouwbare wijze door te rekenen naar een totaalcijfer voor zorgfraude.'[51]
Dit brengt de NZa tot de overtuiging een veel beter inzicht in de omvang van de fraude in zorg mogelijk wordt met toepassing van meer steekproeven. Die zouden ook de deur openen naar opsporing van een van de belangrijkste frauderisico's: spookzorg, het in rekening brengen van zorg die niet is geleverd.
Spookzorg is niet op te sporen via de beschreven data-analyse, die immers uitgaat van daadwerkelijk geleverde zorg conform de declaratie. Een gefingeerde aanbieder die keurig een gemiddeld declaratiepatroon aanhoudt, valt niet op. De kans op opsporing is groter met steekproeven, inclusief onderzoek van medische dossiers.

---

50 'Onregelmatigheden in declaratiebestanden bij huisartsen, mondzorg, farmacie, GGZ, paramedische zorg en medisch specialistische zorg', Prof. dr. H.M.P. Kersten, Dr. W.J. Kowalczyk en F. Kleyn, FDEC, 8 augustus 2014
https://www.nza.nl/regelgeving/bijlagen/Eindrapport_Onregelmatigheden_in_declaratiebestanden_ in_zes_zorgsegmenten_FDEC (geraadpleegd 23 januari 2016).

51 Interview met Daan Molenaar van de NZa.

Privacy en medisch beroepsgeheim

Teneinde veel beter zicht te krijgen op de ruimte tussen behandelingen en declaraties zouden verzekeraars als Achmea baat hebben bij inzage in medische dossiers. Dit is in het kader van de privacy een nogal ingrijpende actie en mag daar om alleen gedaan worden bij sterk vermoedens van onregelmatigheden.[52]

Op dit moment mogen verzekeraars alleen patiëntendossiers onderzoeken als er een signaal is dat dit onderzoek rechtvaardigt. Bij materiële en formele controles geldt ook dat in de regel eerst algemene controles moeten worden uitgevoerd voordat er detailcontroles gedaan mogen worden. Verzekeraars zouden volgens de NZa echter effectiever kunnen zijn, als ze bij een standaardcontrole een steekproef nemen uit patiëntendossiers. Zo sporen zij eerder (vermoede en onvermoede) fraude en frauderisico's op en kunnen zij hun controletaak beter uitvoeren.

Behalve op privacy (van patiënten) stuit het uitbreiden met inzage in medische dossiers ook op het medisch beroepsgeheim. Die mogen volgens de NZa niet ter discussie staan.

Echter, bescherming van beide rechten betekent een aderlating voor de opsporing van onterechte en te hoge declaraties. De NZa kwam dus met de aanbeveling aan de wetgever om opnieuw een afweging te maken tussen het verruimen van controleopties voor zorgverzekeraars met een mogelijk verhoogd risico op schending van privacy en beroepsgeheim.[53]

Ruimere regels gevraagd

De NZa vroeg het ministerie van VWS om een verkenning of het mogelijk en wenselijk is om de regelgeving te verruimen zodat zorgverzekeraars steekproeven kunnen uitvoeren op willekeurige declaraties, zonder dat er sprake is van het vermoeden van onregelmatigheden.

Na overleg met de NZa, ZN en zorgverzekeraars is vastgesteld dat het wettelijk mogelijk maken van steekproeven weinig toevoegt aan bestaande methoden van opsporing van fraude. Zorgverzekeraars zeiden dat steekproeven zonder vermoeden niet nodig zijn. Ze kunnen een vermoeden formuleren en op grond daarvan de (big) data-analyse uitvoeren op declaratiegedrag.

Bovendien is het gezien privacyregels en medisch beroepsgeheim ondenkbaar dat er inzage komt in het medisch dossier teneinde vermoedens van fraude te checken. Declaraties verschaffen al informatie over medische handelingen.

'Gezien het gebrek aan noodzaak voor het instrument druist dit in tegen de waarborgen van proportionaliteit en subsidiariteit, die in wet- en regelgeving zijn neer-

52 Interview met Barry Egberts en Rob Konijn van Achmea.

53 'Samenvattend rapport 'Onderzoek naar kwetsbaarheden en financiële onregelmatigheden in de zorg', NZA, november 2014 https://www.nza.nl/104107/138040/2__Samenv_rapp_Onderzoek_naar_kwets baarheden_en_financi_le_onregelmatigheden_in_de_zorg.pdf (geraadpleegd 22 januari 2016).

gelegd met betrekking tot de controle door zorgverzekeraars […] Er zijn nog voldoende verbetermogelijkheden, waar zorgverzekeraars volop mee bezig zijn.'[54] Oftewel: het aantasten van de medische privacy van zorgverleners en patiënten gaat te ver gezien het doel van de fraudebestrijding. De minister van VWS acht het onhaalbaar om te toornen aan het medisch beroepsgeheim, dus zijn steekproeven in medische data in de fraudestrijding een no-go area.

De NZa had anders geadviseerd en reageert: 'Steekproeven zijn nodig om verder te kunnen gaan dan met de protocollen voor gebruik van medische gegevens mogelijk is. Hoe kom je er immers achter wat er mis is? De Belastingdienst doet dat ook.'[55]

Hulp van patiënten

De NZa vindt het afwijzen van steekproeven met inzage in medische gegevens wellicht politiek realistisch gezien de te verwachten weerstand van belangengroepen, maar maatschappelijk geenszins: 'In Nederland is de discussie veel feller dan in andere landen. Vooral de zorgaanbieders maken zich er zo druk om. Het is meer een norm ter bescherming van de aanbieders, terwijl mijns inziens de discussie en norm zouden moeten gaan over de privacy van de patiënt.'[56]

Zo ontvangt de NZa de nodige tips van patiënten over verdenkingen van te veel declareren, bijvoorbeeld van niet-ondergane behandelingen of door namen van artsen die niet gezien zijn.

'In onderzoek krijgen we alle medewerking, inclusief inzage in de medische informatie. Vervolgens beroept de zorgaanbieder zich op het medisch beroepsgeheim om controle tegen te houden. Dat vinden wij een rare verwording van het recht op medisch beroepsgeheim. Het gaat toch om de bescherming van de patiënt.'

Overigens kan hier de data-analyse in de declaratiebestanden wel soelaas bieden. Dat trad naar voren met de zorgfraude die snel 'oorsmeer-gate' ging heten: in het ZorgSaam-ziekenhuis in Terneuzen bracht een KNO-arts 1066 euro in rekening voor een paar minuten oorsmeer verwijderen. Daarop ging de NZa alle oorbehandelingen over de afgelopen jaren analyseren.

'We zagen steeds meer declaraties van dure behandelingen. Daar zat een patroon in, een verandering in de tijd of in vergelijking tot andere ziekenhuizen. Deze vorm van data-analyse is voor ons essentieel om onregelmatigheden vast te stellen.'[57]

Daarbij vindt de NZa het belangrijk om aan te geven dat zij data analyseert nadat deze dubbel gepseudonimiseerd zijn; dus die niet tot individuele personen te her-

54 Voortgang programma Rechtmatige Zorg 2015, minister van VWS, 29 oktober 2015 http://www.tweede kamer.nl/kamerstukken/detail?id=2015D41067&did=2015D41067

55 Interview met Daan Molenaar van NZa.

56 Interview met Daan Molenaar van de NZa.

57 Idem.

leiden is voor degenen die de analyse doen (wel terug te leiden in een eventuele latere fase, zie hoofdstuk over LSI en SyRI).

Mochten verzekeraars dossiers inzien, dan nog is het de vraag of dit alle fraude aan het licht zou brengen. Immers, dossiers kunnen wel in overeenstemming zijn met declaraties, maar niet met de werkelijk verrichte handelingen.
In de woorden van de NZa: 'We nemen bij de interpretatie van de uitkomsten van onze toetsen aan dat hetgeen is geregistreerd gelijk is aan de werkelijkheid […] van onze toetsen en de conclusies die we daaruit trekken, komen dus direct voort uit de data.'[58]
Om zowel het privacyprobleem als het probleem van de werkelijk verrichte behandelingen op te lossen, is een middel het betrekken van de consument bij de controle van de rekening. Die kan bij inzage in de facturen trachten te bepalen of genoemde behandelingen inderdaad zijn verricht.[59]

Wetgeving voor verruiming datatoepassing
Teneinde onder meer de intensieve samenwerking in fraudebestrijding mogelijk te maken, heeft de minister van VWS het wetsvoorstel Verbetering Toezicht en Opsporing (VTO) als onderdeel van de Wet marktordening gezondheidszorg (Wmg) ingediend bij de Tweede Kamer, waar het in behandeling is.
Het wetsvoorstel verruimt de mogelijkheden om fraude, misbruik en ongewenst gebruik te voorkomen. Een aantal aan de Kamer gedane toezeggingen wordt ingelost. Het wetsvoorstel voorziet onder meer:
– in het bieden van overzichten over nota's, eigen risico en eigen betalingen;
– bestuursrechtelijk optreden tegen nota's voor niet geleverde zorg (spooknota's);
– handhavingsbesluiten (aanwijzingen en bestuurlijke sancties) openbaar te maken, ook als deze zijn opgevolgd;
– een last onder dwangsom op te leggen bij een weigering mee te werken aan een toezichtonderzoek van de zorgautoriteit.

Een van de belangrijke onderdelen betreft de wettelijke verankering van de mogelijkheden voor de zorgautoriteit en andere partijen binnen en buiten de overheid om gegevens uit te wisselen ten behoeve van fraudebestrijding.

In de Memorie van Toelichting wordt uitvoerig stilgestaan bij de privacyaspecten. In het kader van de verstrekte onderzoeksopdracht voerde het te ver om hier in

58 Idem.
59 'Samenvattend rapport Onderzoek naar kwetsbaarheden en financiële onregelmatigheden in de zorg', NZA, november 2014. https://www.nza.nl/104107/138040/2__Samenv_rapp_Onderzoek_naar_kwets baarheden_en_financi_le_onregelmatigheden_in_de_zorg.pdf (geraadpleegd 22 januari 2016).

extensie op in te gaan inclusief de politieke behandeling. Dat laat onverlet dat dit onderwerp inclusief deze wetgeving bij groeiende medische (factuur)datauitwisseling openbare aandacht behoeft.[60]
De afwegingen aangaande privacy in verandering van wetgeving op dit terrein zijn niet of nauwelijks in de openbaarheid gekomen. Dat is gereduceerd tot, in figuurlijke zin, de 'kleine lettertjes'.
Zo staat er in de Memorie van Toelichting van het wetsvoorstel Verbetering Toezicht en Opsporing Wmg: 'Het wetsvoorstel richt zich primair op zorgaanbieders, ziektekostenverzekeraars en overheidsinstanties […] De verzekerde wiens informatie wordt uitgewisseld, kan via wet- en regelgeving en de polisvoorwaarden van de verzekering kennisnemen van het feit dat zijn persoonsgegevens, onder strikte randvoorwaarden, worden uitgewisseld […] In specifieke situaties […] zoals in de geestelijke gezondheidszorg, is aanvullend geregeld dat verzekerden via zorgaanbieders en zorgautoriteit op de hoogte worden gesteld van de wijze waarop ze gebruik kunnen maken van de mogelijkheid dat hun medische persoonsgegevens in uitzonderingsgevallen niet worden uitgewisseld.'
In de Tweede Kamer zijn amendementen ingediend door de TK-leden Leijten en Van Gerven om te voorkomen dat ziektekostenverzekeraars nieuwe bevoegdheden krijgen tot inzage in de medische persoonsgegevens van verzekerden, evenals voor het beschermen van het medisch beroepsgeheim. Ook de Autoriteit Persoonsgegevens en de Raad van State hebben kanttekeningen geplaatst bij het voorstel. Daarop heeft de minister van VWS een nota van wijzigingen ingediend.[61]

Zorgaanbieders anticiperen

Zoals FDEC opmerkte, wordt het traceren van onregelmatig declaratiegedrag moeilijker waar zorgverleners anticiperen op ontdekking. Zo gingen fysiotherapeuten

60 Wijziging van de Wet marktordening gezondheidszorg en enkele andere wetten in verband met het verbeteren van toezicht, opsporing, naleving en handhaving Nr. 3 Memorie Van Toelichting, Kamerstuk 33 980 Nr 3 Vergaderjaar 2013-2014
https://zoek.officielebekendmakingen.nl/dossier/33980/kst-33980-3

61 Wijziging van de Wet marktordening gezondheidszorg en enkele andere wetten in verband met het verbeteren van toezicht, opsporing, naleving en handhaving Nr. 3 Memorie Van Toelichting, Kamerstuk 33 980 Nr 3 Vergaderjaar 2013-2014
https://zoek.officielebekendmakingen.nl/dossier/33980/kst-33980-3
(geraadpleegd 24 januari 2016).
Aanbieding nota's bij wetsvoorstel wijziging marktordening gezondheidszorg
https://www.rijksoverheid.nl/documenten/kamerstukken/2015/09/18/aanbieding-nota-s-bij-wetsvoor stel-wijziging-marktordening-gezondheidszorg
(geraadpleegd 24 januari 2016).
Nota van Wijziging, 33980-9, 18 september 2015, E.I. Schippers, minister van Volksgezondheid, Welzijn en Sport
http://www.tweedekamer.nl/kamerstukken/detail?id=2015D34461 (geraadpleegd 24 januari 2016).

die werden aangesproken vanwege declaraties op twee of meer achtereenvolgende dagen, meer dagen tussen de declaraties agenderen.
Ook zien verzekeraars dat zorgverleners declaraties indienen zonder namen van behandelaars. In dat geval zijn patronen per behandelaar niet te analyseren en afwijkingen moeilijker te traceren. Zo kiezen geestelijke zorgverleners ervoor om de specificatie van behandelingen niet te vermelden, met een beroep op de privacy. Verzekeraars wensen juist inzicht om de rechtmatigheid of zelfs doelmatigheid van declaraties te kunnen vaststellen.
Ondanks het feit dat zorgverzekeraars – net als de Belastingdienst – vooroplopen met fraudebestrijding door data-analyse hebben ook zij soms discussie over het onderwerp privacy. 'Zoveel juristen, zoveel meningen.'[62]

Toekomstige opties dossiergebruik

'We bevinden ons in een wankel evenwicht: enerzijds horen we vaak dat het schandalig is dat het medisch beroepsgeheim op de proef wordt gesteld, maar op hetzelfde moment wordt er geuit dat het schandalig is dat verzekeraars niet beter controleren tegen fraude', aldus de NZa over de spagaat tussen regelgeving enerzijds en maatschappelijke druk anderzijds, waarvoor de politiek afwisselend argumenten hanteert.
Juist deze beide belangen moeten bij elkaar komen in één discussie, aldus partijen in de zorg: hoe ver moeten we kunnen gaan in fraudebestrijding versus beroepsgeheim van de zorgverlener en privacy van de patiënt. Het gescheiden houden van die discussies maakt de weg naar een oplossing lang. Het gaat over deze afweging en over de accountability: partijen in de zorg willen de fraudebestrijding goed kunnen uitvoeren binnen daartoe bepaalde kaders die ruimer zijn dan nu.
En daar vervolgens verantwoording over afleggen. Het huidige driestappenplan voor inzage in medische dossiers door verzekeraars, wat is aangegeven in de polisvoorwaarden, vinden ze een te strak keurslijf. Zo moeten eerst andere methoden worden benut alvorens ze een beroep mogen doen op inzage in medische dossiers. Ook mogen louter medische adviseurs dossiers raadplegen. Met zorgverleners met een contract volstaat dat, is er geen contract, dan is alsnog instemming van de verzekerde nodig. De NZa controleert de protocollen.
Dit is geen ideale situatie, vinden de NZa en de verzekeraars. AEF heeft geadviseerd om een opsporingsdienst in de zorg op te richten. Die zou ver moeten kunnen gaan met bijvoorbeeld inzet van steekproeven bij verdenkingen die voortvloeien uit tips van patiënten en signalen uit data-analyse.

De data die de NZa analyseert om onregelmatigheden op te sporen, zijn dubbel gepseudonimiseerd, zodat ze niet herleidbaar zijn tot de patiënt, maar wel tot de zorgverleners. Ze kan de naam van de patiënt wel terughalen in specifieke verden-

62 Interview Barry Egberts en Rob Konijn, Achmea.

kingen van aanbieders. Bij de NZA vindt discussie plaats over mogelijke systemen met gebruik van patiëntdossiers voor controle zonder privacyrisico's.
Koppeling van hele bestanden van dossiers is onhaalbaar. Ziekenhuizen hebben volgens Achmea wel mogelijkheden om op grote schaal behandelingen te vergelijken met declaraties, in dit geval de uitgaande declaraties. Ook worden mogelijkheden onderzocht om wel toegang te krijgen tot medische dossiers, maar gepseudonimiseerd.
Ook de declaraties waarmee die dan worden vergeleken, moeten dan van namen en nummers worden geschoond. De vraag is hier hoe zonder schending van privacy toch onjuiste declaraties getraceerd kunnen worden met behulp van analyse van dossiers.

De data van zorgdeclaraties zijn weliswaar 'big', maar onder meer de FDEC-onderzoeken toonden aan dat dit op zich onvoldoende is om de groot geachte zorgfraude te detecteren. Bestanden koppelen of tegen elkaar aan leggen gebeurt nog niet in de zorg, en evenmin met andere bestanden, zoals van de Belastingdienst en de Kamer van Koophandel.
Volgens de NZa is het vooralsnog voldoende als verzekeraars en toezichthouders analyses draaien op eigen data. Wel kunnen ze dan signalen samenbrengen, in een vervolg op het teloorgegane EZb.
Het bundelen van bestanden binnen de zorg en met derde partijen is nu niet nodig. Eerst is het zaak dat de NZa, IGZ en verzekeraars hun signalen (verdenkingen) delen. Een mogelijkheid is het opteren voor een opt-in-system: bij uitdrukkelijke toestemming door patiënten zou inzage mogelijk moeten zijn. Dat stuit echter op bezwaren van zorgverleners.
'We komen louter uit dit dilemma door burgers de eigenaar te maken van hun eigen zorgdossiers. Zij bepalen dan wie er wanneer en voor welke doeleinden inzage in de data krijgt, en voor hoelang.'[63]

63 Interview met Daan Molenaar van NZa.

4 BELASTINGDIENST

INLEIDING

De Belastingdienst beschikt over de uitgebreidste databanken die van belang kunnen zijn voor bestrijding van fraude, en is in Nederland voorloper in (big) data-analyse. De dienst zelf nam drie jaar geleden data-analyse al intensief ter hand om kaf (onjuiste aangiften, wanbetaling) van het koren te scheiden. Dat begon met een experimentele eenheid: 'broedkamer'.
Deze aanpak slaagde en werd de norm voor de gehele dienst: van apart functionerende enorme IT-systemen naar een data-gedreven netwerk van applicaties. Risicoanalyse leidt tot selectie van verdachte aangiften.
Op grond van belastingwetgeving kan de dienst vrijwel onbegrensd de eigen (big) data van 11 miljoen burgers en 1,5 miljoen ondernemingen inzetten voor fraudebestrijding.
Big belastingdata zijn ook bij andere instanties voor fraudeopsporing zeer gewild. Zowel in het sociale domein als in de strafrechtelijke opsporing en bestrijding van zorgfraude spelen gegevens over inkomens en vermogen een steeds belangrijkere rol.

In dit hoofdstuk passeert een groot aantal voorbeelden van dataprojecten met inzet van data-analyse door de Belastingdienst de revue. In hoeverre spelen politieke besluitvorming, extern toezicht of het afleggen van rekenschap een rol bij de snel uitdijende inzet van belastingdata voor fraudebestrijding? En welke wegen staan open voor een intensieve en extensieve profilering van burgers op grond van gedrag zoals geboekstaafd door de Belastingdienst (Bd) en partners in fraudebestrijding?

4.1 INNOVATIE IN DATA-ANALYSE IN DE 'BROEDKAMER'

Megadatahuis
De Belastingdienst bezit de grootste hoeveelheid data over personen in Nederland:
- van ruim 11 miljoen burgers, die aangifte inkomstenbelasting doen.
- van bijna 1,5 miljoen ondernemers, vaak dezelfde personen (zelfstandigen).
- van ca. 8 procent van alle betalingstransacties in Nederland, ofwel 1 miljoen transacties per dag.

Dit grote datahuis, aangevuld met uitkomsten van verschillende steekproeven, vormt de basis voor het vaststellen van 'nalevingstekorten' bij aangiften met behulp van steeds meer *predictive modelling,* oftewel het opstellen van voorspellende risicoanalyses. De analyse is gebaseerd op patroonherkenning door statistische analyses: hoe groot zijn de kansen op bepaalde onregelmatigheden en

zijn daarin patronen herkenbaar die nadere aandacht vragen voor controle en eventueel correctie?

Bijna drie jaar werkt de Belastingdienst met een aparte eenheid Business Intelligence en Analytics (BI&A). De afdeling is opgericht om inzichten uit data te genereren. In een interne 'incubator' ('broedkamer') worden deze inzichten omgezet in nieuwe werkwijzen voor de operatie.
De innovatieve analytische producten die op kort-cyclische wijze worden ontwikkeld en ingevoerd, moeten het werk van de medewerkers van de Belastingdienst effectiever, efficiënter en makkelijker maken. Inmiddels circa veertig, veelal jonge creatieve academici, meest wis- en natuurkundigen en econometristen, storten zich op de analyse van de enorme databerg van de Belastingdienst.
De nieuwe eenheid moet gaan bijdragen aan kostenverlaging én opbrengststijging, met krachtige slagen gericht op een maximaal resultaat. Centraal staat het observeren met een frisse blik van de vaak al decennia oude processen van de Belastingdienst, met behulp van analyse van grote verzamelingen gegevens van de aangiften in vele categorieën, met als doel te innoveren. Inmiddels is BI&A opgegaan in het organisatieonderdeel Data & Analytics. Deze afdeling is onder meer verantwoordelijk voor het opwerken van data naar (nieuwe) inzichten en analytische producten.[64]

Werkwijze Broedkamer

BI&A werkt met 'zelflerende' modellen die steeds verfijnder aangeven waar zich risico's bevinden op grond van eerdere geïnspecteerde aangiften en terugkoppeling van resultaten. Risicomodellen worden steeds verfijnd en geactualiseerd met praktijkuitkomsten van controles op grond van voorspellingen.
Met deze risicoanalyse is beter te voorspellen bij welke aangiften het risico op bijvoorbeeld onjuistheden in aftrekposten het grootst is. Hierop worden de selecties aangepast van aangiften die voor controle in aanmerking komen. Bij de correcties scheidt de dienst de incidentele onjuiste aangiften van de indicaties die duiden op mogelijke zware, systematische fraude, met bijvoorbeeld netwerken van BV's en stichtingen.
De Belastingdienst werkt met een nauwgezette methodiek om ruwe data op te werken naar informatie en vervolgens inzichten, die vertaald worden in analyseproducten. Deze methodiek kent verschillende stadia, waaronder:

- verzameling van ruwe data van alle transacties en aangiften via vaste regels voor benadering van data;
- risico- en waardeanalyse;
- segmentatie;
- identificatie;

64 Interview met Cyprian Smits van de Belastingdienst.

– culminerend in een dashboard waarop de analist verschillende soorten data kan filteren en combineren.

Zoals in alle fraudebestrijding ontstaat ook bij risicoselectie respons in de vorm van gecalculeerd gedrag van fraudeurs in een kat-en-muisspel. De fraudeur tracht onder de radar te blijven met pogingen de risico-indicatoren van de dienst te onderkennen.
Modellen zullen daarom 'bijgetraind' moeten worden door steekproeven waarmee 'nieuw gedrag' wordt onderkend met ervaringen van het menselijk gedrag in fraudedetectie door deskundige inspecteurs/controleurs. Dit vraagt om scherpe interpretatie van uitkomsten en creativiteit in het bepalen van nieuwe combinaties, teneinde te komen tot aanscherping van risicofactoren te komen en nieuwe gecombineerde indicatoren.

Dit soort snelle projecten voor data-analyse kent een doorlooptijd van zes tot twaalf maanden van idee tot implementatie, inclusief het programmeren van de software. Dit in tegenstelling tot traditionele datawarehouseprojecten, die alleen al qua ICT-ontwikkeling al snel jaren in beslag nemen, met de inmiddels van ICT-projecten bij de overheid bekende pieken en (vooral) dalen.
Zo waakte de eenheid voor sturing door IT. De leiding was ervan overtuigd dat IT als startpunt van dataprojecten de grootste kans op falen biedt. Bij deze interne Broedkamer van Data & Analytics lopen verschillende projecten tegelijkertijd, tegen lage kosten.
In het eerste van onze vraaggesprekken met de Belastingdienst[65] werd een periode van een maand genoemd waarin de investering in datacapaciteit en ondersteunende ICT zou worden terugverdiend met bestrijding van fraude en (andere) onjuiste aangiften en -gedrag. Zo konden projecten van de Broedkamer ook snel worden beëindigd bij gebrek aan resultaat, in tegenstellingen tot traditionele IT-projecten, die – zoals bekend uit de parlementaire enquête – vaak in drama's eindigden.
De focus ligt op informatieprojecten zonder de wens tot verbouwing van grote transactieprocessen. Gevolg is dat de slaagkans van projecten ten opzichte van de oude situatie flink was toegenomen, mede dankzij eenvoudiger ICT. Benodigde software voor data-analyse is standaard in de markt voorhanden. De resultaten zijn in een webbrowser te delen.[66]

65 Idem.
66 Idem.

Resultaatmeting

De taak van de eenheid BI&A is breder geformuleerd dan louter in termen van handhaving en fraudebestrijding. De vijf waarden waarop resultaten worden gemeten:

1. meer waarde/opbrengst;
2. beter procesbeheer;
3. gemak van de invoering;
4. zinvol voor het personeel;
5. IT-besparing.

Voorbeelden van projecten en gevolgen:

– dynamisch monitoren: deze innovatie signaleert automatisch wanneer verhaalsmogelijkheden (loon, auto's, vastgoed, etc.) ontstaan bij openstaande vorderingen waar beslag gelegd mag worden. De medewerker kan hierdoor openstaande vorderingen effectiever innen. Inmiddels is deze innovatie uitgerold bij alle teams van het Landelijk Incassocentrum, die de vorderingen van particulieren afhandelen.
– De succesratio van loonbeslag steeg met een factor twee, terwijl tegelijkertijd de tijd benodigd voor het afhandelen van een loonbeslag halveerde. Veel minder belastingplichtigen worden onnodig lastiggevallen, waardoor deze Big Data-toepassing ook de nationale stressfactor verlaagt.
– Bij de Inkomstenheffing(IH) is dankzij de inzet van data-analyse en voorspellende modellering de *hitrate*, het aantal gecontroleerde aangiften die correctie behoeven, significant verhoogd. Met de resultaten worden nieuwe analyses gevoed, die tot steeds hogere succesratio's leiden, ofschoon met een afnemende stijging.
– Op grond van data-analyse is de selectie van te controleren bedrijven die btw terugvragen, veel scherper geworden. Met hetzelfde aantal ambtenaren is de slaagkans van btw-correcties meer dan verdubbeld.
– De bestrijding van carrouselfraude en multicelfraude is dankzij netwerkanalyses veel effectiever geworden. Door het voortdurend monitoren van alle handelsrelaties tussen bedrijven en stichtingen worden mogelijke carrouselfraudes eerder en veel omvangrijker dan voorheen gespot en beëindigd. Inmiddels zijn, mede op grond van terugkoppeling van ervaringen, 150 patronen ontwikkeld die uit de grote bestanden relaties van malicieuze netwerkorganisaties in beeld brengen. Ook deze modellen worden voortdurend 'getraind' op grond van uitkomsten en verder geperfectioneerd.
– Doordat de interne data nu op methodische wijze zijn georganiseerd, kan sneller antwoord gegeven worden op actuele vragen, bijvoorbeeld bij beantwoording van Kamervragen. Bij de zogenoemde Bulgarenfraude met toeslagen was dankzij deze afdeling binnen 24 uur het mogelijke schadebedrag bekend: 95,2 miljoen euro. En konden transacties onmiddellijk worden gestaakt.

- Ook: bij de ramp met de MH17 waren binnen enkele uren nadat minister Plasterk besloot om vermissingen als overlijden te behandelen, de schuldenposities van slachtoffers bekend en kon het verzenden van 'blauwe enveloppen' op hun naam worden gestaakt.
- In 2014 signaleerde de Belastingdienst onregelmatigheden met 50.000 aangiften, met 100 miljoen euro aan valse teruggaveclaims. Daarvan is 80 miljoen niet uitgekeerd, de overige 20 miljoen later teruggevorderd.
- In februari 2014 is een belastingadviseur uit Overijssel veroordeeld, omdat hij bijna 3200 valse aangiften voor zijn klanten had ingediend, met vals opgevoerde zorgkosten. De Belastingdienst werd bij deze zaak voor 3,5 miljoen benadeeld, zelf had de tussenpersoon er 150.000 euro mee verdiend. Data-analyse onder adviseurs leverde een relevante bijdrage aan de opsporing.
- In 2014 zijn 106 witwasonderzoeken afgerond, waarvan het Conservatoir Beslag 310 miljoen euro bedroeg.[67]
- Resultaat over 2014 met vroegtijdig onderkennen van onregelmatigheden dankzij data-analyse:
  - 180 miljoen euro aan teruggevraagde inkomstenbelasting niet uitbetaald;
  - 52 miljoen euro aan niet uitgekeerde en gecorrigeerde toeslagen.
- Vanuit data-analyse bestreed het Combiteam Aanpak Facilitators (CAF) gestructureerd misbruik van belastingvoordelen dan wel toeslagen. Het team heeft in het tijdsbestek van ongeveer 1,5 jaar circa tweehonderd zaken opgepakt. Vervolging hoort daarbij.

Begin mei 2016 maakte de Belastingdienst bekend dat het CAF vanuit data-analyse honderd belastingadviseurs met hun 75.000 klanten in het vizier kwamen die voor meer dan 400 miljoen euro aan onterechte aftrekposten hadden geclaimd. Met 79 adviseurs is een schikking getroffen en 21 worden er voor de rechter gebracht.

- De Belastingdienst schonk extra aandacht aan de algemeen nut beogende instelling (ANBI). Er bleek een groot aantal ANBI's te zijn, zo'n 60.000, met geringe fiscale aandacht. De Belastingdienst stelde tweehonderd extra boekenonderzoeken in. De resultaten leveren data op voor permanente analyse voor handhaving alsmede aanbevelingen voor wet- en regelgeving.
- De douane past ook meer en meer data-analyse toe voor de selectie van te controleren zendingen. De intelligencefunctie is van groot belang bij de analyse van risico's en voor de keuze voor instrumenten voor handhaving. Dit is bij-

67 Idem.

voorbeeld toegepast bij de aanpak van kleding en schoenen die tegen een te lage waarde worden aangegeven, voor ontduiking van douanerechten.[68]

Uiteraard meldt de dienst bij voorkeur de successen. Maar projecten leveren soms niet het gewenste resultaat op, waarvoor juist met de korte doorlooptijden ook alle ruimte is. Bijsturen kan dan veel sneller plaatsvinden dan in het sturen met grote IT-systemen.
De Broedkamer werkt met een 'innovatiefunnel': producten worden in meerdere fases ontwikkeld. Aan het eind van elke fase wordt bepaald of een product nog voldoet aan de eerder genoemd criteria (opbrengst, procesbeheer, etc.). Als een idee/innovatie onvoldoende scoort, wordt de ontwikkeling stopgezet.

De getrokken lessen:
– Commitment vanuit het topmanagement is cruciaal. De levert het benodigde draagvlak en versnelt besluitvorming en ontwikkeling.
– Niet te veel ideeën en innovaties tegelijkertijd ter hand nemen. Alleen de beste ideeën, met het grootste effect, gaan door.[69]

4.2 SAMENWERKINGSVERBANDEN MET BELASTINGDATA

Alle twintig convenanten
Een inventarisatie van alle gepubliceerde convenanten biedt een beeld van samenwerkingen met data van de Belastingdienst voor analyse en onderzoek. In totaal publiceert de Belastingdienst twintig convenanten voor uitwisseling van data met overheden en andere instanties.[70]

In alfabetische volgorde met de/het:

1. Arbeidsinspectie en Inspectie SZW (voorheen: SIOD), 2010,
   Uitwisseling: de Belastingdienst levert een groot aantal bestanden, Inspectie SZW deelt de uitkomsten van risicoanalyses met de Arbeidsinspectie en de Belastingdienst zelf.

---

68 15e halfjaarrapportage Belastingdienst, 26 maart 2015 http://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2015Z05518&did=2015D11192
16e Halfjaarrapportage van de Belastingdienst, 16 september 2015 https://www.rijksoverheid.nl/documenten/kamerstukken/2015/09/16/16e-halfjaarsrapportage-van-de-belastingdienst

69 Interview met Cyprian Smits van de Belastingdienst.

70 http://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/belastingdienst/intermediairs/toezicht/convenanten/convenanten_met_afnemers_van_informatie/ (laatst geraadpleegd 8 februari 2016).

Doel: handhaving van sociale zekerheids- en belastingwetgeving, en wetgeving op het gebied van arbeidsomstandigheden, arbeidsvoorwaarden en arbeidsmarkt.[71]

2. Centraal Administratiekantoor (CAK), 2011,
Uitwisseling: 'Authentieke Inkomensgegevens'.
Doel: controle op de hoogte van eigen bijdragen in de zorg voor handhaving Wmo, AWBZ en Wet Tegemoetkoming Chronisch Zieken en Gehandicapten.[72]

3. Centraal Justitieel Incassobureau (CJIB), 2013,
Uitwisseling: de Belastingdienst levert fiscale informatie, het CJIB verstrekt informatie benodigd voor de belastingheffing.
Doel: tenuitvoerlegging wettelijke CJIB-taken zoals inning van boetes en ontnemingen.[73]

4. College van Zorgverzekeringen (CVZ), 2011
Uitwisseling: de Belastingdienst levert data over belastbaar inkomen en premies.
Doel: uitvoering Zvw (Zorgverzekeringswet) en AWBZ; eveneens inzake invorderingen, wanbetalers, risicoverevening zelfstandigen, niet ingezeten zelfstandigen, gemoedsbezwaarden.[74]

5. DG Fiscale Zaken, 2015
Uitwisseling: toegang van de afdeling AFP/Analyse tot data over tien verschillende, apart benoemde vormen van belastingen, in de ICT-omgeving van de Belastingdienst. Productie analysebestanden in de ICT-omgeving van de Belastingdienst. Overzetten geaggregeerde resultaten van analyses naar Ministerie van Financiën.
Doel: analyses ten behoeve van ontwikkeling van fiscaal beleid.[75]

---

71 http://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/themaoverstijgend/brochures_en_publicaties/convenant_met_arbeidsinspectie_siod_deelconvenant_arbeidsmarkt

72 http://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/themaoverstijgend/brochures_en_publicaties/convenant_belastingdienst_cak

73 http://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/themaoverstijgend/brochures_en_publicaties/convenant_belastingdienst_centraal_justitieel_incassobureau

74 http://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/themaoverstijgend/brochures_en_publicaties/convenant_belastingdienst_college_voor_zorgverzekeringen_cvz

75 http://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/themaoverstijgend/brochures_en_publicaties/convenant_belastingdienst_directoraat_generaal_fiscale_zaken

6. Financieel Expertise Centrum, 2014
   Uitwisseling: structurele dataverstrekking in samenwerking van Autoriteit Financiële Markten (AFM), de Belastingdienst, De Nederlandsche Bank, Financial Intelligence Unit Nederland, Fiscale Inlichtingen- en Opsporingsdienst, Openbaar Ministerie en Politie.
   Doel: Kenniscentrum realiseren, uitvoeren van projecten inzake handhaving van de integriteit ten behoeve van doeltreffende bestuurlijke en strafrechtelijke rechtshandhaving in de financiële sector.[76]

7. ICOV (Crimineel en Onverklaarbaar Vermogen), 2013
   Uitwisseling: Bestanden Bd (inclusief FIOD, Douane, Toeslagen), OM, Politie en FIU.
   Doel: 'onverklaarbaar' vermogen en witwas- en fraudeconstructies blootleggen in opdracht participanten. Geen eigen doelstelling.
   Zie uitgebreide analyse van iCov in hoofdstuk 12.[77]

8. Landelijke Stuurgroep Interventieteams, 2003
   Uitwisseling: bestanden van de Belastingdienst, Arbeidsinspectie, UWV (polisadministratie) , de SVB, het OM, gemeenten (VNG), Divosa (sociale diensten)departementen Financiën en SZW.[78]
   Doel: terugdringen belasting-, premie en uitkeringsfraude en misstanden op de arbeidsmarkt en samenhangende wetsovertreding. Permanente werkgroep Informatieanalyse, geleid door de Inspectie SZW, voor ondersteuning negen regionale platforms bij keuze en bepaling van projecten voor interventie.

9. Kansspelautoriteit, 2013
   Uitwisseling: de KSA verschaft bedrijfsgegevens, de Belastingdienst signalen van mogelijk illegaal aanbod van kansspelen en 'gegevens inzake cases die mogelijk van belang zijn' voor KSA
   Doel: heffing, inning, toezicht en handhaving van de kerntaken van beide partijen. Gericht op aanbod van diensten, niet op spelers.[79]

---

76 http://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/themaoverstijgend/brochures_en_publicaties/convenant_houdende_afspraken_over_de_samenwerking_in_het_kader_ van_het_fanincieel_expertise_centrum

77 http://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/themaoverstijgend/brochures_en_publicaties/convenant_belastingdienst_icov_2013

78 http://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/themaoverstijgend/brochures_en_publicaties/belastingdienst_interventieteams

79 http://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/themaoverstijgend/brochures_en_publicaties/convenant_met_de_kansspelautoriteit

10. LIEC/RIEC (Landelijke en Regionale Informatie- en Expertise Centra) 2012
Uitwisseling: informatie tussen ministerie VenJ, politie, burgemeesters, het OM, de politie, de Belastingdienst (incl. Douane, FIOD), Inspectie SZW, provincies, de Marechaussee en de IND. Onder meer structurele inbreng politiedata op grond van de Wet politiegegevens (Wpg). De samenwerking staat open voor andere belanghebbenden.
Doel: aanpak van ondermijnende criminaliteit (zoals mensenhandel, hennepteelt, vastgoedfraude en witwassen) en het tegengaan van infiltratie van de onderwereld in de bovenwereld. Elke twee jaar vindt evaluatie plaats.[80]

11. Ministerie van Infrastructuur en Milieu, 2012 (bundeling en vervanging van eerdere overeenkomsten)
Uitwisseling: Gegevens Douane en de Inspectie Leefomgeving en Transport
Doel: verhoging van de doeltreffendheid en doelmatigheid van beider handhavingstaken, dat wil zeggen nauwe samenwerking bij controles.[81]

12. Ministerie van Justitie (rittenadministratie)
Uitwisseling: irrelevant in kader dit onderzoek.
Doel: komt neer op afschaffing van verplichte rittenadministratie voor het aantonen van beperkt privégebruik.[82]

13. Ministerie van OCW, verlenging 2015
Uitwisseling: informatie over detectie, beoordeling, analyse en nader onderzoek van risicovolle vastgoedtransacties uitwisselen, met name over rechtspersonen en hun bestuurders actief in het onderwijs.
Doel: misbruik, oneigenlijk gebruik en het ondoelmatig van vastgoed tegengaan en mogelijke overtredingen WVA en subsidieregeling Praktijkleren in kaart brengen, te beperken en bestrijden.[83]

---

80 http://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/themaoverstijgend/brochures_en_publicaties/convenant_liec_riec_met_het_ministerie_van_vj_om_politie_burgemeesters_korpsbeheerders_en_lokale_besturen
Zie ook www.riec.nl/
http://www.riec.nl/doc/liec/Boek%20Samen%20gebundeld_LIEC_201510_DEF.pdf

81 http://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/themaoverstijgend/brochures_en_publicaties/convenant_met_het_ministerie_van_infrastructuur_en_milieu

82 http://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/themaoverstijgend/brochures_en_publicaties/convenant_belastingdienst_rittenadministratie_dienstvoertuigen_politie

83 http://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/themaoverstijgend/brochures_en_publicaties/convenant_met_het_ministerie_van_onderwijs_cultuur_en_wetenschap_ocw

14. Ministerie van OCW)/ Dienst Uitvoering Onderwijs (DUO), 2013
Uitwisseling: Duo levert structureel geverifieerde BSN-nummers met geboortedata aan bij de Belastingdienst die data aanlevert over inkomen en vermogen over maximaal laatste vijf jaren. De Belastingdienst levert niet zelfstandig data over partners, anders dan in de DUO-aanvraag genoemd. Bij incidentele aanvragen van data gaat de Belastingdienst de rechtmatigheid na.
DUO levert jaarlijks aan de Belastingdienst data over studiefinanciering, zowel subsidie als leningen.
Doel: oneigenlijk gebruik van studiefinanciering tegengaan en handhaving belastingplichten.[84]

15. Kamer van Koophandel, 2010
Uitwisseling: in principe geen uitwisseling van bestanden of data voor fraudebestrijding.
Doel: samenwerking bij inschrijvingen om lastendruk te verminderen. KvK geeft RSIN-nummers (fiscaalnummers) uit en meldt die terug aan de Belastingdienst.[85]

16. Nederlandse Mededingingsautoriteit, 2007
Uitwisseling: data van NMA naar de Belastingdienst, verkregen uit uitoefening van de Mededingingswet; eventueel tips over en weer over mogelijk strafbare feiten. Geen grootschalige data-uitwisseling voor risicosignalen.
Doel: handhaving Kansspelwet en Belastingplichten.[86]

17. Openbaar Ministerie, 2008, Convenant Gegevensuitwisseling Aanpak Vastgoed
Uitwisseling: de Belastingdienst en de FIOD verschaffen belastingdata, het OM (en politie) strafvorderlijke data en KvK-data. Ook uitgebreide verzameling en uitwisseling van persoonsgegevens.
Doel: fraudebestrijding en oprichting Vastgoed Intelligence Center voor strategische, tactische en operationele analyses, op te zetten in een testomgeving (lab). Samenwerking gefaseerd uitbreidden met partijen die betrokken zijn bij misdaadbestrijding waarbij onder meer vastgoed in het geding is (data worden

84 http://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/themaoverstijgend/brochures_en_publicaties/convenant_met_het_ministerie_van_onderwijs_cultuur_en_weten schap_ocw_dienst_uitvoering_onderwijs

85 http://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/themaoverstijgend/brochures_en_publicaties/belastingdienst_kvk

86 http://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/themaoverstijgend/brochures_en_publicaties/convenant_belastingdienst_nederlandse_mededingingsautoriteit_nma

bewaard zo lang als nodig wordt geacht voor onderzoek naar malversaties. Personen worden altijd actief geïnformeerd tenzij ze al op de hoogte zijn).[87]

17. Politie, 2014
Uitwisseling: van de Politie betrekt de Belastingdienst realtime alle gefotografeerde kentekens van de tweehonderd mobiele en vaste (ANPR)-politiecamera's op de Nederlandse hoofdverkeersaders. Dat is het totale bestaand met miljoenen kentekens onafhankelijk of er een verdenking is. De Belastingdienst beroept zich hiertoe op Art. 11 van de Belastingwet (Awr), dat wil zeggen op 'de autonomie van de inspecteur om op basis van de hem bekende feiten/waarnemingen een aanslag op te leggen'.
Doel: de Belastingdienst wendt de data aan voor bepaling van privégebruik van zakelijke auto's en handhaving en controle inzake , motorrijtuigenbelasting, vennootschapsbelasting en zware voertuigen (Eurovignet).
(De controle richt zich met name op plichten van ondernemers. Van auto's in bezit van particulieren worden enkel data opgeslagen die 'relevant' zijn voor de wegenbelasting: dus voertuigen die wel worden gebruikt, maar worden opgegeven als niet in gebruik zijnde. De niet-relevante data vernietigt de Belastingdienst en komen niet in de 'databank auto'.
Belastingplichtigen hebben recht op informatie over opgeslagen data die aan hun aanslagen zijn gekoppeld en kunnen daar een beroep op doen. Dat worden verwijderd als ze niet relevant meer zijn. Minimaal eenmaal per jaar wordt de databank auto geschoond. Evaluatie van de regeling vindt jaarlijks plaats.[88]

18. Stichting Normering Arbeid, 2009
De Stichting Normering Arbeid en de Belastingdienst hebben een convenant gesloten over de verwerking van de verzoeken van ondernemers over hun aangifte- en betaalgedrag bij de Belastingdienst. Gecertificeerde ondernemers geven de Stichting Normering Arbeid toestemming om de gegevens op te vragen bij de Belastingdienst.

---

87 http://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/themaoverstijgend/brochures_en_publicaties/convenant_gegevensuitwiseling_aanpak_vastgoed

88 Convenant http://download.belastingdienst.nl/belastingdienst/docs/convenant_belastingdienst_politie_anpr_al11421z1ed.pdf
Protocol Convenant Belastingdienst met de Politie betreffende ANPR camera's, versie 2.0 van 7 januari 2015
http://download.belastingdienst.nl/belastingdienst/docs/protocol_convenant_belastingdienst_politie_anpr_al11431z2ed.pdf

Deze specifieke data-uitwisseling is in het kader van dit onderzoek irrelevant.[89]

19. Team Track van het ministerie van VenJ, 2013
Uitwisseling: met Team Track (onderdeel dienst Justis van VenJ) wisselt de Belastingdienst sinds begin 2013 intensief informatie uit voor het toezicht op rechtspersonen (bedrijven en stichtingen).
Resultaten van data-analyse door Team Track monden uit in risicomeldingen, bijvoorbeeld over genoemde carrouselfraude. De Belastingdienst beoordeelt de risicomeldingen en maakt melding van de bruikbaarheid van de tips. De Belastingdienst mag de gegevens verstrekken aan andere partijen die betrokken zijn bij de handhaving en fraudebestrijding.
Doel: uitvoering van de Wet controle op rechtspersonen.[90]

Kenmerken:
– In alle convenanten zijn bepalingen opgenomen voor doelbinding, geheimhouding (beveiliging) en vaak ook betrokkenheid van privacy-officers.
– Alle convenanten kennen een stilzwijgende verlenging. Ook wordt er voor 'nadere afspraken' of 'invulling' van de overeenkomst de mogelijkheid opgehouden voor 'nadere overeenkomsten'. Deze zijn in geen enkel geval toegevoegd.

Voor de navolgende samenwerkingen is op bovengenoemde pagina geen convenant aangetroffen. Volgens de Belastingdienst zijn ze gestoeld op gezamenlijke regelingen, die echter niet allemaal zijn gepubliceerd. Die voor het Financieel Expertise Centrum (FEC), een verband met het OM, politie, FIOD, DNB, FIU en AFM, stond in de *Staatscourant*. Maar deze ging evenmin als de convenanten langs het parlement.
Het gezamenlijke doel van de FEC-partners is het versterken van de integriteit van de financiële sector. Voor verantwoording en transparantie publiceert het FEC op een eigen website met jaarplannen en jaarverslagen. Daar wordt gewag gemaakt van steeds meer signalen van fraude die worden behandeld in 'datarooms'.[91]

---

89 http://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/themaoverstijgend/brochures_en_publicaties/convenant_stichting_normering_arbeid_en_de_belastingdienst_met_betrekking_tot_de_gegevensuitwisseling_van_aangifte_en_betaalgedrag

90 http://download.belastingdienst.nl/belastingdienst/docs/convenant_uitvoering_wet_controle_op_rechtspersonen_al11111z1ed.pdf

91 Convenant houdende afspraken over de samenwerking in het kader van het Financieel Expertise Centrum (Convenant FEC 2014), Staatcourant Jaargang 2014, Nr. 2351 https://zoek.officielebekendmakingen.nl/stcrt-2014-2351.html
FEC-jaarverslag 2014 & FEC-jaarplan 2015 https://www.fec-partners.nl/nl/nieuws/nieuwsbericht/120

Samenwerkingen zonder convenant van de Belastingdienst

- Anti-Money Laundering Centre (AMLC), een multidisciplinair centrum op het gebied van witwasbestrijding. Deelnemers: FIOD en andere Bijzondere Opsporingsdiensten, Financial Intelligence Unit (FIU), politie en OM.
- Landelijk Informatiecentrum Voertuigcriminaliteit (LIV) koppelt informatie van RDW, Nationale Politie, FIOD, de stichting Verzekeringsbureau Voertuigcriminaliteit (VbV) en de Belastingdienst. Voor fraudebestrijding vindt ook data-analyse en informatiecoördinatie met bestanden plaats. Onder meer verzekeringsmaatschappijen maken hiervan gebruik.
- Er is een convenant voor LIV dat de Belastingdienst niet heeft getekend. De Belastingdienst wisselt dan ook geen gegevens uit met de andere partijen.[92]
- Ook kentekens van auto's van politie in gemeenten waarvoor geen parkeergeld is betaald, worden door de Belastingdienst en de RDW vergeleken met bestanden, bijvoorbeeld van gestolen voertuigen en van geïmporteerde auto's. Het gaat volgens de Belastingdienst om 'derdenonderzoek', dus is er geen convenant nodig.[93]

Manifestgroep, Expertisecentrum Fraude

De Manifestgroep is in 2003 opgericht als samenwerkingsverband van DUO, CAK, de Belastingdienst, UWV en de SVB. Ze richt zich op gezamenlijke verbetering en uitbreiding van dienstverlening. Vanuit de Manifestgroep begon in 2012 een poging tot oprichting van een gezamenlijk Expertisecentrum Fraude, waarin deze overheidsorganisaties samenwerken. De Belastingdienst was trekker. Andere partijen die aansloten waren:

- Inspectie SZW;
- Immigratie- en Naturalisatiedienst (IND);
- Dienst Uitvoering Onderwijs (DUO);
- Sociale Verzekeringsbank (SVB);
- Kamer van Koophandel;
- Logius (ministerie BZK);
- Koninklijke Marechaussee (KMAR);
- Centraal Administratiekantoor (CAK-zorg);
- Basisadministratie Persoonsgegevens en Reisdocumenten RVIG;
- Rijksdienst voor ondernemend Nederland;
- UWV;
- RDW;
- NVIK Nationaal Vreemdelingen Informatie Knooppunt.

92 www.liv.nl (geraadpleegd 16 juni 2015).

93 Interviews met Cyprian Smits en Nicole Back van de Belastingdienst.

(Het laatste is een project van de Nationale Politie ter bevordering van het Informatiegestuurd werken van de vreemdelingenpolitie Nederland (nu: AVIM), een club die de afgelopen jaren in veel samenwerkingsverbanden participeerde). Het Expertisecentrum begon met de ontwikkeling van gezamenlijke risicokenmerken en -profielen. De beoogde opzet van het centrum biedt een goed beeld van de ambities met gezamenlijke data-analyse voor fraudebestrijding.

Doelen:
- productie van signalen waarmee fraudeurs kunnen worden getraceerd en aangepakt. Oftewel een *overheidsbreed early warning*-systeem zodat nieuwe fraudes sneller en completer in beeld komen;
- kennis over fraudes en fraudebestrijding (zoals tools, profielen, privacy, invordering) verspreiden en afstemmen.

Middelen:
- Het centrum ging profilering op touw te zetten. 'Beschrijf fraudeprofielen en daarna fraudeursprofielen met daderkenmerken. Pas die toe, valideer en wissel het resultaat daarvan uit.'
- Ook werd al geopperd om daartoe algoritmen op de totale populatie (bestanden) los te laten, teneinde nieuwe fraudes te ontdekken en scheiding aan te brengen tussen groepen burgers en bedrijven met grote en kleine risico's op fraude.
- Het stimuleerde een levendige uitwisseling van kennis over fraude, intelligence, privacywetgeving, van databanksystemen (SAS), data-analyse, van software, fraude-opleidingen, profilering.

De betrokken 'Handhavingsregisseur Landelijke Toezicht Organisatie' van de Belastingdienst verklaarde de beoogde patroonherkenning aldus: 'Als het ware kruipen we dus in de huid van een fraudeur. Essentieel bij fraudebestrijding is natuurlijk ook het delen van elkaars gegevens. Het stelsel van basisregistraties maakt het nu technisch mogelijk gegevens te delen.'[94] Echter, de analyse en profilering overlaten aan machines was geen optie, aldus deze handhavingsregisseur, kennis van specialisten is onontbeerlijk: 'Het blijft mensenwerk. De crux zit 'm juist in het samenwerken. Dan pas verschijnt het complete plaatje.' Hij opperde dus het voornemen om het Expertisecentrum in te richten als een Campus. Er zouden 'datascientists' aangetrokken worden, onder meer om het zoeken op internet naar fraudepatronen te optimaliseren. Dit voornemen uit 2013 is verlaten.

94 Manifest-groep Fraude-analyse – van overheidsbrede bundeling van knowhow tot fraude-expertisecentrum, presentatie Frans Bentvelsen Belastingdienst, 29 april 2014 via Slideshare op 31 december 2015
http://www.slideshare.net/Buzztour/manifestgroep-door-frans-bentvelsen

Pilotprojecten:

1. Gefingeerde dienstbetrekkingen. Ten behoeve van de IND zijn op bedrijfsadressen eendagscontroles uitgevoerd door UWV en de Belastingdienst. De IND leverde risicogevallen. KvK en de Belastingdienst vulden die aan met gegevens. 'Onder deze risicogevallen bevinden zich enkele met aanzienlijke nalevingstekorten bij meerdere overheden. Sommige controles zijn of worden daarom opgeschaald.'[95]
2. De IND vroeg de Belastingdienst om onderzoek te doen naar de aanvraag van verblijfsvergunningen voor vijfhonderd Chinese koks. Is volgens de dienst een 'grote FIOD-zaak geworden' met gefingeerde dienstbetrekkingen.[96]
3. Invordering van studieschulden. DUO heeft te maken met een steeds vaker voorkomend fenomeen waarbij burgers die een studieschuld hebben zich uitschrijven uit de Gemeente basisadministratie (GBA) en waarvan geen adres meer bekend is. DUO wordt geholpen bij het verzamelen van adressen. Is als businesscase voortgezet.
4. Buitenlandse studenten: de IND (verblijfsstatus) en KMar (identiteit en woonplaats) helpen DUO in twijfelgevallen of buitenlandse studenten recht hebben op een studiebeurs. Resultaat: groot aantal studiebeurzen zijn ingetrokken en van (Angolese en Nigeriaanse) jongeren zijn de verblijfsvergunningen ingetrokken.

Vervolgens kwamen er meer 'Antifraudeprojecten':

- monitoring en analyse inkomend webverkeer;
- overheidsbrede veelplegers aanpak;
- Belastingdienst en Logius werken samen in misbruik DigiD voor fraude met toeslagen;
- 'Oriëntatie Rijscholen'. Het UWV wilde een handhavende actie starten en vroeg de Belastingdienst om adres- en omzetgegevens van rijscholen;
- Bulgaarse ondernemers en studietoelagen: DUO vroeg de Belastingdienst om tachtig Bulgaren te onderzoeken, die aangaven een voltijdsonderneming te drijven;
- In de haven van Rotterdam worden in het zogenoemde Regenboogteam, bestaande uit verschillende toezichthouders, risicoanalyses gedeeld, controles afgestemd en inspectieresultaten met elkaar uitgewisseld. 'Zo ontstaat een gezamenlijk beeld van de goede en minder goede nalevers van de wet- en regelgeving in de Rotterdamse haven.'[97]

Maandelijks komen de organisaties van de Manifestgroep bijeen en wordt kennis gedeeld over fraudepatronen, maar geen data. De proefprojecten en definitieve

95 Idem.
96 Idem.
97 Idem.

projecten zijn immers niet uitgevoerd in een Fraude Expertisecentrum van de Manifestgroep, zoals de bedoeling was. Waar nodig, werken partijen operationeel samen en wisselen data uit binnen de bestaande regelgeving en convenanten.

4.3 PRIVACYVRAAGSTUKKEN EN PRIVACYKRITIEK

Manifestgroep twijfels en convenanten

Dit initiatief van de Manifestgroep verschafte ook inzage in de zorgen over botsingen met de privacy. Bij de opzet van deze samenwerking en het beoogde gezamenlijke Expertisecentrum werd de regelgeving omtrent onderling verstrekken van gegevens als probleem gezien. Volgens de deelnemers waren er drie drempels tot intensieve data-uitwisseling:

- de geheimhoudingsplicht van de Belastingdienst;
- de huidige privacywetgeving;
- de aanstaande EU-verordening voor privacy.

'Er bestaan tweehonderd convenanten – Kortom, een lappendeken', aldus de Belastingdienst.[98] Dus werd de vraag opgeworpen of er één algemene regeling voor uitwisseling van data noodzakelijk was.

Die is er niet gekomen, in tegenstelling tot de SyRI-regeling voor opsporing van fraude in het sociale domein, waarvoor de Belastingdienst overigens ook databestanden levert. De Belastingdienst deed de aanbeveling om data zoveel mogelijk te anonimiseren. Eveneens om een Privacy Impact Analyse (PIA) te maken voor het fraudeonderzoek, teneinde beschuldiging van privacyschending vóór te zijn. Er werd evenwel ook geopperd om 'oplossingen' te bedenken, bijvoorbeeld in de vorm van interne 'guidelines'.[99]

Uit uitgewerkte versies van genoemde convenanten blijkt uitgebreide aandacht aan borging van privacy, dat wil zeggen aan de vereisten om in theorie aan de regels van de Wbp te voldoen. Zoals bijvoorbeeld voor de datasets die de RIECs en LIEC hanteren. De stuurgroep 'ziet erop toe dat deze gegevensset wordt vastgelegd in de Checklist Wbp en dat de melding van de gegevensverwerking conform deze Checklist wordt gedaan bij de Autoriteit Persoonsgegevens […] Indien dit noodzakelijk is als gevolg van wijzigingen, wordt deze Checklist Wbp geactualiseerd en wordt de update opnieuw aangemeld bij het Autoriteit Persoonsgegevens.'

Zestien jaar oud onderzoek

Er is passief noch actief toezicht van de Autoriteit Persoonsgegevens op de samenwerkingsverbanden. Op de site van de AP is wel een uitgebreid onderzoek te vinden over data-uitwisseling van de Belastingdienst. Dat dateert echter van 1999.

98 Idem.
99 Idem.

Niettemin is dit onderzoek naar opzet en uitkomst nog redelijk actueel. Het ging de AP (toen nog 'Registratiekamer') om controle op de verstrekking van persoonsgegevens door de fiscus, die verdergaat dan nodig is voor de belastingheffing. De AP deed onderzoek naar het 'spanningsveld' tussen de datahonger van de dienst en privacybescherming. Ze stelde vast dat een adequate wettelijke grondslag en voldoende wettelijke waarborgen tegen ongewenste inbreuken op de privacy ontbraken.
Ze pleitte al voor:

- het vastleggen van de noodzaak van dataverstrekking in verband met maatschappelijke belangen (als fraudebestrijding);
- een duidelijk omschreven rol voor de Belastingdienst;
- ten minste op hoofdlijnen invulling van de begrenzing;
- zoveel mogelijk openheid ten aanzien van de verstrekte data.

Ruim zestien jaar later wordt aan deze vereisten wellicht naar de letter voldaan, bijvoorbeeld met de publicatie van convenanten. Dat is volgens de partijen een voldoende wettelijke grondslag. Parlement noch toezichthouder AP toetsten de convenanten. Ook is er geen of weinig transparantie over de uitvoering van de data-uitwisseling met derde partijen.
Nog afgezien van een afweging van de toen al geldende kernafwegingen voor datavergaring en uitwisseling: doelbinding (data alleen gebruiken voor het doel waarvoor ze zijn verzameld); subsidiariteit (echt nodig), proportionaliteit (sober gebruik). De AP vond dat datavergaring en gebruik wettelijk beter verankerd moesten zijn.
Volgens de Belastingdienst zelf volstaat strenge beoordeling door een fulltime eigen privacy-officer, die toeziet op een correcte behandeling van data in de analyse van grote bestanden. De privacyfunctionaris toetst op de strenge voorwaarden van de Wbp, met name proportionaliteit en doelbinding. Dat weegt zwaarder bij uitwisseling van bestanden die worden gecombineerd voor analyse.
De Belastingdienst moet haar methoden van data-analyse kunnen standhouden in rechtszaken en voor de Auditdienst Rijk (ADR). Dit betekent in gelijke gevallen en (rechts)personen het hanteren van gelijke behandeling. De dienst mag zich niet concentreren op bijvoorbeeld Oost-Europeanen, of nog nauwer, hier verblijvende aangevers met een Bulgaars paspoort. Er moeten concrete verdenkingen bestaan zonder discriminatie van een groep (op de vraag naar de verantwoording verwijst de Belastingdienst naar de ADR). De openbaarheid van de rapporten van Auditdienst staat ter discussie. Er zijn Kamervragen over gesteld.[100]

100 Nummer 2015Z25355. Vragen van de leden Ronnes en Omtzigt (beiden CDA) aan de ministers van Financiën, van VenJ, de staatssecretaris van Financiën en de minister van Defensie over de rapporten van de auditdienst rijk (ingezonden 30 december 2015). Beantwoording werd uitgesteld http://www.tweedeka mer.nl/kamerstukken/kamervragen/detail?id=2015Z25355&did=2016D02139

Koppeling met externe bestanden levert juridische vragen op. De dienst zegt terughoudend te zijn, en daarbij behalve de wettelijke grenzen, ook de grenzen van maatschappelijke aanvaardbaarheid in acht te nemen. 'We zouden natuurlijk ook graag even de registraties van boten willen koppelen, maar dat kan niet zo gemakkelijk.'[101]

Eigen veiligheidsventiel

Spanningen over het delen en vorderen van data door de Belastingdienst treden met enige regelmaat op. Bijvoorbeeld vanwege maatschappelijk verzet tegen het verplicht afstaan van kentekenbestanden door parkeerbeheerders.
De Belastingdienst won een rechtszaak hierover. Deze vordering van kentekens ging de directie van de Belastingdienst echter te ver en het 'programma' is inmiddels stopgezet. Dat was een zelfstandig besluit zonder politieke inbreng of controle.

In een vraaggesprek antwoordde de directeur op vragen over ongebreideld datagebruik: 'Precies om die reden heb ik een veiligheidsventiel ingebouwd. Wij gebruiken voor het opstellen van risicoprofielen alleen gegevens die wij al in huis hebben. Alcoholconsumptie of zoekgedrag zijn geen onderdeel van de fiscale informatie die wij al hebben.'[102]
De Belastingdienst gebruikt externe data niet voor profilering, maar wel voor speurwerk. Zo fungeren er afdelingen met eigen speurbevoegdheden zoals het Internet Service Centrum.

– Op de vraag naar bewaartermijnen van gecombineerde bestanden en 'hits' zegt de Belastingdienst dat ze zich houdt aan de regels van de Archiefwet. De archiefwet kent geen privacyprincipes. De gegevens mogen zo lang bewaard worden als fiscaal relevant wordt geacht, wat een periode van zeker vijf jaar kan belopen, maar ook zeven jaar.

– In een artikel van *De Correspondent* uitten de professoren Theo de Roos, Guido de Bont en Gerrit-Jan Zwenne zich in kritische termen over de mogelijkheden voor de Belastingdienst om bestanden en op de (gerechts)persoon gerichte inlichtingen van andere partijen te betrekken en om eigen data te verstrekken aan derden.
'We hebben een monster gecreëerd', aldus De Bont over de mogelijkheden tot uitwisseling van data tussen de Belastingdienst en derden. De dienst werd ook

101 Interview met Cyprian Smits, Belastingdienst.
102 Directeur Belastingdienst over Big Data: 'Mijn missie is gedragsverandering', 21 april 2015, De Correspondent https://decorrespondent.nl/2720/Baas-Belastingdienst-over-Big-Data-Mijn-missie-is-gedrags verandering/83656320-f6e78aaf

in de vraaggesprekken voor dit onderzoek gezien als een draaischijf voor data voor fraudebestrijding.
Het Besluit SUWI maakt verdergaande uitwisseling mogelijk. Zo mag de Belastingdienst meer externe koppelingen maken die nodig zijn voor risicoprofilering.
Zwenne stelt dat wetgeving onvoldoende is toegesneden op de grenzeloze mogelijkheden om op bestanden data-analyse toe te passen voor risicobepaling, patroonherkenning en uiteindelijk profilering van personen en bedrijven die lang mee gaat.
Dit kan leiden tot omkering van bewijslast: personen en bedrijven zijn eerder en langer verdacht op grond van data en moeten het tegendeel bewijzen. Volgens Zwenne moet in nieuwe belastingwetgeving ook paal en perk worden gesteld aan 'blanco volmachten' van de Belastingdienst en de samenwerkingsverbanden waarvan ze de spil vormt.[103]

– De Algemene Rekenkamer en Auditdienst Rijk waren kritisch over de gebrekkige beveiliging van data en systemen van de Belastingdienst op onderdelen. De dienst vormt een single point of failure, een groeiend risico voor privacyschending bij systeemlekken.[104]

Ook de bevoegdheden van vaste medewerkers en losse krachten van buiten vormen een aanhoudend privacyrisico van de groeiende databerg. Dit risico wordt door de dienst onderkend en er wordt actie op ondernomen, aldus de Belastingdienst.[105]

Parlementaire vragen

In oktober 2014 zijn vragen gesteld in de Eerste Kamer na een publicatie in *De Correspondent*.[106] Daarin reageerden hoogleraren verbaasd op suggesties dat de Belastingdienst ver gaat in informatieverstrekking aan politie, OM en inlichtingendiensten. Minister Opstelten van VenJ en staatssecretaris Wiebes van Financiën antwoordden met een weergave van artikelen 67 van de Algemene wet inzake rijksbelastingen (AWR), dat voorziet in verstrekking van data bij strafvorderingen.

---

103 Vergeet de politiestaat. Welkom in de belastingstaat, 30 september 2014, De Correspondent https://decorrespondent.nl/1766/Vergeet-de-politiestaat-Welkom-in-de-belastingstaat/54315096-f35e98af

104 Hoe veilig zijn onze gegevens bij de Belastingdienst? 30 september 2014, De Correspondent https://decorrespondent.nl/1838/Hoe-veilig-zijn-onze-gegevens-bij-de-Belastingdienst-/56529528-6f10861f

105 Interviews met Cyprian Smits en Nicole Back, Belastingdienst.

106 De Correspondent:
Zie https://decorrespondent.nl/1841/De-Belastingdienst-als-databank-voor-OM-Politie-en-Inlichtingen diensten/56621796–863e993b https://decorrespondent.nl/1766/Vergeet-de-politiestaat-Welkom-in-de-belastingstaat/84550499440–7a67098f

Het tweede deel betrof een verwijzing naar de convenanten die de Belastingdienst publiceert.
In artikel 43c van de Uitvoeringsregeling AWR staan de partijen genoemd waaraan gegevens mogen worden verstrekt en met welk doel. In 'Hoofdstuk 10a. Geen geheimhoudingsplicht', vervat in Artikel 43c staat een zeer uitgebreide opsomming van instanties, voornamelijk overheden, die aanspraak mogen maken op data van de Belastingdienst.[107] Convenanten vormen slechts een uitwerking van die wettelijke basis voor de uitvoeringspraktijk, aldus de minister van VenJ.
Volgens het kabinet voldoet de Belastingdienst volledig aan de plicht om burgers te informeren welke gegevens over hen worden verzameld en opgeslagen, daar er melding van wordt gemaakt bij de Autoriteit Persoonsgegevens en de 'functionaris gegevensbescherming'.
Bovendien staan er folders op belastingdienst.nl en op rijksoverheid.nl. en zijn de convenanten over gegevensverstrekking door de Belastingdienst gepubliceerd op de website. Dit volstaat volgens het kabinet. De minister beweerde bovendien het volgende: 'Als de Belastingdienst gegevens verzamelt bij de burger zelf, zoals bij het invullen van de aangifte inkomstenbelasting, is voor de burger duidelijk welke gegevens worden gevraagd en voor welk doel. Ook is het recht op inzage van eigen gegevens van toepassing.'[108]
De burger wordt, aldus het kabinet, op voortreffelijke wijze geïnformeerd over de Big Data-uitwisseling, zoals de miljarden gefotografeerde kentekens van de ANPR-camera's langs snelwegen. De minister: 'De Belastingdienst ontvangt ook gegevens van andere organisaties. Dat is vastgelegd in wettelijke bepalingen. Daarvoor geldt geen aparte informatieverplichting. De burger die dat wil, kan over die wettelijke grondslag informatie krijgen.'
Het OM kan behalve via vorderingen, ook data verkrijgen via eerder genoemde samenwerkingen. Volgens de minister is dat wettelijk gedekt, wat door het Hof Arnhem-Leeuwarden is bekrachtigd. Het ging om vervolging van een drugshandelaar wegens witwassen op grond van onder meer met het OM op grond van een convenant gedeelde belastingdata.[109]

Enkele weken daarna stelde ook TK-lid Gesthuizen (SP) vragen aan de minister van VenJ en de staatssecretaris van Financiën over uitwisseling van persoonsgegevens door de Belastingdienst met AIVD, politie en justitie. De antwoorden kwam gro-

107 Uitvoeringsregeling Algemene wet inzake rijksbelastingen, Hoofdstuk 10 http://wetten.overheid.nl/BWBR0006736/2016-01-01#Hoofdstuk10

108 Brief van minister van VenJ Opstelten en staatssecretaris van Financiën Wiebes aan de Eerste Kamer, 3 oktober 2014 https://www.rijksoverheid.nl/documenten/kamerstukken/2014/10/04/berichtgeving-over-verzamelen-gegevens-door-belastingdienst-en-uitwisselen-met-andere-overheidsinstanties

109 Vonnis Hof Arnhem-Leeuwarden 8 november 2013 http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:GHARL:2013:8478

tendeels overeen: volgens het kabinet voorzien de belastingwetgeving en convenanten in de legitimering van de uitwisseling. Dat is ook nodig ten behoeve van 'bestuurlijke en geïntegreerde aanpak van georganiseerde criminaliteit'.
De beschikbaarheid van 'alle informatie die nodig is' wordt van zwaarwegend belang geacht door de vragende instantie. Werkelijke toepassingen zijn ook in dit geval, zoals met de meeste data-uitwisseling besproken in deze bijdrage over data-analyse en fraudebestrijding, onbekend. Wel het aantal strafrechtelijke vorderingen van het OM bij de Belastingdienst voor specifieke verdenkingen: vijfduizend in 2013.
De Belastingdienst mag op haar beurt alle persoonsgegevens opvragen als die voor de belastingheffing, uitkering van toeslagen of douane- en overige wettelijke taken nodig zijn. Volgens het kabinet is het toezicht van de Autoriteit Persoonsgegevens afdoende en volstaat de capaciteit om aan haar taken uitvoering te geven. Er is geen actieve handhaving, maar optreden bij melding van ernstige, structurele overtredingen van de privacywet die grote groepen mensen treffen en waarbij inzet van AP-bevoegdheden een verschil kan maken.
Volgens Gesthuizen kunnen de AIVD, het OM en de politie dankzij verregaande bevoegdheden van de Belastingdienst (door artikel 43c van de Uitvoeringsregeling Algemene wet inzake rijksbelastingen 1994) alsnog aan persoonsgegevens komen die ze zelf niet mogen verzamelen dan wel bewaren.
Minister Opstellen ontkende dit niet. 'Van belang hierbij is dat de Belastingdienst alleen de fiscaal relevante gegevens bewaart. De uitwisseling met de Belastingdienst is legitiem en geen achterdeur. De Belastingdienst verstrekt deze gegevens uitsluitend aan andere instanties indien daarvoor een wettelijke grondslag bestaat. In het kader van het convenant vindt dat, zoals reeds eerder gememoreerd, bovendien alleen plaats binnen de doeleinden van samenwerkingsverbanden.'[110]
Ook de (voormalige) TK-leden Schouw (D66) en Oosenbrug (PvdA) oefenden kritiek uit op de minister van VenJ en de staatssecretaris van Financiën gezien de gebrekkige transparantie aangaande de uitwisseling van persoonsgegevens door de Belastingdienst.
Het antwoord van de minister luidde: 'De convenanten die zijn afgesloten met de AIVD, politie en OM zijn uitsluitend een uitwerking binnen de grenzen van die wettelijke basis voor de uitvoeringspraktijk. Er bestond dus geen aanleiding deze convenanten aan uw Kamer te doen toekomen.'
Ook antwoordde het kabinet dat de Belastingdienst het principe 'Selecteer voor je verzamelt en houdt het sober' ten algemene wordt toepast bij het verwerken van gegevens in het kader van de uitvoering van zijn taken, zo ook bij het vastleggen van ANPR-gegevens. 'De voertuigpassagegegevens worden alleen opgeslagen en

110 Antwoord van Minister Opstelten (VenJ) en staatssecretaris Wiebes (Financiën) op vragen van Kamerlid Gesthuizen (SP) van 30 oktober 2014, over uitwisseling van persoonsgegevens tussen Belastingdienst, AIVD, politie en justitie, 24 november 2014) https://zoek.officielebekendmakingen.nl/ah-tk-20142015- 645.html

bewaard, als blijkt dat ze fiscaal relevant zijn. Als dat niet het geval is, worden de gegevens direct verwijderd.'
De politie voert in het systeem referentielijsten in waarop de kentekens staan van personen die bijvoorbeeld een boete moeten betalen of die worden gezocht in verband met een misdrijf. Uitsluitend deze 'hits' worden bewaard en gebruikt.
Volgens de Autoriteit Persoonsgegevens schendt automatische kentekenregistratie van alle passanten op de Nederlandse wegen de privacy van vele burgers, want noodzaak, subsidiariteit of proportionaliteit zijn niet aangetoond. Volgens het kabinet is dit niet het geval.[111]

De Belastingdienst heeft op haar website een brochure gepubliceerd waarin duidelijk wordt gemaakt welk rechten een burger in dit opzicht heeft, zoals het recht op inzage van zijn gegevens en het correctierecht.
Van deze laatste rechten kunnen in principe alle ruim 12 miljoen zakelijke en privébelastingplichtigen gebruikmaken.[112]

4.4 BELEID EN TOEKOMST

Informatiegestuurd werken
Privacy-afwegingen maakt de Belastingdienst naar eigen zeggen veelvuldig, maar ze ontbreken naganoeg in de halfjaarrapportages van de Belastingdienst. Daarentegen is het enthousiasme groot over de successen van data-analyse als belangrijkste onderdeel van informatiegestuurd werken.
Staatssecretaris Eric Wiebes verwoordde dit in overleg met de commissie-Financiën van de Tweede Kamer op 8 oktober 2014 als volgt: 'Veel van het gut feel van die ervaren inspecteur is nu gemoduleerd en halen wij nu uit data-analyse op een manier waar zelfs de meest ervaren inspecteur misschien niet altijd tegenop kan.' Dit informatiegestuurd werken past de Belastingdienst volgens Wiebes vooral toe bij particulieren en het MKB met 'echt massale data-analyse, op basis van steekproeven en ervaringsgetallen'. Het effectiefste instrument in de handhaving is vol-

111 Antwoorden van de minister van VenJ en de staatssecretaris van Financiën op vragen van de (voormalige) TK-leden Schouw (D66) en Oosenbrug (PvdA) van 3 november 2014 over de uitwisseling van persoonsgegevens door de Belastingdienst, AIVD, politie en Justitie, 18 november 2014
https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2014/11/21/bijlage-2014z19545-antwoorden-op-kamervragen-over-uitwisseling-persoonsgegevens/bijlage-2014z19545-antwoorden-op-kamervragen-over-uitwisseling-persoonsgegevens.pdf

112 De Belastingdienst en de Wet bescherming persoonsgegevens (Wbp)
http://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/themaoverstijgend/brochures_en_publicaties/de_belastingdienst_en_de_wet_bescherming_persoonsgegevens

gens de Belastingdienst de vooraf ingevulde aangifte, waarmee controle vooraf plaatsgrijpt.[113]

Van het breder nadenken over controle en fraudebestrijding met data wordt in het 15e halfjaarrapport van de Belastingdienst, over de tweede helft van 2014, melding gemaakt van toenemende fraudebestrijding aan de 'voorkant', bij de aanvraag of de aangifte, in plaats van achteraf: 'Hierbij wordt steeds meer gebruikgemaakt van data-analyse. Door aanvullende selecties en analyses worden risicovolle posten beoordeeld en geselecteerd. Deze detectie wordt vroeg in het proces uitgevoerd, zodat wordt voorkomen dat ten onrechte betalingen op (voorlopige) aangiften plaatsvinden.'[114]

Reorganisatie rond data

De Belastingdienst wil het gebruik van grote databestanden de komende jaren opvoeren ten behoeve van patroonherkenning en hanteren van risico-indicatoren voor het corrigeren van aangiften en opsporen van fraude. Alle datagerelateerde werkzaamheden komen samen onder regie van de Raad van Bestuur.
De staatssecretaris van Financiën presenteerde in mei 2015 een Brede Agenda of Investeringsagenda voor de Belastingdienst, met een reikwijdte van zes tot acht jaar voor totale omvorming van de dienst. Daarin is sprake van de sporen A (vereenvoudiging stelsel), C (operationeel en transparantie) en B (ICT en data). Over de laatste schrijft hij uitvoerig: 'Er is een ontwikkelfilosofie voor de ICT opgesteld, een gegevensinfrastructuur (de 'datalaag') ontwikkeld en gebouwd, een team van specialisten (de 'broedkamer') heeft proefgedraaid met een informatiegestuurde aanpak, de online-aangifte is gelanceerd en het herontwerp van de massale processen is onderweg.' Dit is de beschreven broedkamer voor data-analyse.

Interne dataverzameling is moeilijk, aldus de bewindsman, vanwege benodigde informatie uit verschillende systemen, zoals voor een boekenonderzoek bij een onderneming tot wel 26 in totaal. 'Er zijn afdelingen waar medewerkers gegevens uitlezen uit het ene systeem en intikken in het andere.'
Deze informatiehuishouding is gebaseerd op processen en voor elk proces is destijds een systeem gebouwd. De nieuwe structuur brengt de data bijeen per belastingplichtige. Technisch is het formeren van een 'datalaag' gebaseerd op standaar-

113 'Verslag van een algemeen overleg, gehouden op 8 oktober 2014, over Belastingdienst' Nummer 2014D39685, 4 november 2014
http://www.tweedekamer.nl/kamerstukken/verslagen/detail?id=2014Z17150&did=2014D39685

114 15e Halfjaarsrapportage Belastingdienst, 26 maart 2015
http://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2015Z05518&did=2015D11192

den waarmee de data vanuit verschillende systemen samengebracht worden. Zo ontstaat per 'subject' een dossier c.q. profiel.
'Deze ontsluiting van de gegevens is de moeder van alle andere veranderingen. De Belastingdienst is daar nu klaar voor – het spel kan beginnen. Informatiegestuurd toezicht en inning…', aldus de staatssecretaris.
'Het systeem' selecteert vervolgens op basis van die honderden gegevens per belastingplichtige de grootste risico's op onjuistheden in de aangiften. Al vanaf het najaar 2014 is hiermee proefgedraaid op 'echte' bestanden met belastingplichtigen. De bewindsman: 'En de resultaten waren verbluffend. Niet alleen de trefkans ligt aanzienlijk hoger, het systeem geeft ook de aard van het risico aan, en de behandeltijd door de medewerker gaat aanzienlijk omlaag.'
In de inning hetzelfde beeld van grote successen dankzij risicoanalyse op bijeengebrachte data: 'Het systeem selecteert de meest kansrijke
debiteuren, ontmaskert oninbaar geachte vorderingen en adviseert te nemen maatregelen. De opbrengsten per medewerker spríngen omhoog.'
En zo heeft de Belastingdienst volgens de bewindsman ervaren dat de prestaties op vrijwel alle fronten sterk verbeterd worden door de toepassing van diepgaande data-analyse.[115]

In de rapportage van de Belastingdienst over het eerste halfjaar van 2015 is de voortgang weergegeven.[116] Zo heeft voor het segment Particulieren de broedkamer een nieuw risicomodel ontwikkeld. Dit leidt tot betere selectie van te controleren onderdelen van aangiften (aandachtsgebieden). Dit zou tot meeropbrengsten leiden. Het behandelen van twee aandachtsgebieden is in Eindhoven en Den Haag beproefd. Medewerkers krijgen alle benodigde informatie op één scherm beschikbaar. Voorheen moesten ze data in vier verschillende schermen opzoeken. De broedkamer ontwikkelt het risicomodel verder, en begon een volgende proef in Amsterdam.
Tevens is het aantal systemen waaruit data getrokken kunnen worden verder uitgebreid, alsmede de capaciteit voor data-analyse. Handhaving wordt verbeterd en kosten gereduceerd, aldus de bewindsman.
Een groot aantal transactiesystemen is nu ondertussen ontsloten:
– inkomstenbelasting;
– omzetbelasting;
– bezwaar;

115 Brief over de uitwerking Brede Investeringsagenda Belastingdienst van Staatssecretaris Wiebes van Financiën aan de Tweede Kamer, 20 mei 2015
https://www.rijksoverheid.nl/documenten/brieven/2015/05/20/brief-over-de-uitwerking-brede-agenda-belastingdienst

116 16e Halfjaarrapportage van de Belastingdienst, 16 september 2015
https://www.rijksoverheid.nl/documenten/kamerstukken/2015/09/16/16e-halfjaarsrapportage-van-de-belastingdienst

– klantregistratie;
– vennootschapsbelasting;
– auto;
– loon;
– betalingsverkeer;
– incasso.

Alle andere relevant geachte systemen komen erbij. De informatielagen vanuit de data geproduceerd, worden doorontwikkeld om actueler en completer beelden te verkrijgen van risico's.

Verantwoording moeilijk

De nieuwe digitaal gestuurde werkwijze leidt ertoe dat de politieke verantwoording ('accountability') van de Belastingdienst ook verandert en voortaan de volgende onderwerpen behelst:

1. interactie met burgers en bedrijven;
2. informatiegestuurd toezicht en inning;
3. ontwikkeling data-analyse;
4. sturing, verantwoording en effectmeting;
5. ondersteuning door informatievoorziening.

Echter, het is moeilijk voor de Belastingdienst om rekenschap te geven van de gevolgen en resultaten van de Investeringsagenda, aldus de staatssecretaris: 'Het leggen van een eenduidige relatie in de systemen tussen investeringen, activiteiten en ontvangsten blijkt nog lastig. Dit vereist nadere analyse.'
Deze constatering is boeiend in het licht van de voorspelde voordelen die vanaf 2020 gaan optreden en die door het internationale adviesbureau zijn bekrachtigd. Hoe worden die hardgemaakt? Immers, het data- en ICT-spoor kost meer geld dan beoogd, maar zal ook meer opleveren volgens de staatsecretaris. Hij geeft de term 'businesscase' mee, gezien de rendabele (extra) investering. De plannen zijn doorgelicht door mondiaal adviesbureau Oliver Wyman.
Deze bevestigt dat de totale stapsgewijze investering van 1,1 miljard euro de komende vijf jaar vanaf 2020 zo'n 750 miljoen euro aan extra belastinginkomsten oplevert. Nog afgezien van de kostenbesparingen aan personeel van zo'n 300 miljoen euro per jaar. Dit zijn afgeronde bedragen met een vooruitziende blik van vijf jaar. Wat het 'nulpunt' is op basis waarvan het resultaat over vijf jaar gemeten kan worden, is niet openbaar.[117]

117 Brief over de uitwerking Brede Investeringsagenda Belastingdienst van staatssecretaris Wiebes van Financiën aan de Tweede Kamer, 20 mei 2015
https://www.rijksoverheid.nl/documenten/brieven/2015/05/20/brief-over-de-uitwerking-brede-agenda-belastingdienst

De Rekenkamer vraagt zich af de Belastingdienst in staat zal zijn om deze investeringen en beoogde besparingen en opbrengsten juist te kunnen toerekenen. De Rekenkamer was recent zeer kritisch over de opbrengsten van de extra investeringen van de dienst in het programma Intensivering toezicht en invordering, dat het bestrijden van fiscale fraude, wanbetaling en het witwassen tot doel had.[118]
Het heeft in 2013 en 2014 minder opgeleverd dan was beoogd. Zwaarste kritiek betreft het gebrek aan goede verantwoording. Er werd uiteindelijk 61 miljoen minder binnengehaald dan gepland, maar de investeringen leverden volgens de eigen boekhouding van de dienst wel aanzienlijke winst op. Volgens de Rekenkamer zijn diverse maatregelen en projecten niet of niet zo bedrijfsmatig uitgevoerd als werd aangekondigd. 'Organisatorisch is er het nodige misgegaan.' De Tweede Kamer noch het ministerie van Financiën is juist geïnformeerd. De minister van Financiën antwoordde te verwachten dat met de inzet van data-analyse de invordering van de Belastingdienst effectiever zal worden. Het meten van het nalevingstekort zal deel uitmaken van de monitoring van de Investeringsagenda.

Nabije toekomst

Ook in 2016 worden nieuwe modellen ontwikkeld. 'Echter, aangezien het innovaties betreft die zich niet laten voorspellen, kunnen we geen uitspraken doen over nieuwe producten. Daarnaast vindt doorontwikkeling plaats van de reeds eerder genoemde producten, zodat deze binnen de hele organisatie worden ingezet.'

Met welk doel en welke verwachte opbrengst?
'Doel is om meer opbrengst te genereren voor de schatkist, tegen lagere kosten voor de samenleving en een hogere medewerkertevredenheid.'[119]

Tegen welke grenzen loopt de Belastingdienst aan met de uitbreiding van data-analyse? 'Binnen de kaders die de wet en de maatschappij stellen, is nog veel ruimte voor nieuwe producten. De benodigde expertise om deze producten te ontwikkelen is schaars beschikbaar op de markt. Daarom heeft de Belastingdienst een intern opleidingstraject op het vlak van data-science en worden specifieke externe experts betrokken met ervaring bij andere belastingdiensten.'[120]
De ontwikkeling van inzichten en producten vindt plaats in samenwerking met verschillende marktpartijen, die expertise en ervaring inbrengen van uit buitenlandse belastingdiensten.

---

118 'Intensivering toezicht en invordering bij de Belastingdienst - Voorbeeld van een 'business case' bij de rijksoverheid', 11 februari 2016
http://www.rekenkamer.nl/Publicaties/Onderzoeksrapporten/Introducties/2016/02/Intensivering_toe zicht_en_invordering_bij_de_Belastingdienst

119 Idem.

120 Idem.

Samenwerking buitenland

België vormt een voorbeeld. Volgens de betrokkenen heeft data-analyse de btw-fraude van naar schatting 1,1 miljard euro per jaar teruggebracht naar 48 miljoen dankzij het 'Hybride Detectie Model'. Dat is gestoeld op signalen in het systeem en analyse van (sociale) netwerken.
Opening van een vestiging in Panama door een Belg geeft bijvoorbeeld een signaal, maar ook subtiele verandering van bedrijfsnamen. Dit zelflerende systeem, dat wil zeggen dat resultaten tot verfijning van indicatoren leidt, heeft nu acht typologieën van fraude opgeleverd, met elk een andere combinatie van indicatoren.
Op grond van de signalen uit data-analyse zoekt de eenheid volgens op de naam van de persoon, adressen, nummers et cetera om potentiële btw-fraudenetwerken in kaart te brengen. Vroeger kostte dit weken, nu eerder uren of zelfs minder.
Nederland loopt achter op België en loopt volgens een woordvoerder van de dienst Menno Griffioen zo'n 2 miljard euro per jaar aan btw mis door onjuiste aangiften, waaronder btw-fraude. Dat is circa 5 procent van de totale opbrengsten.[121]

Verbeterslagen bij fraudebestrijding vinden in toenemende mate internationaal plaats, in samenwerking met voorlopers als bijvoorbeeld de Britse en Belgische Belastingdienst, en meer en meer ook met andere diensten.
Mondiale samenwerking is het doel, opgezet via de Organisatie voor Economische Samenwerking en Ontwikkeling (OECD), die de nationale analysediensten bundelde in een forum voor kennisuitwisseling. Internationale samenwerking is primair gericht op vernieuwingen met het doel van elkaar te leren. Zo werd in september 2015 het tweejaarlijkse Forum on Tax and Crime van de OECD in Amsterdam gehouden, met veel aandacht voor voorspellende modellen en data-analyse. Het programma 'Analytics: Exploiting big data to fight tax crimes and other financial crimes' had sprekers uit Singapore, Australië en Ierland.[122]

Vergezicht: ondeugende kinderen en gedragsmeting

De 'kleuterjuffrouw' wist precies welke kinderen 'lief' of 'ondeugend' in welke omstandigheden en in welke interactie waren met welk andere kinderen, en paste daar haar toezicht op aan. Facebook kan uit onze keuzes en gedrag op het scherm exacte portretten van zijn klanten samenstellen. Dit perspectief lonkt ook voor de Belastingdienst.
De staatssecretaris liet de Tweede Kamer weten: 'Een inspecteur, hoe ervaren ook, stuit met deelinformatie op beperkingen. Met massale data-analyse, op basis van

121 'Btw-fraudeurs opgespoord met big data', Cyriel van Rossum, 29 april 2015
http://ibestuur.nl/magazine/btw-fraudeurs-opgespoord-met-big-data
122 Tax Crime Forum 2015 Outcomes Statement
http://www.oecd.org/tax/crime/forumontaxandcrime.htm

zeer grote hoeveelheden beschikbare gegevens, wordt de trefkans aanzienlijk hoger.'[123]

Directeur Hans Blokpoel van de Belastingdienst wil Big Data op naam inzetten om een 'geïntegreerd beeld' van het historische gedrag van iedere belastingplichtige te krijgen. Elke 'cliënt' bouwt een imago op uit de interactie met de dienst. Daar kunnen ze op hun beurt ook voordeel uit halen, zo belooft de dienst dat patronen teruggekoppeld worden naar belastingplichtigen: bijvoorbeeld personen die in een scheiding liggen, worden geattendeerd op de problemen die dit kan opleveren met aangiften.[124]

In feite vindt ook een profilering per aangever plaats en deze bepaalt de mate van controle. Dat kun je aangeven in kleuren en code, net als het KNMI zulks doet met het weer. Daarin worden globaal drie hoofdcategorieën onderscheiden van beoordeling:

1. Mensen die jaar in, jaar uit, voldoen aan hun verplichtingen, zullen verder zo min mogelijk bemoeienis van de Belastingdienst ervaren.
2. Degenen die zonder opzet fouten maken, krijgen hulp en/of voorlichting aangeboden.
3. Degenen die met opzet de Belastingdienst verkeerde informatie verschaffen, worden op de huid gezeten.[125]

In de praktijk zal de categorisering veel gedifferentieerder zijn dan drie kleuren en uiteindelijk kunnen leiden tot een steeds meer individuele behandeling van klanten.
En iedereen wordt er beter van volgens de staatssecretaris van Financiën: 'Doordat de Belastingdienst de belastingplichtige nu beter kent en begrijpt, krijgt elke burger en elk bedrijf vervolgens de behandeling die hij verdient.'
Deze categorisering leidt ook tot een profiel: een persoon of rechtspersoon te kwader of te goeder trouw? Deze profilering moet actueel blijven met aanhoudende steekproeven. Bepaalde patronen geven duidelijk een vergissing aan. Anderen

123 https://www.rijksoverheid.nl/documenten/brieven/2015/05/20/brief-over-de-uitwerking-brede-agenda-belastingdienst
(5 januari 2016).

124 'Directeur Belastingdienst over Big Data: 'Mijn missie is gedragsverandering', 21 april 2015, De Correspondent https://decorrespondent.nl/2720/Baas-Belastingdienst-over-Big-Data-Mijn-missie-is-gedrags verandering/83656320-f6e78aaf

125 Interviews met Cyprian Smits, Nicole Back, Belastingdienst.

tonen onomwonden bewust bedotten aan. Uiteraard is er een grijs gebied daartussen, waar dat minder duidelijk is. Aldus de dienst in een toelichting.[126]

De Belastingdienst die per aangever een dossier c.q. een profiel bijhoudt van alle aangiften en betalingen over een groot aantal jaren, krijgt een veelomvattend beeld van het gedrag van burgers, dat wil zeggen de individuele belastingmoraal, die van families, straten, wijken, steden, per leeftijd, leefsituatie et cetera.
Daar profiteert niet alleen de dienst zelf van, maar ook alle partijen die binnen en buiten convenanten van deze data gebruik kunnen maken in vele varianten.
Bovendien krijgt de dienst, al dan niet in ruil, zelf veel aanvullende data, zoals over auto's op snelwegen.

Zonder dit beeld te opperen of de datamoloch nader te specificeren werd in een interview met algemeen directeur Hans Blokpoel de term Big Brother opgeworpen. Blokpoel spreekt het vermoeden tegen:
'Het leeuwendeel van wat we doen, is gegevens die we al lang in huis hebben, veel beter gebruiken. Wij zijn er niet op uit om zomaar zoveel mogelijk te willen weten. We zetten ook niet achter iedere belastingplichtige een inspecteur. Zo'n maatschappij zijn we niet. We hoeven geen Big Brother te zijn om dit werk te kunnen doen […] Want ik kan van alles over jou zien in de data, maar uiteindelijk hebben we nog steeds die presumptie van onschuld.'
Blokpoel zegt ook dat de intuïtie van de inspecteurs belangrijk blijft: 'Intuïtie zal altijd onderdeel van het vak blijven […] En ik hoop dat ik ook in de toekomst heel goede inspecteurs heb met een goede intuïtie.'[127]

Het beeld per klant werd tot kort opgebouwd uit ingediende aangiften, betalingen et cetera. Met het online invullen van aangiften kan de dienst ook gedrag realtime gaan volgen. De betrokken manager van de Belastingdienst schreef in zijn motivatie van het Fraude Expertisecentrum voor de Manifestgroep een boeiend detail:
'We bekijken stap-voor-stap hoe fraude kan worden gepleegd, bijvoorbeeld al bij het invullen van een formulier.'[128]
Met de aangifte Inkomstenbelasting over 2014 hebben miljoenen Nederlanders voor het eerst via Mijn Belastingdienst in 'the cloud' hun data verstrekt. Niet alleen ontvangt de Belastingdienst daarmee digitaal het resultaat van

126 Brief over de uitwerking Brede Investeringsagenda Belastingdienst van Staatssecretaris Wiebes van Financiën aan de Tweede Kamer, 20 mei 2015 https://www.rijksoverheid.nl/documenten/brieven/2015/05/20/brief-over-de-uitwerking-brede-agenda-belastingdienst

127 Freek Blankena, "Belastingdienst zoekt heil in datalaag", iBestuur.nl 14 oktober 2015 http://ibestuur.nl/nieuws/belastingdienst-zoekt-heil-in-datalaag (5 januari 2016).

128 http://www.digitaleoverheid.nl/actueel/buzz-tour/fraudepreventie/buzz-blog-frans-bentvelsen , geraadpleegd februari 2015, niet meer online.

de aangifte, maar kan zij nu ook eventueel inzicht verwerven in het proces dat tot dit resultaat leidt.
Zo is vast te leggen op welke wijze het formulier wordt ingevuld, maar ook zijn verschillende opgeslagen versies beschikbaar voor de Belastingdienst; waar en op welk tijdstip, hoe lang en met welke mate van twijfel invulling plaatsgrijpt.
Zo kunnen patronen worden ontwikkeld en toegepast voor een bepaalde wijze van invullen, die kan samenhangen met de wil tot frauderen. Ook opgeslagen versies die niet officieel worden ingediend, staan de Belastingdienst ten dienste bij het speuren naar fraude.
Degenen die inkomsten of vermogen aanvankelijk wel invullen, maar uiteindelijk niet, zouden in beeld kunnen komen bij de Belastingdienst. En daarmee ook bij de vele partners die delen in de data en patroonherkenning van de dienst.

5 INLICHTINGENBUREAU

INLEIDING

Het Inlichtingenbureau (IB) functioneert sinds 2001 als knooppunt ofwel schakelpunt voor informatieoverdracht aan gemeenten en andere overheden. Dit met als doel verhoging van de efficiency in het bepalen en controleren van handelingen van instanties die besluiten nemen over uitkeringen en belastingen. Te denken valt daarbij bijvoorbeeld aan het bepalen of uitkeringen terecht worden verstrekt of juist potentiële ontvangers geld laten liggen, zoals huur- en zorgtoeslag. Het aantal afnemers van informatie groeit gestaag, en daarmee ook het aantal bestanden om te analyseren, zoals recent nog alle Box 1-gegevens uit de aangiften inkomstenbelasting.
Big Data wordt gekoppeld en geanalyseerd tot nu tien 'informatieproducten', zoals databundels voor een Rechtmatigheidscontrole Participatiewet. Het IB levert gemeenten en de SVB 'samenloopsignalen', die duiden op mogelijk onrechtmatige uitkeringen. Voor het Systeem Risico Indicatie voor fraudesignalering in projecten van de 'Interventieteams', dat in het volgende hoofdstuk uitgebreid aan bod komt, is het IB 'onderaannemer' of uitvoerder.

Het IB staat voor beheer, analyse en beveiliging van een enorme hoeveelheid persoonsgegevens. Hoe gaat het in de praktijk met de grote verantwoordelijkheid om? Hoe transparant is het werk en hoe wordt verantwoording afgelegd over onder meer privacy? Is Big Brother hier realiteit?
Dit hoofdstuk steunt op informatie uit interviews bij het IB in Utrecht en telefoongesprekken, aangevuld met door de woordvoerders geverifieerde informatie van inlichtingenbureau.nl

5.1 DOEL

Het IB is opgericht in 2001 door het ministerie van SZW, mede op initiatief van de VNG en Divosa (vereniging van managers van sociale diensten). Het IB verschaft gemeenten en andere overheden data enerzijds om te bepalen of personen die geld van de gemeente ontvangen, daar ook recht op hebben (rechtmatigheidscontrole) en anderzijds om te bepalen of ze geld laten liggen, zoals huur- en zorgtoeslag.
Als knooppunt ofwel schakelpunt voor informatieoverdracht heeft het IB in de loop der jaren extra taken op zich genomen. Afnemers van data zijn, behalve gemeenten, ook waterschappen, de Regionale Meld- en Coördinatiefunctie voortijdig schoolverlaters (RMC), Regionale Coördinatiepunten Fraudebestrijding (RCF), de SNG (stichting gerechtsdeurwaarders), het CJIB en de SVB.
Het doel van deze operaties is om de efficiency te verhogen in het bepalen en controleren van handelingen van instanties die besluiten nemen over uitkeringen en

verschillende soorten belastingen. Door automatisch en elektronisch te administreren, te routeren en te antwoorden worden administratieve lasten verlicht en de efficiency en effectiviteit van werkprocessen groter. Hiermee realiseert het IB volgens betrokkenen besparingen voor burgers, overheden en andere publieke partijen.

5.2 OPZET VAN SYSTEMEN

De opdrachten aan het IB groeien gestaag; er zijn inmiddels tien groepen zogenoemde 'informatieproducten'. De uitwisselingsfabriek produceert de navolgende producten:

- Dienstverlening SUWI (Structuur werk en Inkomen):
  1. Rechtmatigheidscontrole Participatiewet
  2. Digitaal klantdossier (DKD)
  3. Fraudebestrijding (Syri)
  4. Participatie & Re-integratie
  5. Armoedebestrijding
  6. Landelijke informatievoorziening Participatiewet
- Dienstverlening Zorg en Jeugdzorg
- Dienstverlening Onderwijs: Prioritering voortijdig schoolverlaters
- Dienstverlening Belastingen: Geautomatiseerde toets op kwijtschelding

Voorbeelden van enkele van de hieronder vallende 'producten' zijn:

1. Rechtmatigheidscontrole voor gemeenten (bijstand, IOAW en IOAZ) en de SVB (AIO) met gegevens van UWV, de Belastingdienst, DUO, de Justitiële Informatiedienst (JustID), CJIB, de RDW en andere gemeenten. Deze gegevens worden vergeleken met de gegevens van de uitkeringsgerechtigde zoals dan bij gemeenten of de SVB bekend zijn, bijvoorbeeld of het een buitenlandse gedetineerde of voortvluchtig veroordeelde betreft

Heffingskortingen als onderdeel van inkomen zijn de meest recente toegevoegde bestanden. Het IB kreeg van de Belastingdienst tot 2015 nog geen Box 1-gegevens inkomstenbelasting, maar sinds het eerste kwartaal van 2016 wel. Van het UWV komt de polisadministratie van actuele gegevens over dienstbetrekkingen. Van zelfstandigen zijn geen actuele inkomensgegevens bekend bij gemeenten en het IB. Gemeenten kunnen deze eventueel direct opvragen bij de Belastingdienst. In hoeverre dit ook wordt gedaan, weet het IB niet.
De aangiften inkomstenbelasting zijn niet actueel, want de processen en data van de Belastingdienst kunnen behoorlijk achter de feiten aanlopen.

Het resultaat van de controle levert het IB in de vorm van wat ze 'samenloopsignalen' noemt: signalen over omstandigheden die kunnen duiden op een onrechtma-

tig verkregen uitkering. Het IB geeft alleen aan dat een situatie onderzoekwaardig is, als suggestie.
Bij de nieuwste generatie signalen levert het IB een prioritering mee, een tag, die de signalen indeelt naar mate van onderzoekwaardigheid. De samenloopsignalen kunnen automatisch worden ingelezen in de meeste uitkeringsadministratiepakketten van de gemeenten om het werkproces te vergemakkelijken.
De signalen vormen samen de productgroep rechtmatigheidscontrole. Hiertoe behoren bijvoorbeeld ook signalen over direct uitgekeerde heffingskortingen en voertuigbezit. Het IB geeft signalen voor beoordeling van het recht op studiefinanciering, de overschrijding vermogensgrens, uitkering in andere gemeenten, detentie en voortvluchtig veroordeeld, inschrijving bij een hogeschool of universiteit, en een overzicht van bankrekeningen en saldi.

2. Landelijke verwijs- en routeerservice: een knooppunt voor de gegevensuitwisseling tussen gemeenten en andere partijen binnen het domein SUWI en de Participatiewet. Partijen kunnen via het IB gebruikmaken van de gemeentelijke verwijsindex, automatische antwoordservices en putten uit een centrale database. De gegevens die beschikbaar zijn, komen voort uit bestandskoppelingen en andere elektronische informatieverstrekking.
   Centraal staat het Digitaal Klantdossier (DKD), een gemeenschappelijk virtueel dossier waarin informatie gedeeld wordt op het gebied van werk en inkomen door UWV, SVB en gemeenten. Het DKD is ontwikkeld in het kader van de Wet eenmalige gegevensuitvraag (WEU), waarmee burgers voor de keten Werk en Inkomen maar eenmalig hun gegevens hoeven te verstrekken.

3. SyRI komt in hoofdstuk 6 uitgebreid aan de orde. Het IB is daarvoor 'onderaannemer'. In het kader van SyRI biedt het IB ondersteuning. In opdracht van de Inspectie SZW verzamelt het IB data waarmee risicoprofielen worden samengesteld. Dat doet het in een geanonimiseerde omgeving. Het IB stelt resultaten beschikbaar waarmee de data-analisten van de Inspectie SZW aan het werk gaan, nog zonder dat het gepersonaliseerd is, ze krijgen van het IB anonieme data.
   De Inspectie SZW heeft een eigen systeem voor data-analyse om signalen van fraude op te sporen, de Blackbox genoemd. Het IB deed al SyRI-achtige exercities vóór de wetswijziging tot stand kwam, in nauwe samenspraak met de Autoriteit Persoonsgegevens. Dat behelsde twee typen onderzoek: er is voor enkele wijken een risicoprofiel samensteld, te weten op basis van postcodes. En voor ondernemingen die een grote kans lopen op wetsovertredingen, zoals bepaalde uitzendbureaus. Het IB is de onderaannemer voor de uitvoering van projecten met bestandskoppeling van de Landelijke Interventieteams op grond

van SyRI. Het IB koppelt daartoe afhankelijk van het doel van het onderzoek maximaal zo'n 55 bronbestanden.

4. Kwijtschelding gemeentelijke en waterschapsbelastingen: verschaffing aan gemeenten en waterschappen van een overzicht van huishoudens aan wie kwijtschelding van gemeentelijke of waterschapsbelastingen kan worden verleend.

5. Participatie en Reïntegratie: gemeenten ondersteuning bieden met behulp van elektronische gegevensuitwisseling voor hun invulling aan taken die gericht zijn op het bevorderen van participatie en re-integratie van kwetsbare groepen in de samenleving.

6. Armoedebestrijding: voorzien in signalen die duiden op recht op voorzieningen en regelingen uit de sociale zekerheid waarvan geen gebruik wordt gemaakt. In sommige gevallen bleek tot bijna 70 procent van personen die recht op een bepaalde bijdrage hadden, daarvan geen gebruikmaakten. Net als bij de fraudesignalen betreft het suggesties waarbij een sociale dienst al dan niet actief betrokkenen benadert. Het IB bezit ook over deze categorie geen informatie over de ondernomen acties c.q. resultaten. Het IB verschaft bijvoorbeeld signalen over betalingsachterstand zorgpremie, het ontbreken van een zorgverzekering, onbenutte bijzondere bijstand 65-plussers, onbenutte huur- en/of zorgtoeslag en onbenutte kinderopvangtoeslag. Om gemeenten hierop zicht te bieden, wisselt het IB gegevens uit met de SVB, de zorgverzekeraars en de Belastingdienst.

7. Informatievoorziening Knooppuntdiensten maakt voor gemeenten, zorgaanbieders en andere ketenpartners het beveiligd uitwisselen van berichten over Wmo en Jeugdhulp mogelijk. Gemeenten kunnen berichten uitwisselen met zorgaanbieders die zijn aangesloten op het knooppunt van VECOZO.

Het huidige systeem heeft het IB zelf gebouwd, tot drie jaar geleden met een adviesbureau, eerst Capgemini, daarna HP. Het systeem voor rechtmatigheidscontrole is in eerste instantie door Cap gebouwd, daarna door HP herbouwd en daarna weer beheerd door Cap. Dat was het 'Sectorloketsysteem'. Het eigen systeem heet Ibis, Inlichtingenbureau Informatiesysteem. Dit wordt extern gehost. De vogel is het symbool.

Alle leveranciers van data leveren in verschillende formaten hun data aan, dus moeten er afspraken worden gemaakt voor het uniform verwerken in een database. Gemeenten leveren gegevens in StUF-formaat. UWV, Belastingdienst hebben hun eigen formaten, zoals XML. Het IB levert data aan gemeenten op BSN-nummers. De

data worden verzameld in maandelijkse rapportages, die gemeenten zelf kunnen ophalen.

5.3 UITVOERING

Het IB verzorgt rechttoe rechtaan koppelingen die gestructureerd en transparant zijn. Het krijgt gegevens van gemeenten over personen die een bijstandsuitkering genieten en matcht deze met bestanden van andere organisaties. Het IB verschaft gemeenten en de SVB de relevante overeenkomsten, hits, samenloopsituaties die mogelijk invloed hebben op het recht op bijstand. Vroeger ging een gemeente bij een aanvraag na of iemand recht had op bijstand en wat de hoogte van de uitkering zou moeten zijn. Daarna deden de gemeenten een periodieke toets, een arbeidsintensief proces. Dat is vervangen door een geautomatiseerd proces, dat continu op de achtergrond gemeenten informatie verschaft indien daartoe aanleiding is.

Een signaal komt in het algemeen tot stand, nadat in wetgeving is opgenomen dat een bepaalde omstandigheid het recht op bijstand blokkeert. Bijvoorbeeld: een jaar of drie geleden is in de Wet werken en bijstand (Wwb) opgenomen dat mensen die zich onttrekken aan een opgelegde gevangenisstraf geen recht hebben op bijstand. Een dergelijke aanpassing geeft voor het ministerie van SZW aanleiding het IB te vragen een signaal te creëren (een gegevensuitwisseling op te tuigen) waarmee het gemeenten erop kan wijzen dat een persoon die bijstand kreeg toegewezen, in het register van voortvluchtig veroordeelden staat geregistreerd. Indicatoren en risicoprofielen komen tot stand vanuit onderzoek. Een dergelijk onderzoek wordt uitgevoerd door de Inspectie SZW.[129]
Het IB kijkt dus met bestandskoppelingen of een uitkeringsgerechtigde naast de uitkering andere inkomsten heeft en geeft dit door aan gemeenten. Het nadeel hiervan is dat gemeenten elk signaal doorkrijgen, ook als het inkomen of vermogen al is verrekend met de uitkering. Het IB werkte aan het slimmer maken van deze signalen.

Voorbeelden van 'slimmere signalen' die in 2014–2015 beschikbaar kwamen:
- Bij signalen over vermogen geeft het IB door of iemand samenwoont.
- Bij signalen over inkomen levert het IB een indicatie van het nettoloon, zodat gemeenten snel een inschatting kunnen maken of het inkomen boven of onder de WWB-norm valt.
- Gemeenten krijgen elke maand een lijst van bankrekeningnummers van bijstandsgerechtigden. In de nieuwe situatie wordt gemarkeerd of er sprake is van een nieuw of een gewijzigd bankrekeningnummer.

129 Interview met Paul Schaafsma en Jan-Peter Bergfeld, Inlichtingenbureau.

Er liepen ook twee proeven:
- In de pilot opsporen buitenlandse gedetineerden zijn gegevens van Nederlandse gedetineerden in het buitenland vergeleken met die van uitkeringsgerechtigden.
- In de pilot bestandskoppeling landelijk register kinderopvang en peuterspeelzalen (LRKP) zijn de gegevens van bijstandsgerechtigden vergeleken met gegevens van gastouders en werknemers in de kinderopvang.[130]

De uitkomst van de proeven is als volgt: van Nederlandse gedetineerden in het buitenland wordt inmiddels standaard nagegaan of ze een lopende bijstandsuitkering hebben. Is dit het geval, dan wordt via het IB de betreffende gemeente geïnformeerd.
De pilot bestandskoppeling LRKP leverde onvoldoende nuttig resultaat op om tot landelijke uitrol over te gaan. Dit was met name vanwege het geringe aantal samenloopgevallen in combinatie met het feit dat de informatie meestal al bekend bleek bij de gemeente en ook geen betrekking had op het feitelijk genieten van inkomsten, maar alleen op het geregistreerd staan.

Het IB voegt steeds nieuwe 'tags' toe aan de signalen. Een 'tag' is in feite een labeltje met contextinformatie over een hard gegeven. Bijvoorbeeld: vanuit een bestandskoppeling met de RDW ontvangt het IB informatie dat een bijstandsklant een voertuig op zijn naam heeft staan. Dit geeft aanleiding de gemeenten hierop te attenderen. Het IB kan op basis van de meegeleverde informatie bepalen hoe oud het betreffende voertuig is, en wat de mogelijke waarde is.
Het IB combineert ook. Dus als het IB vaststelt dat een persoon over een aantal maanden een aantal oude voertuigen tijdelijk op zijn naam heeft gehad, dan geeft elk afzonderlijk voertuig wellicht weinig aanleiding nader onderzoek te starten, maar het feit dat de betreffende persoon gedurende een bepaalde periode kort verschillende voertuigen op zijn naam heeft gehad weer wel.

Niets blijft overigens anoniem. Het gaat wel anoniem door de molen of 'wasstraat', maar de resultaten van de risicoprofielen worden gekoppeld aan BSN-nummers. Het risicoprofiel bestaat uit een groot aantal met elkaar in verband gebrachte indicatoren. Als een bijstandsgerechtigde voldoet aan die indicatoren en daarmee een potentieel risico biedt op frauduleus gedrag, worden de geanonimiseerde gegevens gekoppeld aan personen.
Ze zijn dan nog geen verdachten, maar worden in een hokje geplaatst. Het is een bescheiden deel van de onderzochte populatie. Het IB levert het gegeven af dat er

130 Monitoren van de Fraudewet en rapportage fraudeaanpak en handhaving, 17050-474, 26 mei 2014
L.F. Asscher, minister van SZW, aan de Voortouwcommissie SZW van de Tweede Kamer Misbruik en oneigenlijk gebruik op het gebied van belastingen, sociale zekerheid en subsidies.

een dure auto is gekocht en dat dit aanleiding kan zijn voor een onderzoek naar vermogen.
Anderzijds is de auto op zich geen relevant signaal. 'De helft van de uitkeringsgerechtigden heeft ook een auto, maar dan moet je eerder denken aan een Pandaatje van 12 jaar oud dan aan een BMW van drie jaar oud. Wij geven ook het signaal mee: besteed hier minimale aandacht aan of juist: dit is een indicatie voor nader onderzoek.'[131]
Voor bijvoorbeeld voertuigen ligt dat niet vast. Er komt een lange beslisboom voor bepaling van relevante waarden bij kijken waarvan de criteria samen met de diensten Handhaving van de gemeenten zijn opgezet. Op grond daarvan geeft het IB in dit geval labels mee van mogelijk vermogen. 'Een Porsche is per definitie een auto die een signaaltje krijgt, Rolls Royce, Mercedes of BMW ook wel; auto's die je niet verwacht bij bijstandsgerechtigden.'[132]
Zo'n dure-autolijst wordt periodiek nagelopen om die te herijken en vervolgens in het systeem bij te werken. Daartoe komen gemeentelijke afnemers met het IB bijeen voor expertbijeenkomsten: enige malen per jaar en ten minste één keer per jaar.

Met het BKWI, beheerder van Suwinet, vindt afstemming plaats. Dit bureau coördineert de verstrekking van informatie aan vragende partijen. Bij het BKWI moet je voor inzage een BSN intikken. Dat is ook handig om direct alle relevante gegevens in te zien. Gemeenten kunnen echter niet dagelijks voor elke WWB-klant kijken of er gewijzigde omstandigheden zijn.
Het IB en het BKWI hebben niet dezelfde bestanden, maar wel dezelfde databronnen. Ze delen soms bestanden, bijvoorbeeld gegevens over banksaldi van uitkeringsgerechtigden ('vermogenssignalen') die het IB aan gemeenten verstrekt.

5.4 RESULTATEN

Het IB verstrekt gemeenten maandelijks voor nu 350.000 WWB-uitkeringen de signalen van mogelijke fraude vanuit analyse van gekoppelde databestanden. In het (niet openbare) jaarverslag 2014[133] worden de volgende aantallen nieuw verschafte signalen aan gemeenten voor de rechtmatigheidscontrole WWB genoemd (afgerond):

131 Interview met Paul Schaafsma en Jan-Peter Bergfeld, Inlichtingenbureau.
132 Idem.
133 Idem.

– heffingskortingen: 230.000
– dienstverbanden: 101.000
– SVB-uitkeringen: 86.000
– vermogen: 59.000
– voertuigbezit: 108.000
– sofinummercontrole: 100
– detentie: 8.700
– voortvluchtig veroordeeld: 700
– interne samenloop: 11.000
– recht op studiefinanciering: 1.200

Volgens het IB betreft zeker 80 procent van de verstrekte signalen informatie die reeds bij gemeenten bekend is. Immers, verreweg de meeste bijstandsklanten houden zich aan de informatieplicht om gewijzigde omstandigheden die van belang zijn voor de WWB-uitkering zelf te melden, volgens het IB.
Een deel vergeet het, een deel geeft het moedwillig niet op, en dat laatste wordt met de IB-signalen grotendeels rechtgezet. Dit resterende deel duidt niet per se op onrechtmatigheid. Daarvoor is nader onderzoek nodig, bijvoorbeeld met een uitnodiging van de persoon voor een gesprek met de Sociale Dienst. Sommige gemeenten zijn er strikt in en nemen direct een maatregel (boete), anderen zijn er coulanter in. Daarop heeft het IB geen enkele invloed. Het IB bepaalt nooit of een samenloop bewust handelen als oorzaak heeft of per ongeluk.
Maar het IB zegt: 'De stelling dat een bijstandsgerechtigde beter wordt gecontroleerd dan een gemiddelde belastingplichtige willen wij van harte onderschrijven.'[134]

5.5 HINDERPALEN EN VRAAGTEKENS

Big Brother-imago

Het IB staat voor beheer, analyse en beveiliging van een enorme hoeveelheid persoonsgegevens. Er ontstaat daardoor eenvoudig een imagoprobleem, te meer daar de term 'Inlichtingenbureau' direct afkomstig lijkt uit '1984' of gelijksoortig doemscenario met grootscheepse privacyschending.
'Negen van de tien keer als mensen in aanraking komen met het IB moeten we wel uitleggen dat het niet de geheime dienst is en we niet aan fraudebestrijding doen, maar een proces hebben geautomatiseerd om de rechtmatigheid van uitkeringen te onderzoeken. Dat is nog niet schimmig of crimineel, maar een gewoon proces dat hoort bij het aanvragen van een voorziening bij de gemeente. Van meet af aan heerst de opvatting bij publiek dat wij fraudebestrijding doen.'[135]

134 Idem.
135 Idem.

Het IB werd in 2015 genomineerd voor een 'Computable Award' voor het Gemeentelijk Gegevensknooppunt als beste ICT-project van het jaar bij de overheid. Maar dat is voor technisch kunnen van de koppelingen en draagt eerder bij aan de doem dan dat het er afbreuk aan doet. Het IB heeft dan ook een naamswijziging overwogen, maar deze niet doorgevoerd. Het kiest in plaats daarvan voor meer transparantie over bestanden en activiteiten ('producten') op de website. Naar eigen zeggen van het IB: 'We zijn niet geheim, maar we voeren ook geen publiciteit met jaarlijkse advertenties.'[136] Transparantie is overigens begrensd. Jaarverslagen van het IB zijn niet (meer) publiek.

Privacy-afwegingen

Het IB vindt het lastig dat er zoveel meer mogelijk is met gegevens koppelen. The sky is the limit. 'Zonder privacybescherming zou je veel meer kunnen doen. Maar dan komt de politiestaat wel erg dichtbij.' Dit ervaart het IB eerder als probleem dan als voorrecht. 'We betwijfelen of het werkelijk helpt. Om aan die initiële informatiebehoefte die veel te ruim is te geraken tot een informatiebehoefte die gerechtvaardigd is en ondersteunend, is een ingewikkeld en langdurig proces.'[137] Met de Autoriteit Persoonsgegevens heeft het IB regelmatig overleg. 'Wij hebben het privacyhart op de goede plaats. De Autoriteit Persoonsgegevens wil graag informatie van ons krijgen over wat er speelt. Waar ben je mee bezig? Waar loop je tegenaan? Ze zijn tevreden over de transparantie die wij betrachten.'[138]

In feite moeten de afnemers (gemeenten) als gebruikers van de datasignalen zich afvragen of ze binnen privacygrenzen blijven, maar het IB moet hen regelmatig te hulp schieten bij het maken van de afwegingen, gezien de ervaring van het bureau met veel afnemers. Het gaat met gemeenten in gesprek om hen te helpen de juiste afwegingen te maken. Dat vond in de afgelopen jaren veelvuldig plaats.
De meest actuele vraag komt voort uit de wens van gemeenten om te werken met een 'integrale dienstverleningsbenadering': per persoon/gezin willen gemeenten weten wat er speelt en op welke gronden behoefte is aan welke hulp. Dat is ook een doel van de decentralisatie van zorgtaken vanuit de Rijksoverheid. Gemeenten zijn verantwoordelijk voor jeugdzorg, werk en inkomen en zorg aan langdurig zieken en ouderen op grond van de Jeugdwet, Participatiewet en Wmo.
Het ligt voor de hand dat gemeenten dan ook allerlei informatie willen verzamelen omtrent een aantal leefgebieden (inkomen, schulden, huisvesting, gezondheid, overlast, etc.) van een persoon en/of gezin. Wet- en regelgeving vereist dat het IB per geval nagaat welke gegevens van welke bron voor welk doel op welke wijze en onder welke randvoorwaarden mogen worden gebruikt.

136 Idem.
137 Idem.
138 Idem.

Het is maatwerk. Volgens het IB gaat de discussie altijd over wat vanuit maatschappelijk belang zou moeten mogen, tegenover wat nu feitelijk mag. De gedachte is vaak, aldus het IB, dat oplossingen zich vanzelf zullen gaan aandienen, zodra maar eerst kan worden beschikt over een ruime gegevensverzameling. Wetgeving dwingt gegevensverwerkers echter precies andersom te denken, zo moet het IB haar afnemers regelmatig voorhouden.
De privacywet begrenst de gegevensverzameling aanzienlijk. Doelbinding, proportionaliteit, subsidiariteit zijn dan de breinbrekers waar veel gemeenten op vast lopen. 'Bijvoorbeeld met de decentralisatie van Jeugdzorg doet de gemeentelijke sociaal regisseur zijn entree, met keukentafelgesprekken over verschillende aspecten van leefsituatie en behoefte aan zorg en ondersteuning.
Dan ontstaat bij gemeenten de gedachte dat deze personen hun werk beter kunnen doen als ze niet naar gegevens hoeven te vragen, maar op pad gaan met een dossier met reeds bekende data.' Heel begrijpelijk volgens het IB, maar daar voorziet de wet niet in.
Wil de sociaal regisseur voor initiële, en volgens gemeenten essentiële, informatie inzage in relevante databanken en bestanden, bijvoorbeeld om een gezin beter te kunnen ondersteunen, dan loopt deze al snel aan privacyrecht van diezelfde wetgever.
Dat mag een gemeente niet zien als een beperking, maar zij dient dit te beschouwen als een recht van hulpbehoevenden. Zelfs als deze 'cliënten' er niet op zitten te wachten om aan de keukentafel wederom – en soms moeizaam – allerlei feiten op te lepelen of uit schoenendozen te halen die bij de gemeente al lang bekend zijn.
Soms stuit ook proactief beleid voor armoedebestrijding op deze privacygrens: gemeenten willen data verzamelen en combineren over mensen met een laag inkomen om te bepalen wie er voor hulp, een regeling of voorziening in aanmerking komen en die nog niet krijgen.
Deze data kan het IB wel leveren, maar mag dat niet.
Wel is er een proef gedaan om hiertoe bestanden van de Belastingdienst te koppelen, met vrijstelling van het ministerie van Financiën. Het resultaat van deze test was echter negatief; de hoogte van het belastbaar inkomen bleek een slechte indicatie van actuele armoede van huishoudens.

5.6 TOEKOMST

Momenteel speelt de vraag hoe het IB eerder data kan verstrekken, niet pas als de uitkering is toegewezen, maar reeds tijdens het aanvraagproces van de uitkering. Het IB wil ook het burgerservicenummer dan direct ontvangen, zodat het die aanvraag kan ondersteunen. Het IB kan met haar signalen van 'samenloop' de besluitvorming van gemeenten om een aanvraag al dan niet toe te kennen ondersteunen. Nu beschikken gemeenten vaak niet over alle informatie die voorhanden is.

De tweede kwestie is hoe het IB gemeenten met minder persoonsgegevens toch de juist informatie kan bieden, dus de relevantie van de signalen weet te verhogen. Niet meer gegevens, maar slimmer, effectiever en veiliger. Een voorbeeld: nu worden nog maandelijks alle bankrekeningnummers van personen met bijstand aan gemeenten verstrekt. Als gemeenten dat zelf bijhouden, kan volstaan worden met signalen van louter nieuwe bankrekeningen.

Op de vraag naar Big Datatoepassing zegt het IB dat dit afhangt af van de gehanteerde definitie van Big Data. De gegevensverwerking voldoet aan twee van de drie genoemde factoren van Gartner (hoeveelheid en snelheid). Maar met name de laatste factor (diversiteit) bepaalt of er sprake is van Big Data: analyse van ongestructureerde bergen data, dus nog zonder vooruit bedacht beperkt informatiedoel. Oftewel grote hoeveelheden data verzamelen en analyseren, op zoek naar trends die een voorspellende waarde hebben. Dat laatste doet het IB niet en er zijn ook geen voornemens om dit te gaan doen.
'Het IB werkt niet met ongestructureerde bergen data en er dient altijd een vooraf geformuleerd en gerechtvaardigd doel te zijn volgens de privacywet. Het bedenken van doelen voor ongestructureerde data-analyse, zoals dat plaatsvindt bij SyRI, laten we over aan de voor Syri verantwoordelijke minister van SZW. Wij verlenen hand- en spandiensten bij de uitvoering. Overigens is het ook bij Syri noodzakelijk dat vooraf een specifiek doel is geformuleerd waartoe het belang van de verantwoordelijke redelijkerwijs strekt.
Dit is een generieke beperking van de mogelijkheden van datamining met persoonsgegevens. Als de data waarop analyses worden uitgevoerd, niet terug te voeren zijn op specifieke personen geldt deze beperking uiteraard niet. Maar dat doen we niet uit eigen beweging.'[139]

139 Idem.

6 SYRI EN LSI

INLEIDING

Begin 2004 is voor socialefraudebestrijding de Landelijke Stuurgroep Interventieteams (LSI) opgericht onder (destijds nog) staatssecretaris Rutte van Sociale Zaken, met als deelnemers: UWV, Belastingdienst, de SVB, SIOD en Arbeidsinspectie (nu beiden deel van de Inspectie SZW), het OM, de VNG en Divosa. Data-analyse is een van de middelen.
De voorloper van het Systeem Risico Indicatie (SyRI) voor bestandskoppeling werd onder de naam 'Black Box' jarenlang toegepast voor het speuren naar fraude met uitkeringen, belastingen en toeslagen, faillissementen, arbeidsvoorschriften et cetera zonder afzonderlijke wettelijke grondslag maar wel binnen de regels van de Wet bescherming persoonsgegevens.
Dat onttrok zich grotendeels aan de openbaarheid. Pas de verankering in de wet door minister Asscher en de Tweede Kamer (zonder stemming, dus unaniem) leidde tot beschuldiging van SyRI als Big Brother-achtige opsporingsmethode.
In hoeverre is dit gerechtvaardigd? Hoe uitgebreid en intensief wordt gebruikgemaakt van SyRI en hoe werkt dit in de praktijk, wat wordt er aan data ingebracht en wat levert dit op? Dat komt in dit hoofdstuk gedetailleerd aan bod.

6.1 WETTELIJKE BASIS

Per 1 januari 2013 is de Wet aanscherping handhaving en sanctiebeleid SZW van kracht, bekend als de Fraudewet, gericht op fraudebestrijding in het sociale domein door gemeenten, de SVB en het UWV. Deze verplicht onder meer om bij geconstateerde gebreken in informatieplicht een boete op te leggen aan uitkeringsgerechtigden.[140] Een logisch vervolg was het Wetsvoorstel Fraudeaanpak door Bestandskoppelingen van minister Asscher van SZW. Dat werd zonder stemming aangenomen.[141] Per 1 januari 2014 is daartoe de Wet Structuur Uitvoeringsorganisatie Werk en Inkomen (Wet SUWI) gewijzigd. Een van de wijzigingen betreft de toevoeging van de artikelen 64 en 65. In artikel 64 is geregeld dat de in dit artikel aangewezen overheidsorganen (de colleges van B&W van gemeenten, het UWV, de SVB, de Inspectie SZW en de Belastingdienst) in een samenwerkingsverband data mogen uitwisselen om op te treden tegen misbruik van sociale voorzieningen en inkomensafhankelijke regelingen, belasting- en premiefraude en het niet-naleven van arbeidswetten. Zo kan op basis van risicoanalyses worden bepaald bij welke

140 http://wetten.overheid.nl/BWBR0032087/geldigheidsdatum_30-12-2015
141 Wetsvoorstel tot wijziging van de Wet SUWI en enige andere wetten in verband met fraudeaanpak door gegevensuitwisselingen en het effectief gebruik van binnen de overheid bekend zijnde gegevens (Kamerstuk 33 579).

personen of bedrijven het grootste risico op regelovertreding aanwezig is. Daarnaast werden nieuwe bestandskoppelingen mogelijk, zoals data van gedetineerden in het buitenland bij uitvoerders in de sociale zekerheid, alsmede informatie over gastouders aan bijstandsdata. Indien dit samenwerkingsverband van UWV, Inspectie SZW c.s. data wil laten verwerken voor risicoanalyse moet het de minister van SZW verzoeken om de betreffende gegevens te verwerken in SyRI. De minister bepaalt of het verzoek wordt gehonoreerd en blijft leidend in de procedure. De bestuursorganen of personen verstrekken de databestanden officieel aan de minister van SZW. Voor deze verwerking is het genoemde SyRI ontworpen. De voorwaarden waaronder dit systeem kan worden toegepast, zijn uitgewerkt in een Algemene maatregel van bestuur, het Besluit SyRI. Dit is op 12 september 2014 in werking getreden.[142]

De techniek die in het instrument SyRI een wettelijke basis heeft gekregen, werd overigens ook vóór de inwerkingtreding van de wettelijke regeling al in de praktijk ingezet. De aanleiding tot de ontwikkeling van deze techniek was project 'Waterproef' (soms ook vermeld als 'Waterproof', zie ook hoofdstukken 8 en 10): waterverbruik, gemeten door nutsbedrijven, werd gekoppeld aan adressen van uitkeringsgerechtigden.
In die fase (2008-2010) stond deze techniek bekend als de genoemde 'Black Box'.[143] Het systeem werd zo genoemd, omdat er bij de uitvoering conform de technische voorwaarden geen gegevens bekend zouden kunnen worden van burgers die niet als risicovol werden aangemerkt.
De risicoanalyse is door de toenmalige SIOD (later Inspectie SZW) ontwikkeld en toegepast. De Black Box was de basis voor het instrument SyRI. In de Wet SUWI kreeg dit in een nieuw artikel 65 de wettelijke verankering ten behoeve van integraal overheidsoptreden ter voorkoming en bestrijding van uitkerings-, belasting- en premiefraude en het niet-naleven van de arbeidswetten.[144] Genoemde partijen zetten bestandskoppelingen in om samenhangende misstanden te kunnen onderkennen en om de pakkans te verhogen. SyRI omvat de technische infrastructuur en procedures om in een beveiligde omgeving pseudoniem data te koppelen en analyseren, teneinde risicomeldingen (op naam) te genereren. Een risicomelding bete-

142 Besluit van 1 september 2014 tot wijziging van het Besluit SUWI in verband met regels voor fraudeaanpak door gegevensuitwisseling en het effectief gebruik van binnen de overheid bekend zijnde gegevens met inzet van SyRI https://zoek.officielebekendmakingen.nl/stb-2014-320.html

143 In de Memorie van Toelichting http://www.tweedekamer.nl/kamerstukken/detail?id=2013D10967

144 Wijziging van de Wet structuur uitvoeringsorganisatie werk en inkomen en enige andere wetten in verband met fraudeaanpak door gegevensuitwisselingen en het effectief gebruik van binnen de overheid bekend zijnde gegevens.
http://www.tweedekamer.nl/kamerstukken/wetsvoorstellen/detail?id=2013Z05142&dossier=33579

kent dat een rechtspersoon of natuurlijke persoon een bepaalde kans wordt toegedicht op frauduleus handelen, onrechtmatig gebruik en niet-naleving van wetgeving. Deze werkwijze moet leiden tot een meer effectieve en efficiënte inzet van het controleapparaat.

Voor verwerking in Syri komen de volgende categorieën data in aanmerking:
a. arbeidsgegevens, over verrichte werkzaamheden;
b. gegevens inzake bestuursrechtelijke maatregelen en sancties, zoals boetes;
c. fiscale gegevens van natuurlijke personen en rechtspersonen;
d. bezit van roerende en onroerende goederen;
e. gegevens over uitsluitingsgronden van bijstand of uitkeringen;
f. handelsgegevens van rechtspersonen en bestuurders;
g. huisvestingsdata;
h. identificerende data: naam, adres, woonplaats, postadres, geboortedatum, geslacht en administratieve kenmerken en bij een rechtspersoon: naam, adres, postadres, rechtsvorm, vestigingsplaats en administratieve kenmerken;
i. inburgeringsdata;
j. nalevingsdata, over overtredingen;
k. (financiële) onderwijsdata;
l. pensioendata;
m. data re-integratieverplichtingen;
n. data schulden;
o. uitkerings-, toeslagen- en subsidiedata, de financiële ondersteuning;
p. data over verleende vergunningen en ontheffingen, zoals bouwvergunningen;
q. zorgverzekeringsdata, dat wil zeggen louter om te bepalen of een persoon is verzekerd.

Definities:
indicator: een gegeven dat de aanwezigheid van een bepaalde omstandigheid aannemelijk maakt;
risicomelding: de melding, bedoeld in artikel 65, tweede lid, van de Wet SUWI;
risicomodel: een model dat bestaat uit vooraf bepaalde indicatoren en aangeeft of er sprake is van een verhoogd risico op:
– onrechtmatig gebruik van overheidsgelden en overheidsvoorzieningen op het terrein van sociale zekerheid en de inkomensafhankelijke regelingen,
– belasting- en premiefraude, of
– het niet-naleven van arbeidswetten;

Voorbeelden van relevante bronnen:
- Gegevensuitwisseling gedetineerden in het buitenland;
  Vermogen in het buitenland (Belastingdienst, Internationaal Bureau Fraude-informatie IBF);
- Gegevenslevering nutsbedrijven en woningverhuurders. In de projecten Waterproof is aangetoond dat gegevens van nutsbedrijven een effectieve en doelgerichte indicator voor adres- en leefvormfraude kunnen zijn voor gemeenten en het SVB. Deze fraudegevallen zouden zonder nutsgegevens niet zijn ontdekt. De aanname is dat bij een zeer laag waterverbruik op een adres (minder dan 10 m3 per jaar) sprake is van een feitelijk niet-bewoond adres en daardoor mogelijk van verzwegen samenwoning elders, met uitkeringsfraude en huurtoeslagfraude als gevolg.

Aangezien een volwassen persoon gemiddeld 45 m³ water per jaar verbruikt, is het aannemelijk dat er bij een zeer hoog verbruik (meer dan 70 m³) meerdere personen op het adres wonen. Daarnaast kunnen ook de gegevens van woningbouwcorporaties over de tenaamstelling van huurcontracten en betalingsgegevens een effectieve indicator zijn voor samenwoonfraude.

- Gegevensuitwisseling Registers kinderopvang en peuterspeelzaalwerk: Als een burger een uitkering ontvangt en daarnaast actief is als gastouder, houder is van een kindercentrum dan wel als zelfstandige zonder personeel inkomsten uit kinderopvang ontvangt, dan zijn de inkomsten van invloed op het recht op en de hoogte van de uitkering.
- Opschorten uitkering werknemersverzekeringen en volksverzekeringen in relatie tot inschrijving gemeentelijke basisadministratie persoonsgegevens.
- Uitbreiding gegevenslevering vanuit de polisadministratie aan pensioenuitvoerders, Sociale Verzekeringsbank en gemeenten

---

Met het besluit SyRI wordt fraudebestrijding met behulp van bestandskoppeling binnen de geldende privacywetgeving toegepast. Hiertoe worden data gebruikt die de betrokken partijen in de uitoefening van hun wettelijke taak verzamelen. Dit is ook in het belang van efficiency, aldus het kabinet. Gegevens die door de ene partij zijn uitgevraagd, de burger of werkgever, mogen niet door een andere partij opnieuw worden gevraagd: de gewenste administratieve lastenvermindering.

6.2 UITVOERING SYRI

Volgens het kabinet is sprake van een dringende maatschappelijke behoefte, ook wel pressing social need genoemd, om deze maatregelen door te voeren. Te weten de in 2011 vastgestelde 153 miljoen sociale zekerheidsfraude als gevolg van misbruik en misstanden beperken, zodat het maatschappelijk draagvlak voor de sociale zekerheid behouden bleef.

Het instrument SyRI heeft volgens betrokkenen een substantieel aandeel in de fraudebestrijding; in 2010 was de geraamde opbrengst van de afgeronde interventieprojecten ruim 23 miljoen euro. Er gaat bovendien een preventieve werking uit van handhaving. 'De unieke combinatie en de veelheid van openbare en gesloten bronnen waaruit geput kan worden met behulp van SyRI, de expertise die wordt opgebouwd met betrekking tot risicoprofielen en -analyses en de gepresenteerde samenhang van gegevens in de risicomelding, maken dat SyRI toegevoegde waarde heeft.'[145]

---

145 Wijziging van de Wet structuur uitvoeringsorganisatie werk en inkomen en enige andere wetten in verband met fraudeaanpak door gegevensuitwisselingen en het effectief gebruik van binnen de overheid bekend zijnde gegevens.
http://www.tweedekamer.nl/kamerstukken/wetsvoorstellen/detail?id=2013Z05142&dossier=33579

SyRI is volgens hen niet op de eerste plaats ontwikkeld om geld – genoemde bedragen - binnen te brengen maar om misstanden en misbruik aan te pakken zodat het draagvlak voor het systeem van sociale zekerheid behouden blijft.

Een verzoek om toepassing van SyRI mag alleen worden gedaan door een samenwerkingsverband van de partijen genoemd in artikel 64 SUWI: Colleges van B&W, het UWV, de SVB, de Belastingdienst en de Inspectie SZW. Een bestuursorgaan dat of persoon die op dit moment geen partij is bij de LSI kan eventueel tijdelijk voor de duur van het SyRI-project toetreden.
In de LSI zijn ook diensten en organen vertegenwoordigd (met name het OM en de politie) die met reden niet in artikel 64 SUWI zijn aangewezen. Het OM levert geen data, maar is betrokken in verband met eventuele strafrechtelijke onderzoeken die uit de controles van het interventieteam kunnen voortvloeien. Voor gebruik van politiegegevens is per project een apart besluit van de chef van de regionale eenheid noodzakelijk, op grond van de Wet politiegegevens (Wpg). Hiervoor is een modelbesluit opgesteld. Politiegegevens worden niet vooraf in de risicoanalyse betrokken.

Het risicomodel is een model dat bestaat uit vooraf bepaalde indicatoren die duiden op een verhoogd risico van fraude en misbruik. Bij het ontwerp van het risicomodel beschrijft de Inspectie SZW voor welke specifieke fraudevorm het instrument SyRI wordt ingezet en onderbouwt gemotiveerd welke gegevens daartoe bij elkaar worden gebracht.
Per project wordt daartoe op basis van de doelstelling van dat project bepaald welke gegevens nodig zijn om de doelgroep te identificeren en te onderzoeken. Elke organisatie die aan het project deelneemt, levert bestanden uit de eigen administratie aan. Toepassing van het instrument SyRI vindt in twee fasen plaats.

Fase 1: bestandskoppeling
Fase 1 behelst de bewerking van data door het IB, dat de bestandskoppeling uitvoert. Het IB koppelt daartoe, afhankelijk van het doel van het onderzoek, momenteel maximaal zo'n 55 bronbestanden, maar dit kan uitbreiden naar gelang de toekomstige behoefte. Het IB vult en beheert vervolgens twee bestanden:

A. Het eerste bestand (het bronbestand) bevat de gegevens die het samenwerkingsverband heeft aangeleverd. Persoons- en bedrijfsgegevens worden in dat bestand gepseudonimiseerd. Hierbij worden onder meer persoons- en bedrijfsnamen, burgerservicenummers en adressen vervangen door een code (een pseudoniem). Het IB legt dit bronbestand geautomatiseerd langs het in casu te hanteren risicomodel met indicatoren. Dit is opgesteld door de Inspectie SZW.
B. Het IB maakt ook een 'sleutelbestand' waarin is aangegeven welke persoons- of bedrijfsnaam, burgerservicenummer of adres bij een bepaald pseudoniem hoort. Wanneer bepaalde natuurlijke personen, rechtspersonen of adressen aan

de hand van het risicomodel als verhoogd risico worden aangemerkt, worden deze weer ontsleuteld aan de hand van het sleutelbestand.

Het IB ontsleutelt alleen die gegevens die op basis van de resultaten van de koppeling duiden op een verhoogd risico op onregelmatigheden.
Het IB vernietigt binnen vier weken de aan het IB geleverde bestanden en de door het IB bewerkte bestanden, inclusief de 'no-hits'.
Daarna worden alle gegevens die met de verhoogde risico's samenhangen, doorgeleid (officieel) 'aan de minister' ten behoeve van de tweede fase van de risicoanalyse door de analyse-eenheid van de Inspectie SZW. Die voert fase 2 uit.

Fase 2: analyse
Dit bestand met potentiële 'hits' wordt aan de afdeling Onderzoek & Analyse van de Inspectie SZW geleverd. De Inspectie SZW analyseert de gegevens van het bestand met de potentiële hits en bepaalt in welke gevallen deze tot een risicomelding leiden. De Inspectie levert de risicomeldingen of potentiële fraudegevallen aan de deelnemende partijen zoals UWV et cetera. Zij zijn verplicht om te onderzoeken of het echt gaat om fraude, voordat ze een sanctie treffen. Het OM en de politie kunnen voor zover er van vermeende criminaliteit sprake is, eveneens risicomeldingen ontvangen.

Register risicomeldingen
Er wordt een register risicomeldingen ingericht waarin de definitieve selectie van risicomeldingen wordt opgeslagen. Dit register heeft als doel projectdeelnemers en bestuursorganen te informeren over de risicomeldingen die zijn verstrekt en om subjecten van risicomeldingen op eigen aanvraag te informeren of zij in het register staan opgenomen.
De afdeling Onderzoek en Analyse van de Inspectie SZW (namens de minister) vernietigt eventueel resterende gegevens na terugkoppeling door de LSI-deelnemers uiterlijk twee jaar na aanvang van het SyRI-project. De vernietiging wordt vastgelegd in een proces-verbaal.

Terugkoppeling en evaluatie
De bestuursorganen en personen die risicomeldingen ontvangen hebben, geven binnen twintig maanden na de aanvang van het SyRI-project een terugkoppeling aan de afdeling Onderzoek & Analyse van de Inspectie SZW. Deze behelst de resultaten van de risicomeldingen: waren ze al dan niet nuttig en waarom wel/niet? Hiermee kan de effectiviteit van het risicomodel worden verhoogd.[146]

146 https://zoek.officielebekendmakingen.nl/stb-2014-320.html

6.3 TOEPASSING IN DE PRAKTIJK

Al vanaf begin 2004 zijn interventieteams op instigatie van (destijds nog) staatssecretaris Rutte ingezet. Data-analyse is een van de middelen. De samenwerking in de LSI brengt data samen van Inspectie SZW, gemeenten, de Belastingdienst, het UWV en de SVB. Afhankelijk van het onderwerp of de doelgroep van de controle wordt het Interventieteam onder leiding gesteld van een van de bovengenoemde organisaties.
De minister van SZW, in de persoon van de directeur van beleidsdirectie Stelsel & Volksverzekeringen, is belast met het voorzitterschap en het secretariaat van de LSI. De LSI richt zich op de aanpak en voorkoming van arbeidsgerelateerde fraude binnen het fiscale en het socialezekerheidsdomein en van overtredingen van de arbeidswetten (Wet arbeid vreemdelingen en de Wet Minimumloon en minimumvakantiebijslag). De Interventieteams richten zich op bepaalde branches/sectoren of (stedelijke) gebieden en pakken in de breedte misstanden aan: onderbetaling, schending van regels, misbruik van werknemers en -regelingen, belasting- en premiefraude, uitkeringsfraude, illegale tewerkstelling en de daarmee samenhangende misstanden.[147]
De Interventieteams onderzoeken branches en gebieden waar de kans op fraude groot is. De selectie vindt plaats op grond van tips en risicoanalyses gericht op subjecten met de hoogste trefkans.

Vanaf 2014 hanteert de LSI landelijke thema's waarbinnen projecten worden uitgevoerd: adresfraude, bewoning (recreatieterreinen, huisvesting arbeidsmigranten en wijkgerichte aanpak) en schijnconstructies. Tot en met het tweede kwartaal van 2015 zijn 161 projecten door de LSI goedgekeurd.
LSI-projecten richtten zich in de afgelopen jaren onder meer op gastouderbureaus, uitzendbureaus, schijnconstructies, arbeidsmigratie, recreatieterreinen en op probleemwijken, waarbij is gecontroleerd op fraude en op illegale tewerkstelling. Recent onderzochte wijken waren bijvoorbeeld Weesp-Noord, De Valuwe in Cuijk, Dauwendaele in Middelburg, de kern van Vaals en Meerzicht in Zoetermeer. Ook recreatieparken op de Noord-Veluwe, in West-Brabant, Hardenberg/Ommen, Maasdriel en Zundert waren in de afgelopen jaren onderwerp van onderzoek.

De aanpak van adresfraude is in recente interventieteamprojecten, zoals in de wijk Hoograven (Utrecht), ook een belangrijk thema geweest. Voorstellen voor projecten van deelnemers worden ter goedkeuring aan de LSI (Stuurgroep) voorgelegd.

147 Brochure: Controle door een Interventieteam, 2012
https://www.rijksoverheid.nl/documenten/brochures/2010/06/25/controle-door-een-interventieteam

Meer en meer vindt afstemming en samenwerking plaats met de Regionale Informatie en Expertise Centra (RIEC's), die lokale besturen ondersteunen in de aanpak van ondermijnende criminaliteit. De RIEC's ressorteren onder het ministerie van VenJ.
In de wijkgerichte projecten is het standaardpraktijk dat, wanneer het interventieteam bij de uitvoering van de controles vermoedt dat er sprake kan zijn van georganiseerde criminaliteit of hennepteelt, het RIEC in die regio wordt geïnformeerd. Indien nodig wordt ook het Bureau BIBOB geïnformeerd.
Voorbeelden: interventieteamprojecten G.A.L.O.P. I en II in Eindhoven ('Gerichte Aandacht Leefbaarheid Ondernemerschap Participatie'), de Valuwe in Cuijk, Recreatieparken Zundert, wijkgericht project Schiedam-Oost. In deze projecten is afgesproken dat signalen uit interventieteamcontroles die duiden op mogelijke banden met georganiseerde criminaliteit, aan het lokale RIEC worden overgedragen.
Op het thema adresfraude wordt ook samengewerkt tussen de LSI en het project Landelijke Aanpak Adreskwaliteit (LAA), dat in opdracht van het ministerie van BZK, door de ICTU (ministerie van BZK) wordt uitgevoerd.[148]

Voor 22 van de 160 projecten van de interventieteams tot nu toe gehouden vanaf 2008 t/m 2014 is gebruikgemaakt van de techniek voor bestandskoppeling en risicoanalyse van wat later SyRI werd. Van 21 daarvan vond in 2015 rapportage aan de Kamer plaats, het 22e project was op dat moment nog niet afgerond. De Autoriteit Persoonsgegevens is bij elk project geïnformeerd over gebruik en koppelingen van bestanden (zie bijlage 1).

Zo leverde het gastouderonderzoek in Midden-Nederland bijna 5,8 miljoen euro op, opgehaald met navorderingen en boetes bij dertig bureaus met 1325 gastouders en 1641 'vraagouders'.[149]
De rapporten van interventieteamprojecten bevatten geen informatie over de toegepaste bestandskoppelingen. Gegevens uit bestandskoppelingen worden nooit openbaar gemaakt, maar bij de Autoriteit Persoonsgegevens wordt gemeld welke soorten gegevens zijn gebruikt.
De risicoanalyse op het bestand van potentiële hits levert een aantal risicomeldingen op. Die worden in het register risicomeldingen opgenomen, alle overige gegevens worden vernietigd. Deze risicomeldingen moeten eerst nader worden onderzocht door het projectteam, voordat een sanctie kan worden opgelegd.

148 Interview met Jan Jenezon, secretaris van de Landelijke Stuurgroep Interventieteams (LSI).
149 Eindrapport Interventieproject Gastouderbureaus, Belastingdienst en Regionaal Platform Fraudebestrijding Midden-Nederland, maart 2012
http://www.rtlnieuws.nl/sites/default/files/content/documents/2015/04/14/eindrapportgastouders.pdf

Iedere burger kan infomeren of hij/zij in het register is opgenomen, actieve meldingen zijn er niet. (zie bijlage 2).

Het totaal aan opgelegde belastingaanslagen en boetes bedroeg: ruim 12 miljoen euro.
- Correcties op toeslagen (stopzetting en terugvordering): ruim 3 miljoen euro.
- Teruggevorderde en beëindigde uitkeringen (bijstandsuitkeringen en uitkeringen op grond van werknemersverzekeringen en volksverzekeringen) en opgelegde boetes: ruim 4 miljoen euro.
- Opgelegde boetes wegens overtreding van de Wet arbeid vreemdelingen en/of de Wet minimumloon- en minimumvakantietoeslag: ruim 1,5 miljoen euro.[150]

Het meest valt op dat de Black Box vóór de wettelijke verankering van het instrument SyRI in 22 projecten toegepast is, maar er in het eerste jaar erna geen ministeriële goedkeuring gevraagd is voor toepassing van SyRI voor onderzoeksprojecten.

In 2014 zijn geen nieuwe SyRI-projecten begonnen, vanwege andere prioriteiten dat jaar bij de LSI. Deze had voor dat jaar een aantal landelijke thema's vastgesteld, die zich niet (direct) leenden voor deze analysemethode.
Daarnaast is er per jaar beperkte capaciteit om op lokaal niveau een zogenoemde wijk- of gebiedsgerichte aanpak uit te voeren. SyRI leent zich momenteel niet voor toepassing in projecten waarin een van de landelijke thema's het onderwerp is.
Het belangrijkste risicomodel dat in SyRI is ingebouwd, heeft betrekking op risicoindicatoren die in de wijkgerichte aanpak kunnen worden toegepast. Wijkgerichte projecten kennen een lange voorbereidingstijd. Een gemeente moet bereid zijn om hierin te investeren en dat vergt lokale politieke afstemming.
Daarnaast kent SyRI een zogenoemd Ondernemingenmodel, dat kan worden ingezet om risicofactoren bij bedrijven te toetsen. Tot nu toe is dat niet ingezet, vanwege het ontbreken van daarvoor geschikte projecten.
Het Besluit SyRI is op 12 september 2014 in werking getreden. In de periode ervoor en erna lag voor de LSI de nadruk op projecten op een van de landelijke thema's.
Op dat moment (12/9/2014) was één wijkgericht project in uitvoering: De Valuwe in Cuijk. Dat is het in de Kamerbrief van 29 juni 2015 genoemde 22e project, waarvan de resultaten op dat moment nog niet bekend waren.
In het voorjaar van 2015 is het eerste voorstel voor een wijkgericht project ingediend waarin wordt verzocht om SyRI toe te passen: dat is het project G.A.L.O.P. II, uit te voeren in de wijk Bennekel-Oost en het bedrijventerrein De Greefstraat in

150 Brief rapportage over SyRI-projecten 29 juni 2015.
https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2015/06/29/kamer brief-met-rapportage-over-syri-projecten/kamerbrief-met-rapportage-over-syri-projecten.pdf

Eindhoven. Dit project is in juni 2015 door de LSI goedgekeurd en is nu in uitvoering.
Een tweede project is inmiddels in voorbereiding voor onderzoek naar 'kwetsbare buurten in Capelle aan den IJssel. Het derde project met toepassing van SyRI had een onderzoek naar adresfraude in de Afrikaanderwijk in Rotterdam moeten worden, maar dat is geschrapt in verband met het ontbreken van analysecapaciteit. Hiervoor komt een ander project in de plaats.

6.4 PRIVACY

In reactie op de afkeuring van de aanvankelijke methode met de toepassing Waterproef door de Autoriteit Persoonsgegevens onstond Black Box en vervolgens SyRI. Daarmee kan in een beveiligde omgeving data gepseudonimiseerd worden gekoppeld en vervolgens de 'risico's' op fraude worden geanalyseerd.
Pseudonimiseren, is, anders dan anonimiseren, een techniek waarmee de identiteit van een persoon achteraf wel herleidbaar is. Dat is ook de bedoeling van SyRI: de personen met een hoog risico identificeren. is. Pseudonimiseren kan gedaan worden met een procedure waarmee identificerende gegevens met een bepaald algoritme worden vervangen door versleutelde gegevens (het pseudoniem). Pseudonimiseren onderscheidt zich van anonimiseren, waarbij het koppelen op persoon van informatie uit verschillende bronnen niet mogelijk is.[151]

De AP stelde in september 2006 een op de Wet bescherming persoonsgegevens (Wbp) gebaseerd toetsingskader voor bestandskoppelingen bij fraudebestrijding vast. Dit toetsingskader stelt dat in de fase van controle op mogelijke fraude gestructureerde koppeling van bestanden alleen mag plaatsvinden, indien daaraan een risicoprofiel ten grondslag ligt. In dit profiel zijn de risicoindicatoren op specifieke vormen van overtreding expliciet gemaakt.
SyRI voldoet hieraan.
'De proportionaliteit wordt gewaarborgd doordat deelnemende partijen voorafgaand aan elk project aan de Wbp toetsen welke gegevens noodzakelijk zijn voor het specifieke opsporingsdoel. Hierdoor wordt de inperking van het recht op privacy zo klein mogelijk gehouden', aldus minister Asscher.
De AP (toen CBP) plaatste in zijn advies bij het conceptbesluit SyRI hierbij vraagtekens.[152] Zo vereist artikel 8 van het EVRM dat wetgeving bepalingen bevat die regelen welke soorten data mogen worden verwerkt, de categorieën van personen die het betreft en de omstandigheden waaronder dit gebeurt.
De AP adviseerde om vooraf zoveel mogelijk inzichtelijk te maken welke selectie van persoonsgegevens wordt gemaakt. Echter, omdat de selectie van gegevens per

151 https://nl.wikipedia.org/wiki/Pseudonimiseren
152 Advies conceptbesluit SyRI
https://cbpweb.nl/sites/default/files/atoms/files/z2013-00969.pdf

samenwerkingsverband en per project verschilt, was het volgens de minister niet mogelijk om dit in de regelgeving voor alle individuele projecten uit te werken.
Het advies van de AP is daarop als volgt verwerkt: binnen SyRI worden alleen gegevens verwerkt als daar een wettelijke grondslag voor is. De proportionaliteit van de maatregel wordt gewaarborgd, doordat deelnemende partijen voorafgaand aan elk interventieproject toetsen welke gegevens noodzakelijk zijn voor het specifieke opsporingsdoel.
Bovendien is nu exact aangegeven ten behoeve van welke wetten SyRI kan worden ingezet en is in de wet de zinsnede verwijderd.
Hierdoor kan SyRI op basis van de voorliggende wet alleen worden ingezet voor preventie en handhaving binnen het domein van het ministerie van SZW en het ministerie van Financiën en kunnen alleen die gegevens in SyRI verwerkt worden die voor de doelstellingen binnen die domeinen noodzakelijk zijn.
Verder merkte de AP op dat, om te kunnen voldoen aan de wettelijke vereisten van doelbinding, de taken en verantwoordelijkheden van een nieuwe deelnemer dienen aan te sluiten bij het doel van de inzet van SyRI. Hierop is de wetstekst aangepast: data mogen enkel worden gebruikt voor het sociale domein.[153]

De AP wenste ook dataminimalisatie met *select before you collect:* eerst bepalen wat je nodig hebt, dan data selecteren. Anders zou het koppelen van bestanden kunnen leiden tot een *fishing expedition* en zelfs tot willekeur.
De AP en de Raad van State wilden dat de te gebruiken bestanden inzake SyRI in aantal beperkt zouden worden en in de wettelijke regeling zouden worden vastgelegd. Aangezien de selectie van benodigde gegevens per project verschilt, werd dit onpraktisch geacht.
In plaats daarvan is geregeld dat de Landelijke Stuurgroep Interventieteams voorafgaand aan elk project toetst of in het verzoek om toepassing van SyRI in dat project aan de daaraan in het Besluit SyRI gestelde voorwaarden is voldaan. Voorafgaand aan een samenwerkingsproject wordt afgewogen welke gegevens en indicatoren noodzakelijk zijn voor de bestandskoppeling. De deelnemers verstrekken louter data die daarvoor nodig zijn, aldus betrokkenen. Op deze manier moet worden gewaarborgd dat aan de in de regelgeving gestelde eisen wordt voldaan en dat de projecten zich richten op maatschappelijk relevante (fraude)thema's, aldus de minister van SZW.[154]

153 Advies Raad van State en Nader Rapport, blz. 3 en 4 (Kamerstuk 33 579, nr. 4).
Nota van Toelichting bij het Besluit SyRI (Staatsblad 2014, nr. 320, blz. 17-20)
https://zoek.officielebekendmakingen.nl/stb-2014-320.html

154 Misbruik en oneigenlijk gebruik op het gebied van belastingen, sociale zekerheid en subsidies, Vergaderjaar 2014–2015 Nr. 489 Brief Van De Minister Van Sociale Zaken en Werkgelegenheid aan de Tweede Kamer, Den Haag, 31 oktober 2014 http://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2014D39394

De AP adviseerde ook om de bewaartermijnen van SyRI aan te passen. Nu is vastgelegd dat de risicomeldingen en de bijbehorende gegevens uiterlijk na twee jaar uit SyRI worden verwijderd.
Er geldt ook een wettelijke geheimhoudingsplicht voor de instanties die over de risicomeldingen beschikken. Immers, een risicomelding ontstaat in de beveiligde omgeving van SyRI, maar komt buiten SyRI terecht. Gegevens die niet tot de definitieve selectie behoren, zullen direct worden vernietigd.
Aanvragers van uitkeringen worden gewezen op mogelijk gebruik van data in een bestandskoppeling, en dat derden, zoals de Belastingdienst, data kunnen gebruiken. Bij de voorgenomen evaluatie van de Wet SUWI in 2020 zal ook SyRI worden geëvalueerd. En de privacyaspecten in ogenschouw worden genomen. Er is reeds een Privacy Impact Assessment uitgevoerd.[155]

SyRI is in de media soms beschouwd als een ultieme aantasting van privacy, als de realiteit geworden Big Brother. Volgens betrokkenen is het tegendeel van het geval waar. Nu zijn er regels opgesteld die willekeur en onjuist datagebruik voorkomen. Althans voor wat betreft dit specifieke sociale domein.
Bovendien is de aansprakelijkheid bij misbruik, fouten en lekken nu helder en was het dat voorheen niet. De minister zelf moet toestemming verlenen voor de vergaande datakoppeling van het
Met Big Data-toepassing die met SyRI in het vizier komt, zou zorgvuldiger en neutraler met indicatoren worden omgegaan: 'Kon een inspecteur voorheen nog zeggen: "Bakkerij de Jong komt er niet uitrollen in de top-100 bedrijven van grootste frauderisico, maar die hoort er wel bij", dan kon hij naar eigen inzicht aanpassingen doen met het systeem. Dat wordt uitgesloten met SyRI. Die wasmachine biedt echt een geanonimiseerd proces.'[156]

155 Besluit SUWI, 1 september 2014
https://zoek.officielebekendmakingen.nl/stb-2014-320.html

156 Interviews met Hans Berkhout en Ad van Mierlo van VNG KHN.
Burger wordt straks doorgelicht zoals profiel van crimineel wordt opgesteld
http://www.volkskrant.nl/politiek/burger-wordt-straks-doorgelicht-zoals-profiel-van-crimineel-wordt-opgesteld~a3759563/ 16 september 2014.
'SyRI is watching you', 5 november 2014
http://sargasso.nl/syri/

7 INSPECTIE SZW

INLEIDING

Buiten SyRI en de interventieteams heeft de Inspectie SZW een grote variatie in toepassingen en omvang van data-analyse. Nergens is (nog) sprake van Big Data-analyse waarbij grote bestanden worden onderworpen aan onderzoek naar correlaties. Daarentegen doet de sociale inspectie – die vooral fraude op de arbeidsmarkt onderzoekt – steeds meer aan data-analyse met een team Onderzoek en Analyse (O&A).
Dat maakt meer en meer gebruik van externe bronnen en samenwerkingen. Profilering van wetsovertreders is een van de doelstellingen Risicogestuurd werken, op grond van (Big) Data-analyse heeft volgens de top van de Inspectie de toekomst, zo blijkt uit de onderzoeksagenda. Wat behelzen de huidige praktijk, de resultaten daarvan en de toekomstige wensen? Welke samenwerkingen zijn er? Hoe komen privacy en het leggen van verantwoordelijkheid aan bod? Dat is onderdeel van dit hoofdstuk, opnieuw aan de hand van vele feiten en details.

7.1 BELEID EN WERKWIJZE

Wettelijke basis
Op 1 januari 2013 is de Wet aanscherping handhaving en sanctiebeleid SZW-wetgeving in werking getreden, ook wel Fraudewet genoemd. De wet geldt voor het gehele SZW-domein en bestrijkt:

- de arbeidswetten (Wet arbeid vreemdelingen (WAV), Wet minimumloon (WML), Wet allocatie arbeidskrachten door intermediairs (WAADI), Arbeidsomstandighedenwet (Arbowet) en Arbeidstijdenwet (Atw);
- kinderopvangtoeslag;
- sociale zekerheid (werknemersverzekeringen, volksverzekeringen en de Wet werk en bijstand (WWB).

De wet is op de eerste plaats een aanscherping van het sanctiebeleid zoals dat – wat betreft de sociale zekerheid – wordt uitgevoerd door gemeenten (WWB), de SVB (AOW, AKW en ANW) en het UWV (WAO/WIA, WW en ZW).[157]

Ook de mogelijkheden voor opsporing en handhaving van de Inspectie SZW, voorheen de Arbeidsinspectie, de Inspectie Werk en Inkomen en de SIOD (Sociale

157 Wet aanscherping handhaving en sanctiebeleid SZW-wetgeving
http://wetten.overheid.nl/BWBR0032087/geldigheidsdatum_04-01-2016

Inspectie en Opsporingsdienst), zijn verruimd. Onder meer met een zwaar accent op analyse van interne, en in toenemende mate ook externe, databestanden. Het meest vergaande onderdeel hiervan vormt 'SyRI', dat al in het voorgaande hoofdstuk is besproken. Voor handhaving kwam meer geld beschikbaar.
De capaciteit bij UWV, de SVB en Inspectie SZW werd voor vier jaar uitgebreid met jaarlijks 260 fte, waarvoor cumulatief 100 miljoen euro beschikbaar is gesteld. De verwachte opbrengst van deze uitbreiding is naast een eerlijker systeem (misbruik wordt bestraft), een financiële netto opbrengst van naar verwachting 189 miljoen euro.

Data-analyse vormt een succesfactor in dit voornemen: 'Intensiveren van de handhaving zal niet alleen plaatsvinden door extra budget, maar ook door de bestaande handhavingscapaciteit slimmer en effectiever in te zetten. Dit gebeurt door het scherp bepalen van de prioriteiten en het doorontwikkelen van risicoanalyses en profielen. De prioriteiten van de Inspectie SZW worden gebaseerd op risicoanalyses en de effectiviteit van de toezichtinstrumenten.'[158]
In mei 2014 rapporteerde minister Asscher in een brief over bestrijding van misbruik: 'Het afgelopen half jaar heeft de Inspectie SZW in het kader van het risicogericht handhaven de risicoanalyses verbreed met gegevens van andere publieke organisaties. De Inspectie SZW onderzoekt momenteel de verdere inzet van gegevens van private organisaties. Hiermee kunnen risicobedrijven gerichter worden geselecteerd. Risicomodellen worden geëvalueerd om de effectiviteit te verbeteren. In jaarverslagen van de Inspectie SZW wordt teruggekoppeld over de bereikte resultaten. Ook de SVB en het UWV werken met risicoprofielen en op basis hiervan worden gerichte handhavingsactiviteiten uitgevoerd.'[159]

Uitvoering analyse
Bij de Inspectie SZW fungeert de Directie Analyse, Programmering en Signalering als 'denktank en adviseur' voor de Inspecteur-Generaal (IG) en management. Het team O&A maakt informatieproducten, zoals risicoanalyses. Het verrichten van risicoanalyses wordt in het Jaarplan 2015 een van de belangrijkste uitgangspunten genoemd:
'Door risicogestuurd te werken kan de Inspectie SZW haar mensen en middelen selectief en gericht inzetten. Risicoanalyses zijn de basis voor de keuze voor de toezichtprogramma's voor de lange termijn, de aanpak binnen programma's en de

158 Brief van minister Asscher (SZW) en staatssecretaris Klijnsma (beiden SZW) aan de Tweede Kamer over de maatregelen op het terrein van fraude, handhaving en naleving. 4 oktober 2013.
https://www.rijksoverheid.nl/documenten/kamerstukken/2013/10/04/kamerbrief-over-fraudeaanpak-handhaving-en-naleving (geraadpleegd 6 februari 2016).

159 Idem.

selectie van te inspecteren bedrijven. Dit leidt tot een afgewogen mix van interventies en efficiënt en effectief toezicht.'[160]

En dat geldt niet enkel voor de ondersteuning van keuzes van de Interventieteams maar voor het brede spectrum van de Inspectie SZW.
Dankzij signalen uit informatieanalyse, zegt de Inspectie SZW, krijgt ze toekomstige risico's, witte vlekken en ontwikkelingen in de omgeving in beeld. Daartoe maakt de Inspectie gebruik van informatie en kennis uit meerdere externe bronnen zoals van Belastingdienst, het UWV, de SVB en de IND.

Voorbeelden van onderzoeken:
- In 2015 deed de Inspectie SZW in het kader van niet-naleving sociale zekerheidswetten onderzoek naar de naleving van de inspanningsplicht.
- In het kader van misbruik kennismigranten voert de ISZW inspecties uit bij werkgevers waar buitenlandse studenten werken en stelt rapporten van bevindingen op ten behoeve van de IND.
- De inspectieaanpak van schijnconstructies is geïntensiveerd. Er is een interventieteam opgericht waarin de Inspectie onder meer samenwerkt met de Belastingdienst, UWV en IND.

Sinds 2012 heef de Inspectie een gerichte aanpak om het aantal malafide intermediairs op de arbeidsmarkt terug te dringen, onder meer door samenwerking met publieke partijen als het UWV, de Belastingdienst, gemeenten, de politie en waar nodig het OM, maar ook met private partijen als SNCU, organisatie van de uitzendbranche en SNA, Stichting Normering Arbeid. De samenwerking met private partijen en uitwisseling van informatie is een nieuw terrein voor de inspectie SZW.

Er worden drie vormen van analyse onderscheiden:
1. Werkterreinen bepalen
   De afdeling O&A bepaalt met de programmanagers van de Inspectie SZW welke informatie en data nodig zijn voor maximaal effect. Ten eerste voor de selectie: welke risico's spelen er in welke sectoren en met welke thema's? Zo komt de Inspectie tot een focus op te onderzoeken thema's voor het jaarplan. Vervolgens worden, ook met kwantitatieve en kwalitatieve data (uit dossiers), per programma de risico's geduid via onder andere doelgroepanalyses en netwerkanalyses. Het resultaat hiervan komt in overleg met focusgroepen van deskundigen.
   Na de keuze voor een sector of branche om te onderzoeken, bijvoorbeeld horeca, de wasserijen of bepaalde detailhandel volgt de object- en subjectselec-

160 Jaarplan 2015 Inspectie SZW
http://www.inspectieszw.nl/Images/Jaarplan-InspectieSZW-2015_tcm335-359626.pdf

tie, de meest operationele manier van risicoanalyse: welke bedrijven worden doelwit van onderzoek naar onderbetaling, illegale tewerkstelling et cetera. Voor bijvoorbeeld onderzoek naar kennismigranten worden bestanden van van mensen die Nederland inkwamen en die de IND verdacht vindt aangelegd tegen bijvoorbeeld de polisadministratie van het UWV om na te gaan of er mogelijk illegale tewerkstelling plaatsvindt. Bedrijven die betreffende personen in dienst hebben krijgen inspecteurs op bezoek.
Dit beschouwt de Inspectie SZW als 'witte fraude', van bedrijven die handelen vanuit kennisgebrek en zonder zich te verdiepen in de regels.

2. Indicatoren bepalen
Groepen van inspecteurs en een analist bepalen gezamenlijk indicatoren die kunnen wijzen op illegaliteit. De zachte kennis van inspecteurs wordt verwerkt in indicatoren voor data-analyse in bestanden. Bijvoorbeeld een verdenking van illegale tewerkstelling toetsen met een de omzet-loonverhouding vanuit de bestanden van de Belastingdienst en het UWV.

3. Profilering
Zoeken naar profielen van bedrijven of bestuurders op basis van historische gegevens. Er wordt daarbij, op basis van kenmerken van bedrijven die eerder de wetgeving hebben overtreden, via statistiek gekeken of er een (voorspellend) profiel kan worden gemaakt waarmee bedrijven kunnen worden aangeduid waar de kans op regelovertreding groter is dan gemiddeld.
'Binnen die drie types onderzoeken we voortdurend wat wel en niet werkt: trail and error, heel tijdrovend. De inzet van data verschilt echt sterk per onderzoek. Voor het ene halen we met een simpele bestandsvergelijking al veel indicatoren boven water, dan weer moeten we een complex dataprofiel opstellen, en soms volstaat de kennis en ervaring van de inspecteurs.' O&A gaat altijd eerst na of data-analyse bijdraagt. Bovendien is de afdeling afhankelijk van de kwaliteit van de data.[161]

Inzet systemen

ICT is volgens O&A geen doorslaggevende factor. Louter in de analyse voor Interventieteams (LSI) wordt gebruikgemaakt van het SyRI (Systeem Risico Analyse). Op andere terreinen niet.
Bij de Inspectie SZW is in 2014 een aparte dataserver ingericht voor het koppelen van verschillende databestanden, bewaking van datakwaliteit en geautomatiseerde rapportage. De projecten kunnen nu sneller en gebruiksvriendelijker van data-analyse gebruikmaken, zegt ISZW.

161 Interview met Inge Jonker van de Inspectie SZW.

Het selecteren, analyseren en profileren van(uit) de benodigde data vindt plaats met gangbare programma's als SPSS, iBase en Analist Notebook. Inzet van software is ondergeschikt aan de vraagstelling. 'We doen dus niet aan Big Data-mining, zo maar correlaties en causaliteit gaan exploreren, maar stellen altijd concrete vragen aan de data. We anonimiseren de data niet, omdat we niet of nauwelijks werken met persoonsgegevens. We halen de bronbestanden van de Belastingdienst, het UWV et cetera binnen en passen die toe per project.'[162]

7.2 EXTERNE SAMENWERKING

Met justitie

Samenwerking met politie en het OM is een speciaal terrein wat betreft data-uitwisseling. De Inspectie heeft in 2014 een programma opgesteld voor het signaleren en aanpakken van arbeidsuitbuiting. Samenwerking met politie en andere (inter)nationale partijen is essentieel in de bestrijding van arbeidsuitbuiting en wordt steeds intensiever. De Inspectie voert analyses uit die zorgen voor een scherpere focus bij de bestrijding van arbeidsuitbuiting en doet opsporingsonderzoeken. De samenwerking met Justitie is complex wat betreft privacy. 'Voor gebruik van data van de politie en het OM vallen we onder de wet politiegegevens (Wpg) en zijn we onderworpen aan een veiligheidsonderzoek van de AIVD. opsporingsonderzoeken, onder andere naar arbeidsuitbuiting. We kijken in dossiers naar eerder veroordeelde personen en zaken om eventueel te kunnen voorspellen waar zich risico's kunnen voordoen. Dat is nog prematuur, maar wel een mooie lijn om uit de breiden. Dat zijn niet veel data, maar wel boeiend qua risicoanalyse.'
Ook voor de Inspectie SZW wordt het werken met data over al dan niet illegale immigranten belangrijker en dus de samenwerking met het Nationaal Vreemdelingen Informatieknooppunt (NVIK), die alle politie-informatie over criminaliteit met vreemdelingen beheert zoals mensensmokkel, illegale arbeid, uitbuiting. 'In het algemeen kijken we nog per zaak, dus uit casuïstiek. We toetsen meer voor verrijking van data per zaak. Dat vergt zorgvuldig handelen. Wij mogen niet zomaar onze data uit het toezicht op de arbeidsmarkt koppelen aan de data van NVIK.'
'Zij mogen dat wel doen, want opsporing en strafrecht mag gebruikmaken van data uit toezicht, maar niet zomaar andersom. Daar zit een streng regime op, terecht. Dat doen we ook met de dienst Justis. Die doet zelf veel verrijking met de eigen politiedata. Dus we brengen ook zaken naar Justis om te kijken of ze die met hun data kunnen verrijken.
Ook dat vergt eenzelfde regime. Strafrecht is van een andere orde, maar we willen voor de profilering er wel meer van toe te passen.' Zo is de Inspectie SZW op justitieterrein ook participant in ICOV, die data-analyse doet op zoek naar crimineel vermogen. 'We helpen mee in de analyse en leveren onderzoekscapaciteit. Wij

162 Idem.

proberen bijvoorbeeld meer richting verdachte bestuurders kunnen komen die vaak zaken failliet laten gaan en doorstarten.'[163]

In projecten

De Inspectie SZW werkt ook samen in data-analyse in zogenoemde businesscases. Deze naam geven ministeries aan projecten in onder meer fraudebestrijding die naar verwachting de investeringen (ruimschoots) terugverdienen: In één businesscase werkt de Inspectie nauw samen met het UWV om gefingeerde dienstverbanden, premie- en uitkeringsfraude op te sporen, waarmee onder andere uitkeringsfraude wordt gepleegd.
Ook vinden projecten plaats om data-uitwisseling soepeler te laten verlopen. Rijksbreed vindt een ontwikkeling plaats naar zogenoemde sectorale knooppunten, waarlangs gegevensuitwisseling moet gaan plaatsvinden. Zoals naar de noodzaak van het inrichten van een 'knooppunt' om de sector Werk & Inkomen (UWV, gemeenten, SZW) op het Handelsregister (NHR) aan te sluiten.
Op dit moment ontvangen ze via Suwinet gegevens uit het NHR. Daarnaast wordt het NHR ook rechtstreeks geraadpleegd door de Inspectie SZW, de directie Kinderopvang (via DUO) en UWV. De conclusie luidde dat er in financieel-economisch opzicht geen significant verschil is tussen het handhaven van de huidige situatie en de inrichting van een sectoraal knooppunt.[164]

Ook werkt de Inspectie SZW sinds begin 2013 nauw samen met het ministerie van VWS als opsporingsdienst van fraude met pgb's. En sinds begin 2014 vanuit VWS belast met de strafrechtelijke handhaving van fraude met de AWBZ en de Zvw. Ook declaratiefraude is een taak geworden van de ISZW, zo maakte het kabinet eind 2014 bekend.
VWS besloot mede om de handhaving en opsporing van fraude in de Zorgsector te intensiveren met de Inspectie SZW, omdat ze beschikt over brede mogelijkheden

163 Idem.
164 http://www.digitaleoverheid.nl/onderwerpen/stelselinformatiepunt/stelselthemas/knooppunten
Berenschot, Businesscase NHR 2015, Rapport voor het ministerie van SZW, augustus 2015. https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2015/10/30/rapport-businesscase-nhr-2015/20150803-rapport-businesscase-nhr-2015-v1.0-definitief.pdf

tot inzage in, en koppeling van vele bestanden voor data-analyse (zie verder hoofdstuk 3 Zorg).[165]

Samenwerking basisregistraties

Een bijzondere samenwerking betreft het opwaarderen van de basisregistraties voor adequater gebruik voor onder meer fraudebestrijding. Het grote project Adreskwaliteit van het ministerie van BZK is daarin een voorloper. Net als bij veel andere instanties in fraudebestrijding gaan er bij de Inspectie SZW stappen vooraf aan het toepassen van (big) data-analyse. Zo is er onderzoek gedaan naar de Basisregistraties als fundament voor modernisering toezicht bij Inspectie SZW.
Voor het voorkomen en bestrijden van fraude maak de Inspectie SZW veelvuldig gebruik van basisregistraties zoals Basisregistratie personen (BRP), Handelsregister en Kadaster, maar nog niet in voorspellende zin met data-analyse. Daartoe zijn de databanken niet beschikbaar. De basisregistraties tezamen vormen een datareservoir *a boire*, maar analyse daarvan op grond van de principes van Big Data-analyse vormen nu nog een 'stip aan de horizon'.[166]

7.3 TOEKOMST

Jaarplan 2016

Voor 2016 staat exact dezelfde passage als voor 2015 was ingebracht wat betreft analyse: 'De Inspectie werkt risicogestuurd. Daardoor kan zij haar mensen en middelen selectief en gericht inzetten. Risicoanalyses zijn de basis voor de keuze voor de toezichtprogramma's voor de lange termijn, voor de aanpak binnen programma's en voor de selectie van te inspecteren bedrijven. Dit leidt tot een afgewogen mix

---

165 Brief van staatssecretaris Van Rijn (VWS) aan de Tweede Kamer over zijn plan voor het intensiveren van de aanpak van de fraude met het persoonsgebonden budget (pgb), 2 december 2012.
https://www.rijksoverheid.nl/documenten/kamerstukken/2012/12/02/aanpak-pgb-fraude
Opsporing zorgfraude komende jaren taak van Inspectie SZW, Nieuwsbericht Rijksoverheid.nl, 12december 2014 | http://www.rijksoverheid.nl/nieuws/2014/12/12/opsporing-zorgfraude-komende-jaren-taak-van-inspectie-szw.html

166 Stelsel van Basisregistraties.
http://www.digitaleoverheid.nl/onderwerpen/stelselinformatiepunt/stelsel-van-basisregistraties (geraadpleegd 8 februari 2016).
'Basisregistraties als fundament voor modernisering toezicht bij Inspectie SZW', Ruud Boot (ICTU) en Wimfred Grashoff (Servicepunt Basisregistraties), zonder datum
http://www.digitaleoverheid.nl/images/stories/stelsel_van_basis registraties/best-practice-iszw.pdf (Geraadpleegd 8 februari 2016).

van interventies en efficiënt en effectief toezicht.'[167] Een specificatie blijft achterwege. Wel wordt data-analyse op een aantal terreinen aangestipt:

– In 2016 ligt bij het toezicht op het domein Eerlijk werk meer nadruk op grootschalige onderzoeken van complexe fraudes en constructies. Dat past bij de focus van de Inspectie op notoire overtreders en misstanden, maar betekent ook dat er in dit domein minder reguliere inspecties plaatsvinden.
– De Inspectie zou in 2016 significant meer tijd inplannen voor ongevalsonderzoek. Dit is nodig omdat de behandeltijd per onderzoek toeneemt. De ongevalsonderzoeken leveren informatie over potentiële misstanden en voor risicoanalyse. Zo trad naar voren dat er veel meer ongevallen plaatsvinden met de toename van inhuur van zzp'ers in de bouw.
– De Inspectie heeft vastgesteld in hoeverre werknemers in specifieke sectoren worden blootgesteld aan arbeidsrisico's, op grond van data uit de Nationale Enquête Arbeidsomstandigheden (NEA) van het CBS en uit Arbo In Bedrijf (AIB) door de Inspectie zelf. Op basis van deze gegevens is een maat voor risico op blootstelling opgesteld.

De Inspectie heef een aanvullende risicoanalyse uitgevoerd voor het domein Werk en Inkomen, onder meer vanwege decentralisatie naar de gemeenten van het sociale domein via de Participatiewet, de Wmo en de Wet op de jeugdzorg.

Onderdeel vormt de analyse van de risico's, met een 'eindoverzicht' van 22 hoofdrisico's en ruim 150 subrisico's; de basis voor de programmering van de inspectie op het domein Werk en Inkomen. Bijvoorbeeld 'kwaliteit van dienstverlening' en 'knelpunt ICT' traden naar voren als grote risico's voor problemen bij decentralisatie.
De Inspectie heeft ook risicoanalyse toegepast gericht op het in beeld krijgen van de risico's op toenemende uitsluiting en armoede van de kwetsbaarste burgers. Daartoe worden gegevens uitgewisseld met de Inspectie voor de Gezondheidszorg (IGZ), de Inspectie van het Onderwijs (IvhO), de Inspectie jeugdzorg (IJZ) en de Inspectie Veiligheid en Justitie (IVENJ), ook in een al bestaand coördinerend orgaan: Samenwerkend Toezicht Jeugd (STJ).

Meerjarenplan 2015-2018

Genoemde passage over 'risicogestuurd werken' keert ook letterlijk terug in het Meerjarenplan 2015-2018 van de Inspectie SZW. In een risicodiagram staan de uitkomsten van het combineren van analyse van bestanden en meldingen van personeel en derden. Het betreft risicothema's en verschillende risico's. Risicoanalyse neemt een voorname plaats in het nieuwe programma. In de komende jaren zal de

167 Jaarplan 2016 Inspectie SZW http://www.inspectieszw.nl/Images/jaarplan-2016-inspectie-szw_tcm 335-369124.pdf

Inspectie SZW de methode van signaleren en het afgeven van signalen verder ontwikkelen.[168]

7.4 PRIVACYPROBLEMEN

Onderzoek en Analyse van de Inspectie SZW worstelt, evenals vrijwel alle onderdelen van de overheid die fraude bestrijden, aanzienlijk met privacy. Bij gebrek aan helder wettelijk kader – buiten de Wbp – voor het samenwerken en combineren van data proberen diensten voor zichzelf en in samenwerking de grenzen vast te stellen.

'We houden ons zo goed mogelijk aan de Wbp. Als we persoonsgegevens niet nodig hebben, gebruiken we ze niet. Als we er wel mee werken, zoals met het profileren van verdachte bestuurders, moeten we er een hele goede, transparante onderbouwing voor hebben. We proberen zoveel mogelijk te beschrijven hoe we voldoen aan de eisen van de WBP waaronder de proportionaliteit en subsidiariteit. Daar plegen we het afgelopen halfjaar en komende halfjaar meer inspanningen voor. Met de toepassing van SyRI is dat aanvankelijk onvoldoende gedaan, waardoor er verkeerde beelden onder andere in de media zijn ontstaan. Transparantie en samenwerkingsafspraken zijn nu doorlopend onderdeel van het werk, om het goed juridisch te onderbouwen. Dat is erg belangrijk, want we hebben zelf zo weinig data dat we voor meer risicogestuurd werken altijd data van andere partijen nodig hebben.'

Inzage geven in deze afspraken is niet mogelijk. De Inspectie zegt er transparant in te willen zijn, maar ze staan nog niet goed op papier. 'We moesten steeds per project met de Belastingdienst, het UWV en de IND afspraken maken, wat bewerkelijk was, dus nu proberen we tot één stelsel van afspraken te komen waarmee we kunnen werken, bekrachtigd op bestuurdersniveau van de betrokken diensten, zodat we het echt goed op orde hebben. Met de kanttekening dat dit met de ene dienst makkelijker gaat dan met de andere. Dus steken we er veel inspanning in.'[169]

168 Meerjarenplan Inspectie SZW 2015-2018
http://www.inspectieszw.nl/Images/Meerjarenplan-InspectieSZW-2015-2018_tcm335-359627.pdf

169 Interview met eerdergenoemde.

8 UWV

INLEIDING

Het UWV heeft een heldere, voortvarende visie op de inzet van data voor fraudebestrijding. Het UWV is actief met het ontwikkelen van risicoprofielen. Het UWV heeft een aantal onderzoeken gedaan naar de inzet van data, modellen opgesteld, testen uitgezet en nieuwe methoden in praktijk gebracht. Een aanzienlijke verbetering van de resultaten van bestrijding van 'onjuist handelen' is deels het gevolg van de inzet van risicoprofielen.
Het UWV heeft een helder toekomstbeeld aangaande data-analyse op grond van klantgedrag. De dataverzameling richt zich ook op het indelen van individuele personen in een categorie met behulp van een risicoprofiel, gebaseerd op hun 'kans' op niet naleven van de regels. Ook voor gezondheidsfraude gaan risicoprofielen de handhaving helpen, met in beeld gebrachte 'verwondergevallen'.
Hoe zet UWV data-analyse op, met welke verwachtingen en hoe komen privacy, IT en samenwerking aan bod? Daarover handelt dit hoofdstuk dat grotendeels stoelt op vraaggesprekken en toelichtingen van betrokken deskundigen. Ze tonen een scherp beeld van de mogelijkheden en wensen van UWV op het terrein van data-analyse.

8.1 DOEL EN VERWACHTINGEN

Het UWV formuleert dit als volgt: 'Het UWV werkt continu aan het toepassen van de nieuwste technieken op het gebied van ICT en data-analyse om de beschikbare klantgegevens optimaal te benutten bij het voorkomen en opsporen van misbruik van uitkeringsgeld. Hierbij houdt het UWV altijd de privacy nauwlettend in de gaten en overlegt indien nodig met onder andere de Autoriteit Persoonsgegevens.'[170]

8.2 TOTSTANDKOMING VAN SYSTEMEN EN PROJECTEN

Momenteel ligt het accent nog op bestandsanalyse op basis van inhoudelijke ideeën en nog niet op datamining: de data laten spreken. Wel is bij het UWV consequent het BSN de kapstok om informatie aan te binden, maar het geautomatiseerd relateren van een uitkeringsgerechtigde aan een fraude- of bezwaarzaak is niet mogelijk. Dat heeft een technische oorzaak: het is voor het UWV nog niet mogelijk om de geschikte bestanden met kenmerken die een relatie hebben met de kans op

170 Interview met Ernst Veenhoven, Strategisch beleidsadviseur UWV, en Michael van Eck, Risico-Onderzoeker UWV. Zij zijn verantwoordelijk voor alle verdere citaten in dit stuk van het UWV, tenzij anders vermeld.

regelovertreding te koppelen. Alle UWV-onderdelen werken met eigen registratiesystemen en dat zijn workflow- en verantwoordingssystemen die niet (helemaal) op elkaar aansluiten. Sommige systemen bevatten gescande documenten en kunnen daarom geen relevante data genereren. Echter, na het slechten van de technische hobbels wordt datamining op grond van BSN, maar ook geanonimiseerd, wel mogelijk. Dan nog moet aan een aantal voorwaarden worden voldaan, bijvoorbeeld aangaande privacy en relevantie van onderzoek. Zo is het aantal geconstateerde overtredingen voor bepaalde regels te laag voor UWV om op grond hiervan risicoindicatoren te kunnen bepalen. Overigens is niet a priori sprake van 'pakkans' of schuld: Het kan zijn dat een klant de regels niet kent of niet weet hoe hij ze moet naleven. Dit is volgens het UWV in het grootste deel van de geconstateerde overtredingen de reden. Degenen die de regels niet willen naleven, vormen volgens UWV de kleinste categorie.

8.3 UITVOERING (EN RESULTATEN)

Het UWV is wel actief met het ontwikkelen van risicoprofielen. De dataverzameling richt zich op het indelen van individuele personen in een categorie met behulp van een risicoprofiel, gebaseerd op hun 'kans' op niet naleven van de regels. Het UWV heeft echter een voorkeur voor het handhaven met wat zij noemt 'verwondersignalen': gegevens die moeilijk met elkaar te rijmen zijn ofwel anomalieën. Dit draagt momenteel meer bij aan succesvol handhaven dan het berekenen van kansen op overtreding op grond van analyse van databestanden, die zou moeten leiden tot risicoprofielen. Het UWV heeft de volgende onderzoeken gedaan:

1. Risicomodellen opgesteld voor het selecteren van klanten voor huisbezoeken en telefonische controles, gebaseerd op uitkeringsbestanden (WW, WAO, WIA, etc.) en frauderegistraties. Deze modellen bevatten kenmerken als leeftijd, geslacht, soort uitkering, uitkeringsduur en -hoogte, sector, toeslag, beslaglegging en recidive (eerdere regelovertredingen). Als methode is gekozen voor logistische regressie (kansverhoudingen met verschillende variabelen), om twee redenen:
   - Het hieruit resulterende risicoprofiel leent zich beter voor het selecteren van een specifiek aantal te controleren klanten dan een beslisboom.
   - Het is inzichtelijker dan een profiel in de vorm van een neuraal netwerk, terwijl de voorspelkracht nagenoeg gelijk is.

Een voorbeeld volgens de UWV-woordvoerders: 'Zo kan met een logistisch regressiemodel voor de WW, periodiek voor alle WW'ers, via een expliciete formule en dus transparant, de kans op regelovertreding worden berekend en een, door de controlecapaciteit bepaald, specifiek aantal WW'ers met de hoogste kans op regelovertreding worden geselecteerd voor controle.'

Dit heeft de voorkeur boven louter een beslisboom of via een neuraal netwerk selecteren: 'Met een beslisboom kan alleen een aantal categorieën en geen precies aantal worden geselecteerd. Een model op basis van een neuraal netwerk levert geen expliciete formule op die bij navraag gepresenteerd kan worden en is dus niet transparant.'
Bij het risicomodel WW bleek over 2014 ruim een verdubbeling van de trefkans, namelijk van 9,8 procent bij aselecte controle tot 24,6 procent met behulp van het 'WW-model'.
Momenteel vindt reeds 90 procent van de controles van het UWV plaats op basis van risicoprofielen en nog 10 procent van de controles aselect. Door vergelijking van de resultaten van de controles met risicoprofielen en de controles bij aselect gekozen klanten kan de effectiviteit van het risicoprofiel worden bepaald en het profiel zo nodig worden aangepast. Tegelijk kan worden voorkomen dat nieuwe risico's niet worden ontdekt.

2. Risicoprofielen voor de kans op het overtreden van specifieke regels (voldoende solliciteren, melden van inkomsten, vakantie en vrijwilligerswerk, e.d.), maar ook profielen van klanten die geen gebruik (kunnen) maken van het e-kanaal of waarbij de overtreding verminderd verwijtbaar was. Ook hierbij maakt het UWV gebruik van uitkeringsbestanden en frauderegistraties, maar ook van SONAR (het registratiesysteem van Werkbedrijf met kenmerken als opleiding en beroep) en van telefoniedata, dat wil zeggen de door klanten gestelde vragen via de UWV-telefoon die in databanken zijn verwerkt tot data. Dit leverde UWV een basis op voor het ontwikkelen van nalevingscommunicatie en input voor de ontwikkeling van instrumenten voor het bevorderen van nalevingsgedrag. Voorbeelden? 'Zo ontwikkelde het UWV risicoprofielen voor de nalevingscampagnes 'Werken met een uitkering' en 'Vrijwilligerswerk' op basis van de kenmerken van klanten die werkzaamheden niet meldden en via UWV-telefoon vragen stelden over vrijwilligerswerk en het mogen bijverdienen.
   Deze profielen maakten het mogelijk om de campagnes op de juiste doelgroep te richten. Hierbij werd overigens wel gebruik gemaakt van beslisbomen omdat niet individuele risicoklanten, maar risicogroepen werden benaderd.'

3. Risicoprofielen voor interventieteams, ontwikkeld in samenwerking met de Belastingdienst, de SVB, RCF/Gemeenten en de Inspectie SZW met gebruikmaking van SyRI (Systeem Risico-indicatie). Dit is een systeem om bestanden door een *trusted third party*, i.c. het IB, te koppelen en klanten te selecteren op basis van een vooraf vastgesteld risicoprofiel. Alleen de namen van klanten met een hoog risico worden door het IB geleverd aan de interventieteams. Doordat zo ook bestanden van bijvoorbeeld energie- en waterleidingbedrijven gebruikt konden worden, nam de opbrengst van de interventieteams sterk toe.

Interventieteam projecten zijn gericht op diverse vormen van fraude, waaronder zwart werken en woonfraude. Zo werd in het eerder genoemde project Waterproef gebruikgemaakt van het kenmerk waterverbruik. Ook kon hiermee bij een zeer hoog waterverbruik zwart werken worden getraceerd, bijvoorbeeld als thuiskapster, of het onderhouden van wietplantages.

4. Onderzoek naar anomalieën ofwel verdachte combinaties van kenmerken, in plaats van kansen. In dit kader probeert het UWV gegevens te achterhalen over niet gemelde inkomsten en gefingeerde dienstverbanden. De Polisadministratie met gegevens over alle dienstverbanden vormt de voornaamste bron. Dit leverde concrete signalen op waarmee de betreffende klanten geconfronteerd konden worden en om uitleg gevraagd.
   Met deze onderzoeken verkent het UWV de toepassing van het koppelen van databestanden bij het opsporen van misbruik van uitkeringsgelden. Vooralsnog zijn dit projecten die bottom-up en/of in samenwerking met partners tot stand komen. Dit heeft nog niet geleid tot overkoepelend beleid voor het gebruik van Big Data op het vlak van fraudebestrijding.
   Een voorbeeld is het ontdekken van faillissementsfraude door in de Polisadministratie dienstverbanden te selecteren en te controleren die na de faillissementsdatum zijn aangemeld of waarbij kort voor het faillissement het loon aanzienlijk is verhoogd.
   Een ander voorbeeld zijn zelfstandigen met WW, die bij UWV maar weinig gewerkte uren meldden, maar bij de Belastingdienst zelfstandigenaftrek claimden, omdat ze minstens 1225 uren per jaar aan hun bedrijf besteedden.

Resultaten

Cijfers over de resultaten van handhaving:

Overtredingen inlichtingenplicht	**2013**	**2014**
Onderzoeken	50.935	71.543
Geconstateerde overtredingen	46.855	65.505
Benadelingsbedrag (x € 1.000)	71.599	88.200
Opgelegde boetes	37.886	50.045
Boetebedrag (x € 1.000)	23.257	55.284
Waarschuwingen	5296	9225
Processen-verbaal (OM)	302	276
Overtredingen inspanningsverplichtingen		
Opgelegde maatregelen	90.294	97.399
Waarschuwingen	31.153	51.450

De verbetering van de resultaten in 2014 ten opzichte van 2013 is deels te danken aan bovengenoemde onderzoeken met risicoprofielen en deels aan meer ingezette handhavingscapaciteit. Immers, het UWV ontving van het ministerie van SZW

extra geld voor de aanpak van uitkeringsfraude. Bovendien zijn enkele van deze onderzoeken gericht op preventie.

8.4 HINDERPALEN EN VRAAGTEKENS

De afgelopen jaren is gebleken dat de ICT-systemen van het UWV kwetsbaar zijn. Het UWV geeft prioriteit aan het oplossen van technische problemen waar de klanten last van hebben. De media hebben uitgebreid bericht over deze euvels van het UWV. Toepassing van data-analyse en koppeling van bestanden vraagt om nieuwe aanpassingen in de systemen om de gegevens uit de betreffende bestanden te ontsluiten.
Dit legt druk op de capaciteit van de programma's en brengt ook risico's met zich mee op nieuwe technische problemen. Dit kan een rem zijn op de ontwikkeling van Big Data-analyse. Het UWV voerde overleg met de Autoriteit Persoonsgegevens over in te zetten risicomodellen voor huisbezoeken en telefonische controles en over het registreren van begeleiders en specialisten bij Ziektewet- en WIA-klanten. Dat werd akkoord bevonden, aldus UWV.
Ook voerde de Inspectie SZW namens het UWV en de andere deelnemers aan de Interventieteams overleg over het koppelen van data over onder andere water- en energiegebruik en werd de SyRI-werkwijze als oplossing geaccepteerd door de AP. Voor de andere twee bovengenoemde projecten is geen overleg gevoerd met de AP.

Opvallend is de vaststelling van het UWV op vragen over het boekstaven van 'beroepsfraudeurs'. Dit voornemen keert in veel besproken plannen voor handhaving terug, ook door het kabinet gepresenteerd. Het antwoord luidt: 'Samenwerking tussen instanties heeft niet geleid tot een lijst van beroepsfraudeurs. Een reden is dat dit binnen de bestaande wettelijke mogelijkheden van gegevensuitwisseling niet is toegestaan. Een andere reden is dat het niet wenselijk is dat mensen die vaak, en soms onbewust uitkeringsfraude plegen, op een lijst terecht komen van "echte criminelen".'[171]

8.5 TOEKOMSTIGE VOORNEMENS

Het UWV is voornemens om het zwaartepunt in de preventieve handhaving te verschuiven van klantkenmerken naar klantgedrag: het volgen van gedrag van UWV-cliënten via online kanalen (internet, apps). Het UWV wil zich richten op het online informatie verzamelen van *customer journeys*: hoe gedragen klanten zich online en wat kan als afwijkend en voorspellend voor regelovertreding worden gekenmerkt. Vervolgens kan het (afwijkend) gedrag worden beïnvloed.

171 Interview UWV.

Voor zover mogelijk wordt dit een vorm van 'automatisch handhaven': een signaal over een online afwijkend gedrag leidt tot een verzoek tot verbetering of uiteindelijk sanctie.

Het traceren van patronen in onlinegedrag die samenhangen met het afwijken van de regels is volgens het UWV belangrijk in het preventief onderkennen van het niet weten, niet kunnen of niet willen naleven van de regels. De profielen gebruikt het UWV om klanten met afwijkende kenmerken te stimuleren tot naleving via een op hen afgestemde interventie: herinnering, waarschuwing, concrete (gewetens)-vraag of opdracht.
RUEI (Real User Experience Insight) is een database opgebouwd uit klik- en navigeergedrag van klanten op werk.nl. De RUEI-data worden opgeslagen in een timestamped format. Ieder datarecord bevat onder andere BSN, tijdstip en tijdsduursessie, opgevraagde webpagina's op werk.nl en klantgegevens zoals header, http statuscode en IP-adres.
RUEI biedt UWV inzicht in het onlinegedrag van klanten op welke momenten, en vanuit welke plek/computer de klanten in contact zijn met het UWV.
Datawarehousing wordt in de nabije toekomst ook toegepast op SONAR en andere registratiesystemen. In SONAR staan gegevens zoals CV, inhoud sollicitaties, het lezen van berichten en uitvoeren taken door klanten inclusief tijdstippen en tijdsduur. Oftewel: in hoeverre voldoet de klant aan de inspanningsverplichtingen die samenhangen met de uitkering?
UWV voert structureel analyses uit op RUEI-data en maakt hierbij gebruik van het IBM QRadar Security Intelligence Platform. De RUEI-data heeft onder andere bij het opsporen van DigiD-fraude een bijdrage kunnen leveren.
Vooral Logius en de Belastingdienst hebben gediend als inspiratie voor RUEI. Een andere bron voor deze dataverzameling en sturing is het gedrag van klanten met betrekking tot de Inlichtingenplicht. Zo kijkt het UWV of WW'ers vanuit het buitenland inloggen en controleert dan of ze ongemeld met vakantie in het buitenland verblijven. Zo ja, dan kan dit reden zijn voor een controlebezoek, zogenoemde flitscontroles.

Een tweede voornemen betreft de aanpak van gezondheidsfraude. Met behulp van systeemscreening worden opmerkelijke situaties ('verwondergevallen') in beeld gebracht en nader onderzocht. De hiervoor te ontwikkelen profielen zouden diagnoses kunnen bevatten, wat stuit op privacybezwaren inzake het medisch geheim.
Dit kan worden opgelost door een met SyRI (zie boven) vergelijkbare anonimisering toe te passen en alleen de verwondergevallen te de-anonimiseren en door een medicus te laten beoordelen alvorens een fraudeonderzoek te starten. Ook is er naar aanleiding van eerdere fraudegevallen een registratie van begeleiders en specialisten opgezet, maar die wordt nog onvolledig gevuld.

Wat behelst 'systeemscreening'?

Met behulp van gegevens in de bestanden van Sociaal Medische Zaken (SMZ) van het UWV kunnen met profielen bijvoorbeeld de volgende verwondergevallen worden geselecteerd voor nader medisch (dossier)onderzoek.

Profiel 1: 'De cliënt heeft een diagnose met een gunstige prognose, is jong, heeft al langere tijd een WIA 80-100 uitkering en had een hoog dagloon. Voor deze cliënt is het gunstig dat hij nog een volledige arbeidsongeschiktheidsuitkering ontvangt en daarom is er een reële kans dat hij een verbetering van zijn gezondheid niet heeft gemeld.'

Profiel 2: 'Een cliënt is in behandeling bij een psychiater die ook diverse andere WIA-ontvangers behandelde die arbeidsongeschikt werden verklaard met dezelfde diagnose. Dit doet denken aan eerdere fraudes waarbij psychiaters valse medische dossiers opstelden en samen met anderen uitkeringsinstanties oplichtten.'

Een derde voornemen voor data-analyse betreft openbaar internetonderzoek: het navorsen van het aanbieden en/of uitvoeren van economische activiteiten en mogelijk daaruit voortvloeiende inkomsten, zoals het exploiteren van webwinkels en het aanbieden van goederen en diensten op marktplaats.nl en werkspot.nl. Het UWV heeft hierop middels web crawling en web scraping gegevens kunnen downloaden van klanten van het UWV.

Facebook en dergelijke worden tot nu toe alleen gebruikt voor het 'verrijken' van een fraudemelding die betrekking heeft op onder andere het zonder toestemming in het buitenland (o.a. op vakantie) verblijven en samenwonen. Voor het uitvoeren van dit soort internetonderzoek heeft het UWV een protocol opgesteld teneinde te voldoen aan privacyregels.

Een vierde voornemen is dat UWV meer gebruik wil gaan maken van bestanden van derden. Zo wil het UWV bestanden van de Kamer van Koophandel aan de eigen bestanden koppelen om werken als zelfstandige te kunnen traceren, evenals (relaties tussen) personen achter faillissementsfraude en gefingeerde dienstverbanden.

Hetzelfde geldt voor data van de RDW, bijvoorbeeld om klanten met 'klusbusjes' te traceren die worden ingezet voor zwartwerken. Ook de DUO-bestanden zijn van belang vanwege studiefinanciering en het volgen van een opleiding zonder toestemming van het UWV. Al deze voornemens bevonden zich nog in een verkennend stadium begin 2016.

Samenwerking met derden

Het UWV werkt mee aan gezamenlijke data-analyse in de Manifestgroep: data-uitwisseling in het kader van thema-gerichte samenwerking rond thema's als schijnconstructies.

UWV GegevensDiensten (UGD) wisselt bestanden uit, zoals met de Belastingdienst. Deze ontvangt actuele dienstverbandgegevens uit de Polisadministratie en

verschaft aan UWV onder meer data van personen die zelfstandigenaftrek ontvangen en personen die werken voor mensen met een PGB.
Logius levert aan het UWV IP-adressen van klanten die via DigiD inloggen op de site werk.nl en waarvan het BSN dus bekend is. Bureau Keteninformatisering Werk en Inkomen (BKWI) levert het UWV de GBA-gegevens,
De IND levert aan het UWV de aanvragen voor gezinshereniging.

Organisaties als het UWV, de DWI en de SVB delen hun gegevens via hetBKWI. Een aantal jaren geleden zijn ook diensten uit het opsporingsdomein, zoals de Inspectie SZW, aangeschoven. Deze gegevens kunnen echter alleen op individueel niveau via SUWI-net Services worden geraadpleegd. Het is voor de participanten niet mogelijk om deze gegevens op bestandsniveau voor meerdere klanten tegelijk op te vragen. Daardoor kunnen ze niet gebruikt worden in risicoprofielen.

Het UWV koestert de uitdrukkelijke wens om over de SUWI-gegevens ook in bestandsvorm te beschikken, maar dat past niet binnen de wettelijke basis van SUWI-net Services. Dat mag louter worden geraadpleegd.

9 SVB

INLEIDING

De SVB verzorgt onder meer de toekenning, herziening en eindiging van kinderbijslag (AKW), het ouderdomspensioen (AOW), de nabestaandenuitkering (Anw), de aanvullende ouderdomsvoorziening (AIO) en het persoonsgebonden budget (pbg). De SVB zet data-analyse in om fraude te beperken en ontvangt daartoe aanvullend budget.
Nauwe samenwerking met andere diensten moet helpen om onder meer 'businesscase Intensivering Toezicht van de SVB' tot een succes te maken: dus winst te maken op de investering. De ambities en verwachtingen van de SVB met de inzet van data- en risicoanalyse en eventueel profilering blijken echter een stuk bescheidener dan van veel andere in deze studie behandelde instanties. Dit is ongetwijfeld mede een gevolg van de omvangrijke IT- en politieke problemen bij de uitvoering van taken.
Deze euvels komen onderstaand aan bod bij de beschrijving van de fraudebestrijding door de SVB, de zorgen om privacy en de problemen in de samenwerking.

9.1 DOEL

De SVB zet data-analyse in om fraude te beperken. In het regeerakkoord heeft het kabinet de mogelijkheid opgenomen om door versterking van het toezicht van het UWV en de SVB te besparen op uitkeringen. Dit doen het UWV en de SVB door meer in te zetten op preventie, toezicht (controle), opsporing en afdoening.

Bij een brief van 4 oktober 2013 over dit onderwerp bood het kabinet de Kamer een pakket 'intensiveringsmaatregelen' aan.[172] Er werd een nauwe samenwerking aangekondigd tussen de Belastingdienst, de IND, het UWV en de Inspectie SZW om meer fraude op te sporen en af te handelen met behulp van gezamenlijke data-analyses.
Het accent zou daarbij liggen op het fraudefenomeen 'schijnconstructies', waarvan een 'enorme toename' werd waargenomen. De IND lijkt in deze samenwerking een vreemde eend in de bijt, maar minister en staatssecretaris lichtten deze zo toe: 'Een dienstverband kan op enig moment worden verzilverd in de vorm van een uitkering, maar het kan ook dienen voor het verkrijgen van leningen of als garantstel-

172 Kamerbrief over intensivering toezicht in het sociale zekerheidsdomein, 4 oktober 2013, minister Asscher en staatssecretaris Klijnsma van SZW
https://www.rijksoverheid.nl/documenten/kamerstukken/2013/10/04/kamerbrief-over-intensivering-toezicht-in-het-sociale-zekerheidsdomein

ling bij een gezinshereniging en tal van andere doeleinden. Werkgever en (pseudo)werknemer kunnen samenspannen in een lucratieve vorm van fraude, die leidt tot onacceptabele maatschappelijke uitkomsten op het vlak van de arbeidsmarkt, de sociale zekerheid, belastingen en immigratie.'
Het UWV en de Inspectie SZW kregen extra personeel, onder meer specialisten in data-analyse. De maatregelen zouden naar verwachting 7,5 miljoen euro kosten en 19 miljoen extra opleveren.

De extra inspanningen door de SVB op fraudebestrijding zouden in de praktijk echter veel geringer zijn, en vooral gericht op samenwonen en genieten van WWB en/of WWB-uitkering en vermogen in het buitenland. In een aparte brief informeerde minister Asscher de Tweede Kamer over de 'businesscase Intensivering Toezicht van de SVB', een beoogde intensivering in drie activiteiten:

1. extra capaciteit voor verwerking van alle fraudetips die bij de SVB binnenkomen, onder meer via de SVB-website, met 3,9 miljoen euro besparing in 2015, oplopend tot 5,9 miljoen euro in 2018;

2. risicogerichte steekproefcontroles, onder meer op basis van de bevoegdheid om gebruiksdata van nutsbedrijven op te vragen en te benutten, teneinde de opgegeven leefvorm van uitkeringsgerechtigden te controleren. De SVB zou de onderzoekscapaciteit uitbreiden om vijf keer zo veel steekproefonderzoeken te verrichten: van 1000 naar 5000. Daarnaast zouden 500 extra onderzoeken worden ingezet om nieuwe risico's te identificeren. Kosten: jaarlijks 2,5 miljoen euro met verwachte besparingen in 2015 van 2,7 miljoen euro, door cumulatie van de in voorgaande jaren behaalde besparingen oplopend tot 4,9 miljoen in 2018 euro;

3. uitbreiding risicogericht onderzoek in het buitenland met het Controle Team Buitenland (CTB). De SVB voert meer signaalgestuurde onderzoeken en meer risicogerichte steekproefcontroles uit, in totaal driemaal de huidige omvang van 450 onderzoeken: 700.000 euro aan kosten jaarlijks, met verwachte besparingen in 2015 van 0,8 miljoen euro, oplopend tot 2,2 miljoen euro in 2018.[173]

Dit vergde investering in de professionalisering van de risicoanalyse, mede gericht op nieuwe, met name digitale, fraudevormen. In totaal zou een kleine 30 miljoen euro aan extra investering in de periode 2015-2018 tot een extra besparing van ruim 46 miljoen moeten leiden.

173 Kamerbrief 'aanpassingen Fraudewet, aanbevelingen Nationale ombudsman', Bijlage 1 Aanvullende maatregelen intensivering toezicht SVB, 30 april 2015
https://www.rijksoverheid.nl/documenten/kamerstukken/2015/04/30/kamerbrief-aanpassingen-fraude wet-aanbevelingen-nationale-ombudsman

9.2 UITVOERING

De Bedrijfscoördinatoren Handhaving van de SVB zijn binnen de SVB verantwoordelijk voor data-analyse in het kader van de bestrijding van fraude. Zij zijn zelf geen professionele data-analisten, maar binnen de Businesscase Intensivering Toezicht wordt de SVB-formatie van handhavers ondersteund door professionele analisten.
Ondanks de politieke aansporing vervat in de businesscase wijzen de woordvoerders[174] erop dat de aard en omvang van fraude bij de volksverzekeringen veel beperkter zijn dan bij meer fraudegevoelige regelgeving als de WW en de WWB (Participatiewet). Daarom zal de meerwaarde van de professionalisering van data-analyse dan ook van een andere orde zijn dan bijvoorbeeld bij het UWV. Per onderscheiden volksverzekering betreft, zijn dit de bevindingen:
- Fraude bij de kinderbijslag komt voor, maar het gaat om weinig geld.
- Fraude bij de AOW en de Anw komt ook weinig voor, maar gaat om grotere bedragen.
- In relatieve zin komt fraude meer voor bij de Anw dan de AOW.

De SVB analyseert de eigen bestanden en werkt ook samen met partners in binnen- en buitenland. Zo is de Manifestgroep Fraude-analisten volgens de SVB erg actief met uitwisseling van tactische informatie over de ontwikkeling van fraude. Dit is een initiatief vanuit het Programma Compacte Overheid. Vooral de Belastingdienst heeft hierover veel kennis in huis. De Belastingdienst beschikt zelf over veel data en de combinatie van bestanden van de Belastingdienst levert veel fraudesignalen op.
De SVB werkt mee aan een project waarbij gerichte casussen worden uitgewisseld met de Belastingdienst en inspectiediensten om mogelijke postbusondernemingen, doorleenconstructies of andere schijnconstructies die gericht zijn op premieontduiking, tijdig te herkennen en gezamenlijk aan te pakken. Daarnaast heeft de SVB een risicoanalyse uitgevoerd die leidde tot het verbeteren van de processen voor de afgifte en ontvangst van de A1-verklaringen (bij detacheringen). Dit vloeide voort uit een Actieplan Schijnconstructies van de minister van SZW.

Ook op andere fronten wordt met ketenpartners als de Belastingdienst en inspectiediensten gezamenlijk data-analyse verricht: bilateraal wisselen de IND en de SVB informatie uit om gezamenlijk risico's vast te stellen. Dit betreft onder meer mogelijke risico-indicaties voor fraude met pensioenen of uitkeringen ingeval de gerechtigde tevens (ten onrechte) een verblijfsstatus in Nederland heeft. Als er inderdaad aanwijzingen voor fraude worden gevonden, kan een bestandsvergelijking worden opgezet.

174 Interview SVB, met Paul Burrough en Frits Werner van de afdeling Handhaving.

Bij het handhaven van de Anw blijkt het zinnig te zijn voor de SVB om geboorten van kinderen van Anw-gerechtigden, die meer dan negen maanden na het overlijden van de rechtgevende partner hebben plaatsgevonden, te onderzoeken. Onderzoek heeft uitgewezen dat in deze gevallen een verhoogd risico bestaat van een niet-gemelde gezamenlijke huishouding met een nieuwe partner waardoor de nabestaandenuitkering moet worden beëindigd.
De tweelingenfraude bij de kinderbijslag (kinderbijslag werd aangevraagd voor niet-bestaande tweelingen) in de jaren negentig van de vorige eeuw bleek te traceren door data-analyse van de eigen bestanden. Als in een bepaald land of streek of stad opvallend veel kinderbijslag voor tweelingen wordt aangevraagd, kan er sprake zijn van fraude. Valse aangifte van de geboorte van kinderen kan ook een signaal zijn van mensenhandel dat wordt gedeeld met de politie.

De SVB participeert verder in de Landelijke Aanpak Adreskwaliteit (LAA), een groot project voor bestrijding van adresfraude van het ministerie van BZK. Het is de bedoeling dat in dit project bestanden worden uitgewisseld om fraudesignalen te ontdekken. Dat betreft overigens geen bestanden van de SVB. De SVB verrijkt wél de signalen met informatie uit de uitvoering van verschillende andere regelingen. Dat wil zeggen dat SVB aangeeft of er bij een signaal sprake is van een SVB-pensioen of -uitkering.
'Windhappers' is een verschijnsel dat door de Belastingdienst wordt onderzocht. Het gaat hierbij om personen die in de Basisregistratie personen (BRP) zijn ingeschreven, maar van wie bij de Belastingdienst geen enkele vorm van inkomsten bekend is. Dat kan duiden op criminele activiteiten, of simpelweg op onjuiste inschrijving in de BRP omdat de persoon feitelijk in het buitenland woont.

9.3 RESULTATEN

Data-analyse als zodanig moet bij de SVB verder ontwikkeld en geprofessionaliseerd worden. De geïnterviewde SVB-medewerkers willen zich hoeden voor pretenties door harde resultaten te melden.

De resultaten van de Manifestgroep Fraude-analisten bestaan vooral uit kennisdeling en netwerkvorming. Beide hebben wat de SVB betreft geleid tot diverse onderzoeken naar gezamenlijke klantgroepen. Het betrof tot nu toe kleine steekproefsgewijze onderzoeken om vast te stellen of een mogelijk handhavingsprobleem zich daadwerkelijk voordeed.
Een hoofdstuk apart vormde de persoonlijke zorgbudgetten, beter bekend als pgb's. De uitbetaling ging over naar de SVB. Staatssecretaris Van Rijn van VWS noemde ook de fraudebestrijding als voordeel, juist gezien de mogelijke analyse en koppeling van bestanden: 'Doordat de SVB nu op een centraal punt de pgb-bestanden beheert, nemen de mogelijkheden toe voor analyse en controle van deze bestanden op fraude over de pgb-domeinen heen. Fraude kan eerder en beter wor-

den opgespoord en de resultaten kunnen gedeeld worden tussen zorgkantoren, gemeenten en zorgverzekeraars.'[175]
In de praktijk sneeuwde dit echter het afgelopen jaar onder in de grote problemen met de uitvoering van pgb-voorziening door de SVB, die ook een politiek heet hangijzer werden. De controles van aanvragen werden ook op sterk water gezet, teneinde de voortgang van de uitkering niet te storen. In de toekomst verwachten de SVB en de Inspectie SWZ wel vruchten te kunnen plukken van bestandsanalyse ter bepaling van risicofactoren.
Naar verwachting zal de Directie PGB van de SVB in 2016 starten met systematische risicoanalyse en waar nodig maatregelen nemen om het frauderisico in te perken.

De SVB kende behalve politieke tegenslag, ook ICT-problemen, die de overheid en bestuursorganen in de breedte troffen. Zo uitten minister Asscher en staatssecretaris Klijnsma de Kamer eind 2013 hoge verwachtingen van samenwerking in data-analyse in het sociale domein om fraude terug te dringen: 'Ook de SVB, het UWV en gemeenten streven naar een risicogerichte controle en handhaving.
De SVB heeft daarvoor het nieuwe Multiregelingensysteem (MRS) in ontwikkeling. Hierbij wordt via risicokenmerken en risicoprofielen steeds gerichter en volgens vaste uitvoeringsprotocollen gecontroleerd.' Volgens de bewindspersonen zou potentiële fraude sneller opgespoord worden met profielen voor 'uitkeringssituaties' en ook fenomenen zoals faillissement-, jobcoach- en medische fraude. 'Al deze risicoprofielen worden de komende jaren vergeleken en gedeeld tussen de verschillende partijen in de handhavingketen. Zo wordt een steeds preciezer beeld gekregen van (potentiële) fraudeurs.'[176]

Dit belangrijke Multiregelingensysteem werd echter een ICT-debacle. Externe deskundigen – Johan Hakkenberg, ICT-deskundige en Lieneke Sneller, hoogleraar toegevoegde waarde IT bij Nyenrode Business University – adviseerden om te stoppen met het project, nadat eerder KPMG er negatief over oordeelde. De SVB zegde naar aanleiding van het debacle het contract met bouwer Capgemini op. Navraag bij de SVB leert dat de zaak voor arbitrage is voorgelegd. De SVB bekijkt of en zo ja

175 'Terugblik en vervolg pgb-fraude aanpak, brief staatssecretaris Van Rijn van VWS aan de Tweede Kamer, 29 januari 2015 https://www.rijksoverheid.nl/documenten/kamerstukken/2015/01/29/kamerbrief-over-terugblik-en-vervolg-pgb-fraude-aanpak
Bijlage: Afschrift brief 'Signalering pgb-fraudeonderzoeken Inspectie SZW', 31 oktober 2014 http://www.rijksoverheid.nl/documenten-en-publicaties/brieven/2014/10/31/afschrift-brief-signalering-pgb-fraudeonderzoeken-inspectie-szw.html

176 Brief van minister Asscher en staatssecretaris Klijnsma (beiden SZW) aan de Tweede Kamer over de maatregelen op het terrein van fraude, handhaving en naleving. 4 oktober 2013 https://www.rijksoverheid.nl/documenten/kamerstukken/2013/10/04/kamerbrief-over-fraudeaanpak-handhaving-en-naleving

hoe zij delen van het systeem alsnog kan gebruiken. Er was bijna 44 miljoen euro mee gemoeid tot dan toe.[177]

Het MRS-systeem zou aanvragen en mutatie die aan bepaalde risicoprofielen voldoen, eruit filteren voor nadere handmatige controle en behandeling. Nu dit niet kan, resteert de bestaande methodiek: risicoselectie op basis van risicoanalyse en validerend vooronderzoek. De SVB gaat dit verder professionaliseren in genoemde businesscase.[178]

9.4 HINDERPALEN EN VRAAGTEKENS

De SVB signaleert dat maatschappelijke ophef over (mogelijke) fraude al sturend kan werken: Zo is het goedkoop en eenvoudig om je naam te veranderen in een aantal Oost-Europese landen. Vervolgens zou men hier opnieuw aanvragen voor kinderbijslag of AOW kunnen doen. Dit kwam aan het licht door een rapport van het Nationaal Vreemdelingen Informatie Knooppunt (NVIK) van de politie. De ophef hierover was groot, maar inmiddels blijkt er geen sprake te zijn van daadwerkelijke fraude. Alleen van het risico daarop. 'De ophef hierover bevestigt dat je beter eerst kunt onderzoeken of een in theorie bestaand risico zich in de werkelijkheid ook voordoet, alvorens de alarmbel te luiden. Dat is dan ook de lijn van de SVB.'[179]

Het karakter van fraude is internationaler geworden. Met de toegenomen immigratie en arbeidsmigratie is het belang groter geworden om ook internationale fraudebestrijding te ondersteunen met data-analyse. De SVB werkt sinds de jaren negentig van de vorige eeuw met attachés voor sociale zaken en lokale medewerkers op Nederlandse ambassades. Onlangs zijn er ook lokale medewerkers actief op de ambassades in Polen, Roemenië en Bulgarije. Zij werken samen met de buitenlandse zusterinstellingen en verzamelen informatie ter voorkoming en bestrijding van schijnconstructies en uitkeringsfraude.

177 http://www.svb.nl/int/nl/over_de_svb/actueel_kennis/nieuws/140902_svb_stopt_ontwikkeling_mrs.jsp (Inmiddels verwijderd)
Bijlage 2 - Eindrapport Externe deskundigen - SVB Tien / Ontwikkeling van het Multi Regelingen Systeem (MRS)
https://www.rijksoverheid.nl/documenten/rapporten/2014/12/17/bijlage-2-eindrapport-externe-deskun digen-svb-tien-ontwikkeling-van-het-multi-regelingen-systeem-mrs
'Mislukt MRS levert SVB strop op van 43,7 miljoen', Computable, 2 september 2014
https://www.computable.nl/artikel/nieuws/overheid/5158099/250449/mislukt-mrs-levert-svb-strop-op-van-437-miljoen.html

178 Interview met Paul Burrough, Frits Werner, SVB.

179 Idem.

De SVB heeft ervaren dat fraudebestrijding met gebruik van 'Big Data' niet de enige oplossing is. Het doen van steekproeven kan effectiever zijn. In de meeste gevallen volstaat data-analyse alleen niet, maar vereist het opvolging met veldonderzoeken waaronder huisbezoeken. De capaciteit daarvoor is echter wel begrensd.

Ook de SVB ervaart enerzijds de maatschappelijke en politieke roep om strengere handhaving en anderzijds de zorgen om privacy. Een ontdekte fout met privacy levert direct 'straf' op van de toezichthouder of de rechter. De SVB is dan ook voorzichtig met datamining en gegevensuitwisseling. Voorgenomen activiteiten worden altijd voorafgegaan door een 'Privacy Impact Analyse'. 'Het huidige maatschappelijke klimaat is niet geschikt voor het opzoeken van privacygrenzen of voor experimenten voor handhaving met ongewisse bijeffecten.'[180]
In 2013 vroeg de SVB buitenlandse sofinummers van klanten met als doel vermogen in het buitenland te onderzoeken en daarmee mogelijke onterechte AIO-uitkeringen vast te stellen. Daarop kwam protest van Marokkaanse belangenorganisaties, die meenden dat conform de privacywetgeving alleen bij gerichte verdenkingen data opgevraagd mogen worden en toepassing van een 'sleepnet' in de vorm van analyse van complete bestanden aan buitenlandse uitkeringsgerechtigden onjuist is.
Privacy is een voortdurende zorg van de SVB. Zo kreeg de SVB in 2007 kritiek na een uitspraak van de Autoriteit Persoonsgegevens wegens het gebruik van waterverbruiksgegevens omdat de hoogte van dat verbruik een indicator is voor mogelijke uitkeringsfraude. De wettelijke basis hiervoor bleek bij de SVB te ontbreken. Inmiddels is de wet aangepast en is de SVB wel bevoegd om deze gegevens te gebruiken.

De discussie rond SyRI speelt ook bij SVB. De uitbreiding van wettelijke mogelijkheden met het SyRI-besluit levert de Landelijke Structuur Interventieteams volgens de SVB echter juist een 'privacyveilige' omgeving op voor bestandsvergelijking. Hierin kunnen gegevens worden verwerkt van nutsbedrijven (water, energie) en woningcorporaties (bewoning).
Gebruik van de nieuwe mogelijkheden is nog bescheiden. De Inspectie SZW is nog bezig met een project "dynamisering risicomodellen SyRI" waarin onder andere de SVB en het UWV participeren. Als proef wordt SyRI wel ingezet bij één project van het Landelijk Structuur Interventieteams (LSI).

De SVB doet geen mededelingen over de risicoprofielen die ze hanteert. 'Door middel van *queries* op onze systeembestanden kijken we dan hoeveel en wat voor soort gevallen aan de risicokenmerken voldoen. Door middel van steekproeven

180 Idem.

wordt vastgesteld wat omvang en aard van het risico is en welke handhavingsmaatregelen genomen kunnen worden.'
De SVB gebruikt doorgaans de eigen uitkeringsbestanden en soms die van gelieerde partijen in samenwerkingen. Gevallen met bepaalde kenmerken uit het bestand van een andere instantie houden de SVB-analisten dan tegen de eigen bestanden, teneinde verdachte gevallen c.q. personen te detecteren. Voorbeeld zijn de eerdergenoemde 'windhappers' oftewel spookpersonen van wie nauwelijks iets bekend is, maar die wel een uitkering genieten.
Problemen die optreden zijn tweeledig voor de SVB, juridisch en praktisch: juridisch moet de methode voldoen aan de vereisten van de privacywetgeving. Dat wordt intern bekeken en eventueel met een externe jurist. De praktijk is weerbarstiger: 'Voor een veilige overdracht van data kunnen de verschillende ICT-systemen tot problemen leiden. Bovendien moet je de inhoud van bestanden op elkaar afstemmen. Alle organisaties hanteren begrippen op eigen wijze.'
Neem bijvoorbeeld een veld 'naam' die in administraties heel verschillend ingericht kan zijn qua notering van voor- en tussenvoegsels, voorletters en -voornamen, eigennamen van getrouwde personen, buitenlandse samengestelde namen, et cetera.

De vraag beantwoorden welke concrete resultaten van alle verrichte data-analyses er zijn geboekt, noemt de SVB 'onbegonnen werk'. Wel worden voorbeelden genoemd. Een concreet recent resultaat volgt uit de samenwerking tussen de SVB en de IND, met analyse van in Nederland wonende SVB-klanten met een verblijfstitel en betaling in het buitenland. Daaruit rolden 96 AOW- en 563 AKW-gerechtigden.
De steekproef telde 46 zaken. Bij 15 van de 26 inmiddels onderzochte zaken is de verblijfstitel op basis van SVB-informatie ingetrokken. Welke lessen zijn er getrokken? 'Data-analyse en ketensamenwerking zijn tijdrovend. Samenwerking in de keten vereist grondig overleg in de voorfase om misverstanden te voorkomen. Men moet elkaars taal leren spreken. Wat de één met bijvoorbeeld het begrip "wonen" bedoelt, heeft bij de ander soms een geheel andere betekenis.'[181]

9.5 TOEKOMST

De mislukking van het Multiregelingensysteem en het niet doorgaan van de daarmee beoogde geautomatiseerde risicoselectie zijn voor de SVB geen reden om de voornemens met analyse voor fraudebestrijding op een laag pitje te zetten.
'De lijn en ambitie is nog steeds om zo risicogestuurd mogelijk te handhaven. Dat doen we ook al, ook zonder MRS. Op basis van risico-analyses en validatie van die risico's met voorafgaande onderzoeken met vragen als: bestaan die risico's ook in

181 Idem.

de praktijk? Wat zijn dan de aard en omvang en hoe ondervang je ze het beste? Dat is meer en meer grond voor onze handhavingsmaatregelen de komende jaren.'[182]
Er is extra geld beschikbaar gesteld vanuit de Businesscase Intensivering Toezicht. Uit die businesscase blijkt dat verwachte opbrengsten de voorziene investeringen overtreffen. Naast de intensivering van repressieve toezichtactiviteiten wordt ook geïnvesteerd in de professionalisering van onder meer datamining en risico-analyse, ter verhoging van de effectiviteit van de algehele handhaving. De SVB richt in 2016 een aparte eenheid 'intelligence en risico-analyse' op. Deze unit moet leiden tot verbeterde en meer gedetailleerde risico-analyses, mede op basis van nieuwe vormen van bestandsanalyses. De eenheid moet zich ook richten op digitale fraude.
'De resultaten van de analyses zullen moeten leiden tot verfijnde fraudeprofielen. Vervolgens kunnen we die loslaten op onze bestaande systemen. Dat wil zeggen dat we uit die systemen de gevallen selecteren die voldoen aan die profielen. Dan gaan we validerend onderzoek doen, dus kijken wat aard en omvang van de daadwerkelijke risico's zijn. En dan kun je structurele maatregelen nemen om de risico's te ondervangen, zoals extra controles.'
Naast het vergroten van de 'pakkans' vindt de SVB het ook belangrijk om de preventieve handhaving verder te verbeteren, onder andere door verbeterde informatievoorziening aan klanten en aanpassing van de regelgeving waar die fraudegevoelig blijkt te zijn. Het is vrijwel onmogelijk om de opbrengsten van preventieve handhaving te kwantificeren, dus hier zijn nadrukkelijk geen baten aan verbonden.

De kosten en opbrengsten van de voorstellen in de Businesscase Intensivering Toezicht SVB, die in maart 2015 zijn goedgekeurd[183]:

	2015	2016	2017	2018
Investering	7.500.000	7.300.000	7.300.000	7.300.000
Opbrengst	8.200.000	10.400.000	12.600.000	14.900.000
Resultaat	700.000	3.100.000	5.300.000	7.600.000

De cijfers over de werkelijke kosten en baten in 2015 zijn nog niet beschikbaar. De vaste kosten van de SVB voor het natrekken van externe en interne fraudetips, inclusief die uit analyse, belopen 1,2 miljoen euro per jaar. De opbrengsten vormen hier de som van de besparingen op uitkeringen voor de toekomst en de geïncasseerde teruggevorderde teveelbetalingen en boetes. Die zijn uitgesplitst in de plannen.

182 Idem.
183 Idem.

De voorlopige cijfers en schattingen over 2015 bevestigen dat de opbrengsten gehaald kunnen worden. Wel was 2015 een jaar waarin de investeringen en het starten met de activiteiten om de baten te genereren pas effectief vanaf 1 april, na de goedkeuring van het voorstel in maart, konden worden gerealiseerd. Onbenutte budgetten kunnen worden doorgeschoven. Daardoor kan de feitelijke realisering van de businesscase eventueel doorlopen tot na 2018.

De SVB merkt daarbij vervolgens op dat 'in 2018 de interessante vraag (zal) moeten worden beantwoord of investeringen en activiteiten ook na afloop van deze businesscase – en de uitloop in 2019 – doorlopen en zelfs een structureel karakter kunnen/moeten krijgen. Als de baten inderdaad de kosten overstijgen, zou het onverstandig zijn dit niet te doen. De vraag die daarbij vooral moet worden beantwoord, is of de opbrengsten niet afnemen omdat de "vijver van onrechtmatigheden leeggevist raakt".'[184]

184 Idem.

10 GEMEENTEN

INLEIDING

Vanaf 2007 pogen gemeenten en hun organisaties data-analyse een plaats te geven in de methoden voor bestrijding van onterecht verstrekte WWB-uitkeringen. Regionale adviescentra voor fraudebestrijding, eerst RCF geheten en sinds kort onderdeel van de VNG, waren aanvankelijk zeer optimistisch over de mogelijkheden. Maar de praktijk bleek weerbarstig. Tientallen gemeenten testten verschillende systemen. Hoe pakte dit uit in de praktijk? Waar zijn er wel en waar zijn er geen successen geboekt?
In onderstaande beschrijving wordt minutieus het (glibberige) pad gevolgd dat gemeenten betraden op weg naar data- en risicoanalyse als middel om – al dan niet vermeende – uitkeringsfraude terug te dringen.

10.1 DOELEN

Gemeenten maken bij het voorkomen en tegengaan van misbruik van voorzieningen, zoals de uitkeringen WWB gebruik van het VNG Kenniscentrum Handhaving en Naleving en daarbinnen het Expertisecentrum Sociaal Domein (voorheen; RCF, Regionaal Coördinatiepunt Fraudebestrijding), verder afgekort als VNG KHN.
In 2007 ontving VNG KHN (RCF) grote respons op een uitgebreide enquête naar fraudebestrijding bij sociale diensten. Vooral controle op bestaande uitkeringsgerechtigden vereiste meer en betere instrumenten.
Immers, na de goedkeuring van een aanvraag met strenge toetsing moet de gerechtigde wel wijzigingen melden, maar vindt er geen toetsing meer plaats. De Autoriteit Persoonsgegevens gaf in 2007 het ministerie van SZW groen licht om vanuit gekoppelde databestanden gedurende twee jaar risicoprofielen te ontwikkelen voor bestrijding van uitkeringsfraude. De profielen moesten objectiveerbaar zijn, niet tot individuen herleidbaar.
De verwachtingen van dit 'informatiegestuurd handhaven' (IGH) of 'analysegestuurd handhaven' waren aanvankelijk bij lokale bestuurders hooggespannen. Zo liet wethouder Eric Faassen van Capelle voorafgaand aan een test met VNG Kenniscentrum H&N in data-analyse optekenen: 'We gaan van tandenborstels tellen naar de digitale stofkam bij het bestrijden van bijstandsfraude.'[185]

Gemeenten werden ook vanuit de Rijksoverheid aangespoord. Ze schoten tekort bij fraudecontrole van WWB-uitkeringen, schreef VVD-staatssecretaris Paul de

185 http://www.capelleaandenijssel.nl/over-capelle-aan-den-ijssel/capelse-courant_3183/item/bijstands fraude-sneller-zichtbaar_16659.html, 14 december 2015.

Krom in 2011 en 2012 aan de Tweede Kamer ter motivatie van nieuwe wetgeving om handhavings- en sanctiebeleid op het SZW-domein 'aan te scherpen'.[186] De Kamer onderschreef breed de noodzaak om uitkeringsfraude terug te dringen: het percentage fraudeurs met verwijtbare vorderingen boven de 25.000 euro in de bijstand was gegroeid van 7,0 procent in 2008 naar 7,7 procent in 2010.
Er was daarnaast echter vooral sprake van een groeiende groep van grote fraudeurs. Het grootste openstaande terug te vorderen bedrag aan fraude van de overheid in 2011, ongeveer 500 miljoen euro, betrof de WWB.
Bij het UWV stond eind 2011 voor ongeveer 300 miljoen euro aan vorderingen open en bij de SVB 90 miljoen euro, waarvan steeds een deel als gevolg van fraude. In 2010 was er voor 119 miljoen euro aan socialezekerheidsfraude geconstateerd, waarvan voor 53 miljoen euro aan fraude met WWB-uitkeringen.
'Dit is diefstal van gemeenschapsgeld en een aanslag op de solidariteit van het socialezekerheidsstelsel.' De bewindsman beloofde strengere sancties en meer mogelijkheden voor huisbezoek en voor datakoppeling.
Zo had de rechter net goedgekeurd dat gemeenten data over huishoudelijk waterverbruik mogen gebruiken om verdenkingen van fraude op te sporen, bijvoorbeeld van zwart werk als thuiskapper. Of samenwonen van een WWB-gerechtigde met kinderen met een studietoelage of met een verdienende partner.
De Krom liet in oktober 2011 aan de Kamer weten dat een inventarisatie van SZW, gemeenten, het UWV en de SVB met succes mogelijkheden hadden verkend van een bredere inzet van gegevensuitwisseling om fraude te voorkomen en te bestrijden. De gemeenten werden gestimuleerd door middel van een 'Verzamelbrief'.[187] De meeste maatregelen lagen op het terrein van de gemeenten en waren mogelijk binnen de huidige wet- en regelgeving. Een aantal maatregelen voor 'verbetering van bestandskoppeling' noodzaakte wel tot een wetswijziging. De regering streefde ernaar deze in het najaar van 2012 aan de Tweede Kamer voor te leggen.
Juist in het combineren van data schuilt een groot potentieel voor fraudedetectie, zo schreef De Krom: 'Om te zorgen dat gemeenten over voldoende gegevens beschikken om fraude te kunnen voorkomen, te ontdekken en te bestraffen, is het uitwisselen van gegevens een belangrijk instrument. Voor gemeenten is het daarom cruciaal om de mogelijkheden van bestandskoppeling goed te benutten.'
Gewezen werd op een intensiever gebruik van de 'inkijkfunctie van SUWI-net Services' bij beoordelingen van aanvragen voor een WWB-uitkering. Deze worden verschaft door de BKWI, die gegevens ophaalt bij het UWV, de SVB, gemeentelijke sociale diensten, de RDW, het Kadaster, DUO en de Kamers van Koophandel. Voor beoordeling van bezit en inkomsten van bestaande uitkeringsgerechtigden moes-

186 http://www.tweedekamer.nl/kamerstukken/detail?id=2012Z05627&did=2012D25730
http://www.tweedekamer.nl/kamerstukken/kamervragen/detail?id=2011Z17249&did=2011D47636

187 Verzamelbrief special fraudebestrijding
http://www.tweedekamer.nl/kamerstukken/detail?id=2012D10640&did=2012D10640

ten gemeenten intensiever gebruik gaan maken van de data van het Inlichtingenbureau (zie ook hoofdstuk 5).

In 2012 ging het IB over langere perioden inkomen, vermogen en transacties analyseren, beloofde de staatssecretaris. Nieuwe signalen voor voertuigbezit, bankrekeningnummers en toeslagen werden geïntroduceerd, en later ook nieuwe signalen voor woon- en leefsituatie en gezinsinkomen. De Krom gaf als voorbeeld het meermalen achtereen een auto inruilen dat tot de 'codering verdenking van handel' leidt. Onder de kop 'Wat gaan we mogelijk maken?'
Ook zouden spoorloze debiteuren bij gemeenten beter in beeld komen; 70 procent van hen genoot immers een uitkering. Op verzoek van Rotterdam heeft het IB de handmatige, arbeidsintensieve speurtocht vervangen voor een geautomatiseerd 'volgen' van de spoorloze debiteuren met bestandskoppelingen, door verbetering van adresregistratie en opsporing van fouten in de BRP met data uit de UWV Polisadministratie (zie hoofdstuk 11).[188]

Er waren wel privacyvraagstukken. Zo twijfelden gemeenten of ze via KvK-bestanden persoonlijke data voor WWB-controle en opsporing mochten gebruikten. De staatssecretaris gaf zijn fiat. Ook werd het licht op groen gezet om de gegevensuitwisseling van het UWV aan gemeenten wettelijk mogelijk te maken. De Autoriteit Persoonsgegevens had de proef van Amsterdam met adrescontrole met de UWV Polisadministratie immers afgekeurd.
Gemeenten werden gemaand om het inzage- en correctierecht beter te hanteren. De beveiliging van bestanden bleek bij honderd gemeenten echter te wensen over te laten. Zorgvuldig gebruik van gegevens uit SUWI-net Services liet ernstig te wensen over. Er startte een campagne, maar nog tot in juni 2015 werd misbruik en 'lekkage' vastgesteld.[189]

10.2 OPZET SYSTEMEN

De uitvoering van de besluiten op gemeenteniveau werd opgepakt door VNG KHN (toen nog RCF) in samenwerking met de Inspectie SZW. Informatiegestuurd Handhaven (IGH) betekende het koppelen van bestanden, teneinde risicoprofielen te genereren voor bestrijding van uitkeringsfraude, oftewel: databestanden in de 'wasmachine' met kansrijke verdenkingen als resultaat. Met verder als bijkomende gevolg goedwillenden minder lastig te vallen met onnodige controles.

188 http://www.tweedekamer.nl/kamerstukken/detail?id=2013D16427&did=2013D16427
189 Interviews met Hans Berkhout en Ad van Mierlo van VNG KHN.
'Ambtenaren misbruiken digitaal klantdossier', Argos, Vpro, 20 juni 2015
http://www.vpro.nl/argos/media/afleveringen/2015/Lek-Suwinet.html

VNG KHN onderscheidt verschillende onderzoeken:
- Themaonderzoeken gaan over een enkelvoudige kwestie. Bijvoorbeeld waterverbruik, autobezit en bijstand, of niet-erkende kinderen die geboren zijn in de bijstandsperiode.
- Fenomeenonderzoeken zijn – net als themaonderzoeken – gericht op enkelvoudige zaken, zoals tupperwareparties, ballonvaarten of Ubertaxis. Kenmerk is dat deze vaak alleen maar goed via internet zijn te onderzoeken.

Bestandsrisico's worden zichtbaar door een bijstandsbestand met allerlei gemeentelijke en landelijke bestanden te vergelijken op basis van vooraf gedefinieerde risico-indicatoren, ofwel vragen op basis waarvan je de bestanden vergelijkt. Deze methode werkt met massa's gegevens: het uitkeringenbestand met honderden namen wordt vergeleken met de BRP (het vroegere GBA), gemeentelijke belastinggegevens, Kadaster, vergunningen en dergelijke. Dit levert hits op in een lijst met risico's van hoog tot laag. Doelmatigheidsrisicosystemen zijn gericht op de inschatting van de kans van personen om weer uit een uitkering te geraken en aan het werk te gaan.

VNG KHN hanteert drie eenvoudige criteria voor IGH:
- voldoende kwaliteit van data;
- kwaliteit van analysemethoden;
- kwaliteit van personeel.

Bovendien moet een systematiek passen bij de gemeente. Om die reden stelt VNG Kenniscentrum H&N momenteel eerst met gemeenten scenario's vast alvorens aan de opbouw van een methode en eventueel onderliggend systeem te beginnen. Hieruit zijn SyRI, Alert en SmartBox voortgekomen als systemen voor vergelijking van grote uitkeringsbestanden met relevante gemeentelijke en landelijke bestanden. SyRI was bedoeld voor eenmalig gebruik bij gemeenten, Alert had een projectmatige aanpak voor één of enkele malen, terwijl SmartBox een structureel gebruik van data voorstond met een 'vaste' aansluiting op de datasystemen van de gemeente.

Voor het Informatiegestuurd Handhaven werkten VNG KHN en de Inspectie SZW samen aan indicatoren om tot risicoclassificaties te komen met een stoplichtmodel; rood-oranje-groen.
Deze theoretische uitgangspunten vormden de basis voor twee systemen: SmartBox Info Support in Veenendaal, maker van business intelligence software en Alert van Capgemini in Utrecht. Ze komen hieronder ter sprake.

10.3 UITVOERING

Info Support ontwikkelde met VNG KHN de SmartBox om databestanden te koppelen en via kruisverbanden suggesties voor verhoogd risico te leveren. SmartBox is getest in Zoetermeer, Westland en Capelle a/d IJssel. In 2013 besloten de gemeenten Den Haag en Delft om SmartBox in een 'light-versie' te gaan gebruiken, met louter invoer van data van het Inlichtingenbureau en de Sociale Dienst. Bij beide gemeenten kwam vanuit de politiek de aansporing om meer te doen aan fraudebestrijding.
SmartBox zou signalen opleveren over inkomens-, samenwoon- of vermogensfraude: combinaties van familieverbanden, vakantiebestemmingen, beroepen, aanvragen van rijbewijzen en bouwvergunningen. Om zo veel mogelijk fraudegevallen te detecteren zou Info Support per gemeente het systeem optimaliseren. Een licentie kostte 20.000 euro.[190]
'Een voorbeeld is het aantal keren dat iemand op vakantie gaat naar het land van herkomst, voor lange perioden van bijvoorbeeld zes weken. Eén keer hoeft niet zo erg te zijn, maar als iemand elk jaar gaat naar één bepaald adres, dan kan het interessant zijn om het vermogen in het buitenland te onderzoeken', aldus een chef Handhaving in Den Haag. Een ander voorbeeld zijn 'aanvragen van bouw- of parkeervergunningen, die duiden op vermogen, van marktvergunningen, die duiden op handel. Of neem meldingen van woonoverlast zoals burenruzies. Als daar steeds een nieuwe partner aan meedoet, is dat wel raar.'[191]
SmartBox zou ook de data van fraudegevallen van afgelopen jaren moeten bevatten. 'Waar je nu zegt: hij is niet warm genoeg, deze pakken we niet op, kan hij opnieuw naar voren komen met nieuwe signalen dankzij verrijking van de data […], nu verdwijnt dat eigenlijk. Nu prioriteren we hem dan niet en verdwijnt hij weer uit beeld. Goede fraudeurs pak je niet zomaar.'[192]

Ook de gemeente Delft ging enthousiast aan de slag met SmartBox, nadat de gemeenteraad B&W maande om werk te maken van vermindering van bijstandsfraude. Delft stopte de data van het IB plus eigen bestanden van de Sociale Dienst in de SmartBox, waarna indicatoren die op fraude kunnen wijzen, werden losgelaten op de data, zoals bezit van voertuigen, vermogen, leefvorm, het al dan niet aangevraagd hebben van bijzondere bijstand. De expertise voor het vaststellen van de indicatoren en behandeling van resultaten komt vooral van de fraudeambtenaren intern. Zij kennen de risicofactoren die op fraude kunnen wijzen uit hun praktijk. De burgerservicenummers die eruitrollen, worden aan nader onderzoek onder-

190 Interview met Hans Berkhout en Ad van Mierlo, VNG KHN.
191 Verdacht door data – Van tandenborstels tellen naar datafuiken, iBestuur, 2 oktober 2014 http://ibestuur.nl/magazine/verdacht-door-data (geraadpleegd 16 februari 2016).
192 Idem.

worpen, administratief, telefonisch, met een afspraak aan de balie of met bezoek van opsporingsbeambten.[193]

Slimme datadoos

SmartBox bracht in potentie zo'n veertig dataverzamelingen samen, maar het werkelijke aantal was afhankelijk van de wensen en technische mogelijkheden van koppeling bij de gemeenten. Via draaischijf Inlichtingenbureau krijgen gemeenten maandelijks signalen uit de bestanden van het UWV, de SVB, de Belastingdienst, DUO, JustID, het CJIB en de RDW, te weten:

- inkomsten uit heffingskortingen;
- voertuigbezit;
- storingen rechtmatigheidscontrole;
- signaal voor beoordelen aanvraag bijstandsuitkering;
- inkomsten uit inkomstenverhouding;
- recht op studiefinanciering;
- overschrijding vermogensgrens;
- uitkering in andere gemeente;
- indetentiename;
- voortvluchtig veroordeeld;
- inschrijving hogeschool of universiteit;
- overzicht bankrekeningen.

De gemeente tracht eigen bestanden geschikt te maken voor bundeling en analyse binnen een systeem als bijvoorbeeld SmartBox, bijvoorbeeld:

- detenties;
- bankrekeningnummers op naam;
- uitkeringen bij andere instanties of gemeenten;
- gemeentelijke OZB-belastingen;
- niet-aangevraagde bijzondere bijstand;
- eerdere fraudesituaties;
- veranderingen in gezins- en woonsituaties;
- aanvraag bouwvergunningen;
- hondenbelastingen;
- aanvragen vakanties uitkeringsgerechtigden;
- fraude-informatie uit het verleden;
- re-integratie trajecten, afgebroken of niet meer verschenen;
- openstaande schuldenposities;
- aangevraagde, maar niet afgewikkelde schuldsaneringen.

Data gaan de SmartBox in op naam en met sofinummer, en worden vervolgens geanonimiseerd alvorens de analyse plaatsvindt aan de hand van ingebrachte indicatoren. Vooral het optreden van combinaties van factoren, bijvoorbeeld het bezit van drie honden (hoge belasting), een duurdere auto en verre vakantiebestemmingen en/of aanvragen van bouwvergunningen kunnen leiden tot verdenkingen van inkomens-, samenwoon- of vermogensfraude. Maar ook aangegeven geboorten zonder vader of nooit aangevraagd hebben van bijzondere bijstand kunnen risico-indicaties van dit IGH vormen.

193 Interview met Reggie Bosch, Projectleider/Teamcoördinator van de gemeente Delft.

De weegfactoren verschillen: elke indicator (hit) krijgt een getal naar gewicht. Een hit op inkomen weegt bijvoorbeeld veel zwaarder dan die van de hondenbelasting. Maar vele kleine hits kunnen wel een interessant risico aangeven. Bovendien was de opzet zodanig dat naar verwachting het effect van de inzet van data-analyse zou groeien, naarmate profielen dynamischer zijn, dus permanent worden aangepast op grond van nieuwe analyses.[194]

Hokjes: gedeprimeerden en onaantastbaren

VNG KHN noemde op het najaarscongres 2013 van Divosa zes globale typen fraudeurs naar hoofdmotief:

1. gemakzuchtigen: financieel gewin;
2. actieve WWB'ers: financieel gewin;
3. onafhankelijke vrouwen: financiële onafhankelijkheid;
4. gedeprimeerden: ongevoelig voor risico's;
5. onaantastbaren: financieel gewin;
6. klanten die worden gebruikt: financieel gewin (van derden).

Type klantgedrag en karakterisering van fraudeurtype zijn als volgt:

1. Wel willen werken, wel kunnen werken:
   actieve WWB'ers, onafhankelijke vrouwen;
2. Wel willen, niet kunnen: onafhankelijke vrouwen;
3. Niet willen, wel kunnen: actieve WWB'ers,
   gemakzuchtigen, onaantastbaren;
4. Niet willen, niet kunnen: gedeprimeerden en klanten
   die worden gebruikt door derden.

Deze krachtige wijze profilering is momenteel niet van toepassing in het IGH van VNG KHN, maar geeft een indicatie van het denken in de praktijk over profilering in fraudeaanpak.[195]

Het tweede systeem voor data-analyse door gemeente, Alert, is onder leiding van VNG KHN samen met Capgemini in 2009 getest met populaties bijstandsgerechtigden in Utrecht en vervolgens in 2010 en 2011 in Tilburg, Nijmegen, Middelburg, Hilversum, Amersfoort, Leiden en Almere.
De steden Utrecht, Groningen, Zwolle, Tiel en Drechtsteden gingen zelfstandig met Alert aan de slag, plus enkele passief deelnemende steden.
Het betrof testen met 'geautomatiseerde risicosignalering' met inbreng van verschillende bestanden: BPR (GBA), uitkeringsregistratie, frauderegistraties en

---

194 Interviews met Hans Berkhout en Ad van Mierlo, VNG KHN.
Infosupport productinformatie www.infosupport.com
'Verdacht door data - Van tandenborstels tellen naar datafuiken, iBestuur, 2 oktober 2014 http://ibestuur.nl/magazine/verdacht-door-data (geraadpleegd 16 februari 2016).

195 Voordracht 'Werkwijzer "Handhaving rechtmatigheid en arbeidsverplichtingen", Peter Haas en Wim Heersink van VNG Kenniscentrum H&N
https://www.divosa.nl/sites/default/files/bijeenkomst_bestanden/112_vakmanschap_is_ook_handha ving.pdf

externe bestanden van RDW (kentekens). Op basis van een set – geheim gehouden – indicatoren kwamen 'cliënten' in een stoplichtmodel: rood (hoog risico op fraude), groen (laag risico) en oranje (gemiddeld).

10.4 RESULTATEN

Het aantal dankzij toepassing van Alert bespaarde uitkeringen was gering, 17 (Tilburg) en 3 (Leiden), met volgens VNG KHN een kleine 1,2 miljoen euro aan opbrengsten gerekend over meerdere jaren. Echter, ruim een derde van de uitkeringen was al gestopt om andere redenen.
Alert kwam gezien de resultaten niet echt van de grond. De gemeenten lieten het systeem links liggen, met uitzondering van beperkt gebruik in Utrecht, Tiel en Zwolle. De laatste meldde over 2013 bij 1,7 miljoen euro kosten een opbrengst van 2 miljoen euro aan stopgezette uitkeringen. Het effect van de inzet was niet conform verwachtingen. In 2014 leidde het stopzetten van uitkeringen nog slechts tot 1 miljoen aan besparingen. Bij 78 van de 120 stopgezette uitkeringen speelde bestandsvergelijking een rol.[196]

Verder bleek het hanteren van het systeem dermate complex dat gemeenten afhaakten. Grootste belemmering was het gebrek aan kennis om de benodigde data uit de gehele gemeente bij elkaar te krijgen. Dat was mede te wijten aan uitbesteding van systemen en databeheer.
Met Alert liep het ondertussen ook mis bij een project van VenJ. Alert was bovendien inzet van een rechtszaak. Een tweede betrokken partij bij de ontwikkeling van Alert, CMC Consultants, betwistte het intellectueel eigendomsrecht van Capgemini. Zowel het vonnis van de rechtbank Den Haag als het vonnis van het Hof begin 2014 pakte in het voordeel van Cap uit. VNG KHN was van deze kwesties niet op de hoogte, want bij de overheid ontbreekt coördinatie van de initiatieven in data-analyse.[197]
Bij de eerste testgemeenten ging het werken met het systeem SmartBox al minder goed dan gehoopt, vooral een gevolg van het vergaren en bundelen van de benodigde data. Ook hadden medewerkers moeite met het werken met de uitkomsten. Verwachte resultaten bleven uit. Zo liet wethouder Marga de Goeij van Westland weten: 'De resultaten zijn tegengevallen en het gebruik is tijdrovend.'[198]

---

196 Ruim 1 miljoen aan uitkeringsfraude opgespoord, nieuwsbericht Gemeente Zwolle, 16 februari 2015 https://www.zwolle.nl/actueel/ruim-1-miljoen-aan-uitkeringsfraude-opgespoord (geraadpleegd 18 februari 2016). Toelichting gemeente Zwolle.

197 Uitspraak Gerechtshof Den Haag 28 januari 2014 http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:GHDHA:2014:71.

198 Geciteerd in 'Verdacht door data - Van tandenborstels tellen naar datafuiken, iBestuur, 2 oktober 2014 http://ibestuur.nl/magazine/verdacht-door-data (geraadpleegd 16 februari 2016).

In Delft ontstond vertraging, als gevolg van organisatorische problemen en het ontbreken van deskundigheid in het bijeenbrengen van de benodigde data. De testperiode is met een jaar verlengd.
Het resultaat was tot nu toe stopzetting van drie uitkeringen, op een totaal van zo'n drieduizend. De kosten bedragen zo'n 20.000 euro per jaar voor het systeem. Delft noemt dit 'een bescheiden succes' en inmiddels is het besluit genomen om door te gaan met de inzet van dit systeem. De gemeenteraad was hier niet bij betrokken, evenmin bij het besluit om juist dit systeem aan te schaffen.
Den Haag zet SmartBox nog steeds in, maar belangrijker voor fraudebestrijding dan Big Data blijken 'little data', waarbij privacy overigens per definitie wordt geschonden: tips van buren en kennissen, geuit via bijvoorbeeld kliklijnen: de gemeente Den Haag ontving 3300 fraudetips over WWB-uitkeringen in 2012 en ruim 10.500 in 2013. Dit leverde een veel belangrijker bijdrage aan de 760 gestopte uitkeringen in 2013 (op een totaal van 20.000) dan de SmartBox. B&W van Den Haag meldde eind mei 2015 dat fraudebestrijding in 2014 veel succesvoller was dan in 2013, maar niet door de inzet van de Smartbox. Die wordt nog steeds wel gebruikt, maar op een bescheidener wijze:
'Smartbox wordt gevuld met variabelen die zijn geselecteerd op basis van succesvol aangetoonde fraudezaken in Den Haag. Uit deze fraudezaken zijn overeenkomende kenmerken gehaald die tot op zekere hoogte een voorspellende waarde hebben voor het vaststellen van fraude.'[199]
Eigen informatie over uitkeringen uit het verleden en signalen van het IB zijn met behulp van Smartbox in één overzicht naast elkaar gezet.

Het Forensisch Instituut (NFI) onderzocht in opdracht van Den Haag datacombinaties om fraudekansen te kunnen voorspellen. Ook moest er een vaste methodologie komen op grond waarvan B&W van Den Haag een voorstel voor invoering van data-analyse kon doen aan de gemeenteraad.
Een goed werkend systeem zou ook voor andere gemeenten ter beschikking kunnen komen, zo luidde de verwachting. In elk geval binnen de G4, voor Amsterdam, Rotterdam en Den Haag, die interesse toonden.
Het NFI onderzocht of het combineren van data uit een aantal gemeentelijke systemen plus IB-signalen een 'fraude-voorspellende waarde' zou hebben. Het NFI ging verder na welke risicofactoren samenhangen met fraude en vervolgens hoe deze in de praktijk konden bijdragen aan het opsporen van fraude, met mede scherpere risicoprofielen als beoogd eindproduct. De conclusie was negatief: koppeling van andere gemeentelijke systemen zou niet direct tot betere risiscoprofielen en meer en betere fraudedetectie leiden.[200]

199 Gemeente Den Haag, verslaglegging Dienst Werk en Inkomen.
200 Interview VNG KHN, uitkomsten onderzoek NFI niet openbaar.

SmartBox was in het voorjaar van 2015 nog bij slechts enkele gemeenten – volgens de leverancier bij Den Haag en Delft – in gebruik, Alert in het geheel niet meer, ondanks een positieve en optimistische Eindrapportage Analysegestuurde Handhaving van VNG KHN.
Vooral de indicatoren aantal voertuigen, leeftijd, burgerlijke staat, aantal kinderen en aantal trajecten bleken belangrijke signalen te kunnen opleveren voor vermoedens van fraude. Ook nationaliteit gaf relevante signalen, maar met gebruik daarvan waren gemeenten terughoudend.
Belangrijk was de conclusie dat de kwaliteit van de data, van de software en van de medewerkers 'op peil' moet zijn. Met andere woorden: aan de voorwaarden voor kwaliteit werd in het geheel niet voldaan, er was veel geleerd van een serie mislukkingen.
De praktijk bleek immers weerbarstig. Technisch gezien was het inbrengen van verschillende databestanden en invulling van de benodigde velden een grote hobbel. In de praktijk was het euvel om geschikte en vooral schone bestanden te hanteren een nog veel groter obstakel gebleken.
Tests in de gemeenten toonden aan dat bestanden niet aansloten, moeizaam te koppelen waren en/of geen direct beschikbare data bevatten. Ook bleken uitkomsten van exercities vaak niet werkbaar: een te kleine 'hit' (weinig personen) levert onvoldoende op, een te grote hit vergt te veel onderzoek bij individuen. Daaruit is de les getrokken dat het gebruik van minder data tot een hogere succesfactor zou kunnen leiden, en bovendien beter tegemoet komt aan privacybezwaren.
Dit staat haaks op het Big Data-uitgangspunt dat oorspronkelijk is gehanteerd: hoe meer databestanden ingebracht, des te groter de kans op geschikte uitkomsten.
Vooral de formulering van indicatoren luistert nauw. Gemeenten ontberen ervaring en deskundig personeel in het formuleren van de juiste analysevragen. Bovendien is uit basale data nog veel informatie te halen zonder de alomvattende koppeling van bestanden. Er is veel 'laaghangend fruit' dat over het hoofd wordt gezien en dat bij minder inspanning geoogst kan worden.

De voorkeur voor hanteerbare systemen op gemeenteniveau bleek ook uit het kortstondige, grote succes van systeem DPS: Diagnose-, Plan- en Sturingsinstrument. Na een bericht over het 'Bijstandswonder van Boxmeer' stonden gemeenten in de rij om DPS te gaan toepassen. Boxmeer slaagde erin om aan de hand van risicoprofielen de uitstroom van WWB-ontvangers te verhogen en de instroom te beperken.
Combinatie van data en analyse op grond van eenvoudige analyse – op grond van 'gezond verstand' – bepaalden het succes. Zo werden beroepen gefilterd met een hoog frauderisico zoals – al dan niet werkloze – kapsters, bouwvakkers of automonteurs. De meerderheid van de gerechtigden met kleine fraudekans werd daarop minder lastiggevallen.
Vervolgens konden echter vooral grote gemeenten niet met DPS uit de voeten gezien de omvang van hun bestanden.

Er ontstonden vaak problemen met de data zelf en de verwerking, zodat IGH (informatiegestuurd handhaven) ook met behulp van dit systeem nog niet van de grond kwam. Dat viel samen met gebrekkige kennis en ervaring met data-analyse. Bovendien waren in dit geval de fraudesignalen vooral direct op individuen gericht en niet op risicopatronen voor een hele groep.[201]

10.5 PRIVACYKWESTIES

Bij de ontwikkeling van Alert in samenwerking met de steden was er ondersteuning van een privacyjurist om de grenzen vast te stellen van wat juridisch verantwoord is. De Autoriteit Persoonsgegevens heeft verder een 'normoverdragend gesprek' gevoerd met de makers van SmartBox om de wettelijke eisen extra onder de aandacht te brengen. Dit impliceerde geen goed- of afkeuring.
De AP velt louter concrete oordelen ingeval van behandeling van een klacht. Gemeenten waren onzeker over privacy en bestandskoppeling, mede als gevolg van verschillende geluiden, bijvoorbeeld voor het veelvuldig genoemde 'Waterproof' over energieverbruik.
In 2004 werd deze methode voor het eerst toegepast met data van de waterleverancier in Overijssel. De stad Groningen coördineerde Waterproof in de noordelijke provincies, met toepassing in 65 gemeenten. De AP oordeelde in 2007 dat de methode in strijd was met de privacywetgeving.[202] Maar in april 2010 oordeelde de Centrale Raad van Beroep – de hoogste bestuursrechter – in een zaak van de gemeente Hoogeveen dat deze bestandskoppeling niet onwettig is.[203]
Vooraf is een melding richting de AP gegaan over het koppelen van bestanden voor onderzoek. Immers, gegevens worden verwerkt door softwarebedrijf Info Support, die de data niet mag gebruiken. Dit is vervolgens vastgelegd in een bewerkersovereenkomst. Daarmee wordt aan de wet voldaan, maar dit voorkomt geen mogelijke privacyschending.

SmartBox en Alert leverden ook onderzoeksthema's die gevoelig liggen. Er wordt niet op etniciteit geselecteerd, maar indirect kunnen allochtonen op grond van

---

201 'Het bijstandswonder van Boxmeer', Binnenlands Bestuur, 4 februari 2011
http://www.binnenlandsbestuur.nl/sociaal/achtergrond/achtergrond/het-bijstandswonder-van-box meer.699608.lynkx

202 https://www.APweb.nl/nl/nieuws/bestandskoppeling-voor-fraudebestrijding-water proof-onrechtma tig-%C2%A0 persbericht
'Bevindingen ambtshalve Operation Waterproof', 29 mei 2007
https://www.APweb.nl/sites/default/files/downloads/uit/z2006-00476.pdf

203 http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:CRVB:2010:BM3881
Bijvoorbeeld toegepast in Brabantse gemeenten met bestanden van Brabant Water.
http://www.binnenlandsbestuur.nl/sociaal/nieuws/waterverbruik-leidt-tot-stopzetting-uitkering.9074070.lynkx

vakantiebestemmingen, vakantieduur en/of gezinsgrootte wel min of meer als groep worden geformuleerd vanuit de indicatoren.
Zoals blijkt uit het voorbeeld van de indicator 'langere vakanties in hetzelfde land', dat ook de factor etniciteit in beeld kon brengen met vakantie naar het thuisland door allochtonen. Gemeenteraadslid Fatima Faïd van de Haagse Stadspartij had kritiek op de stigmatiserende werking van controles op familiebezoek gedurende vakantieperiodes: 'Gaat SmartBox deze mensen aanmerken als potentiële fraudeurs? Komen mensen van niet-Nederlandse afkomst vaker dan anderen onterecht in de statistieken als mogelijke fraudeurs?'
Ook vreesde zij een jacht op buitenlanders – 140 nationaliteiten – wonend in Den Haag die op familiebezoek gaan. Volgens Den Haag waren louter de voor WWB-gerechtigden verplichte meldingen van vakanties van belang als een van de mogelijke indicatoren.[204]

Gemeenten laveren bij de uitvoering van de sociale wetten tussen de maatschappelijke roep om harder op te treden en privacyregels. Transparantie en accountability zijn onvoldoende uitgewerkt en democratische controle op toepassing van nieuwe gemeentelijke systemen schiet tekort.
Temeer daar ambtenaren voor het dilemma staan dat geheimhouding van methoden op gespannen voet staat met het afleggen van verantwoording. Sociale Zaken van Den Haag verwoordde het in de pers zo: 'We hebben nog honderd voorbeelden, maar we willen de fraudeur niet op voorsprong zetten. Hierover wensen wij niet te communiceren, omdat we ons eigen succes in de wielen kunnen rijden. We kiezen niet voor groot uitmeten van onze methoden, want daarmee verliezen wij onze voorsprong op de klant die we nu opbouwen.'[205]

De uitkomsten, signalen of risico's die de data-analyse met systemen als SmartBox oplevert, worden vervolgens opnieuw gekoppeld aan personen, met hun naam en BSN-nummer. Kenmerk van dit systeem is immers dat alle data geanonimiseerd worden vóór koppeling, maar dat de 'hits' daarna worden gebruikt om personen op naam (en BSN) te selecteren die aan de gevonden kenmerken voldoen. Ze vormen concrete verdenkingen om nader onderzoek naar te doen.
Volgens VNG KHN is elke privacypijn bij toepassing van de SmartBox echter a priori voorkomen. 'De gegevens die in eerste instantie worden getoond, zijn anoniem. Pas op het moment dat besloten wordt dat nader fraudeonderzoek is geïndiceerd, worden de persoonsgegevens erbij gehaald', aldus B&W van Den Haag. In principe worden de 'negatieve' resultaten, dus personen die geen extra verdenking

204 Geciteerd in 'Verdacht door data - Van tandenborstels tellen naar datafuiken, iBestuur, 2 oktober 2014 http://ibestuur.nl/magazine/verdacht-door-data (geraadpleegd 16 februari 2016).
205 Geciteerd in idem.

opleveren, steeds 'weggegooid', voordat ze voor degenen die het systeem hanteren, zichtbaar zijn geweest.
Dat is een voorwaarde van de Autoriteit Persoonsgegevens. Officieel werkt het systeem louter 'realtime': data combineren, indicatoren formuleren en louter de ene uitkomst gebruiken voor nadere 'risico's' ofwel verdenkingen. Echter, juist de opbouw van historische gegevens op grond van een reeks analyses kan extra signalen voor verdenkingen opleveren.
Dit 'in beeld houden' of profileren van WWB-klanten met een hogere kans op fraude staat op gespannen voet met privacywetgeving. Er is geen helder beeld over de bewaarperiode van uitkomsten en van het combineren van verschillende uitkomsten over een langere periode.
Bovendien krijgen gemeenten met de decentralisatie ('3D') van de Wmo en Jeugdzorg nieuwe taken, maar ook bestanden die kunnen bijdragen via profilering per persoon beter overzicht te krijgen. Veel van de WWB-uitkeringen gaan samen met zorgbehoeften. Er ontstaan nieuwe behoeften en mogelijkheden voor fraudeonderzoek. Met de inventarisatie wordt nu een begin gemaakt.[206]

Gemeenten staan volgens VNG KHN huiverig tegenover IGH als gevolg van onduidelijkheid van regeringswege over het koppelen van data om fraude op te sporen. Dit maakt het vervolgens voor commerciële partijen moeilijk om systemen te blijven ondersteunen. Weliswaar heeft SZW zelf bestandskoppelingen met het systeem SyRI wettelijk geregeld, maar op gemeenteniveau is fraudeonderzoek op grond van data-analyse hierdoor niet zondermeer gedekt. De regering heeft tot nu toe volgens VNG KHN nagelaten helderheid te scheppen. 'Mag je wel koppelen, welke bestanden betreft dat dan en welke beslist niet, mag het structureel?'[207]
De Autoriteit Persoonsgegevens geeft zelf ook alleen maar achteraf aan of het gebruik van data en datakoppelingen (in projecten of systemen) conform de Wet bescherming persoonsgegevens was of niet. Deze onduidelijkheid is niet weggenomen met de wetgeving rond SyRI. Nagelaten is aan te geven wat een gemeente zelf mag (dus los van een samenwerkingsverband) op het gebied van datakoppelingen. Hoever mag het werken met systemen als SmartBox en Alert gaan om niet op gespannen voet te staan met de Wbp?
SyRI-wetgeving is volgens VNG KHN, dat namens gemeenten deelneemt in de toepassing, geen legitimatie van Big Brother, integendeel: VNG KHN, vindt dat met de komst van de wetgeving juist voldoende waarborgen voor privacy zijn ingebouwd, die de toepassing van het systeem zonder wetgeving ontbeerde.

206 Interviews Hans Berkhout en Ad van Mierlo, VNG KHN.
207 Interviews Hans Berkhout en Ad van Mierlo, VNG KHN.

10.6 TOEKOMST

Er heerst de nodige onzekerheid bij gemeenten over toepassing van (Big) Data-analyse. Koppelen van veel databestanden staat op gespannen voet met het proportionaliteitsbeginsel van de Wbp. Een adviseur Cap stelde vast: 'Veel gemeenten en instanties stellen zich Roomser dan de paus op uit angst een slechte naam te krijgen. Ze worden gek van de grenzen die juristen hun opleggen vanuit de privacywet […] want het is een ratrace met aan de ene kant personen die de overheid misbruiken als een flappentap en steeds nieuwe methoden bedenken, en aan de andere kant instanties die te weinig mogen om dat te bestrijden dan wel denken dat ze te weinig mogen om dat te bestrijden.'[208]
Wellicht is eerder sprake van het intensiveren van relationele data-analyse dan van Big Data-analyse. De laatste geeft informatie, in dit geval risicoprofielen, op grond waarvan via nader onderzoek specifieke gevallen kunnen worden gezocht bij het profiel. Relationele data-analyse is gericht op specifieke subjecten, bijvoorbeeld personen.

Ook internet vormt een bron van signalen voor fraudebestrijding met Big Data. Gemeentelijke Diensten Werk en Inkomen (DWI) speuren ook op Marktplaats naar handel en kijken of de exploitatie van – inmiddels vele tienduizenden – webshops samengaat met het genieten van een uitkering.
Ook andere 'fenomenen' of risico-indicatoren, zoals bijvoorbeeld de organisatie van ballonvaarten, bijeenkomsten voor thuisverkoop en het organiseren van kinderfeestjes, geniet belangstelling van gemeentelijke speurders. Dat geldt ook voor ruildiensten waarin geld omgaat, zoals Airbnb-kamerverhuur en Uber gedeelde autoritten. Ook relatieonderzoek op LinkedIn en Facebook kan duiden op economische activiteiten, bijvoorbeeld in de freelancesfeer.
Dit geschiedt (nog) niet in de vorm van Big Data, dat wil zeggen analyse van grote dataverzamelingen om patronen te ontdekken die leiden tot indicatoren van mogelijke fraude; geen 'bulk-onderzoek' met koppeling van een compleet uitkeringenbestand aan een andere bestanden op zoek naar 'hits' voortkomend uit risico-indicatoren.

Internetonderzoek is vrijwel altijd gericht op personen. Dit levert vragen op over de correctheid van het inzetten van dergelijke onderzoeken onder concrete ver-

208 Interviews Hans Berkhout en Ad van Mierlo, VNG KHN.

denking. In augustus 2014 bracht VNG KHN het protocol 'Internetonderzoek door gemeenten' uit, met antwoorden.[209]
De WWB vormt volgens het protocol de grondslag voor het doen van rechtmatigheidsonderzoek. Bij aanvraag van een uitkering worden gegevens van uitkeringsgerechtigden geverifieerd in zowel landelijke bronnen zoals de RDW, het Kadaster, het energiebedrijf, het Handelsregister en dergelijk als lokale bronnen, zoals bij verhuurders van woningen, energiebedrijven en de voormalige werkgever (artikelen 63 en 64 WWB).
Op grond hiervan worden personen geselecteerd voor wie op individueel niveau wordt onderzocht op internet naar aanwijzingen voor fraude. Het internetonderzoek vindt plaats bij een gegrond vermoeden van misbruik/fraude. De voorwaarden uit de Wbp worden getoetst. Het onderzoek vindt plaats in voor iedereen rechtstreeks toegankelijke openbare bronnen, en duurt drie tot zes weken. Verkregen informatie wordt maximaal drie jaar bewaard, maar een aanwijzing van fraude twintig jaar in verband met juridische plichten.

Grotere schaal

Deloitte meent dat de (gemeentelijke) overheidsaanpak van fraude te versnipperd is, wat nog toeneemt door de decentralisatie van overheidstaken. Terwijl de roep om aanpak van fraude harder wordt, verminderen de mogelijkheden. Deloitte bepleit centralisatie van fraudebeleid en uitvoering, ook om de slagkracht van data-analyse te vergroten.[210]
Nu zijn eenheden vaak te klein om tot relevante patronen voor fraudebestrijding te komen. Zo schat Deloitte dat voor gemeenten met minder dan 10.000 uitkeringsgerechtigden de data niet 'big' genoeg zijn en data-analyse naar fraudepatronen weinig soelaas biedt, na een analyse bij een middelgrote gemeente. Idealiter komt er volgens Deloitte een nationale samenwerking op het gebied van data-analyse, met bundeling van de lokale bestanden, zodat analyse en risicoprofilering optimaal worden.
Daarbij dient de expertise centraal te worden wordt opgebouwd.
Een nationaal coördinator fraudebestrijding zou landelijk de kwaliteit en de efficiëntie van de fraudebestrijding moeten vergroten: hoe meer data (van goede kwaliteit), des te nauwkeuriger de risicoprofielen. Deze persoon zou ook moeten toe-

209 https://APweb.nl/sites/default/files/atoms/files/protocol_internetonderzoek_door_gemeenten.pdf 20 februari 2015.
https://APweb.nl/sites/default/files/atoms/files/besluit_internetonderzoek_gemeenten.pdf Besluit.
https://APweb.nl/nl/nieuws/besluit-internetonderzoek-door-gemeenten nieuwsbericht 17 april 2015.

210 'State of the State', Deloitte
http://www2.deloitte.com/nl/nl/pages/data-analytics/topics/state-of-the-state.html (laatst geraadpleegd 16 februari 2016).

zien op het koppelen van databestanden van verschillende instanties binnen de grenzen van de privacyregels.

Het koppelen van lokale bestanden met persoonsgegevens is nu volgens Deloitte te beperkt mogelijk vanwege privacywetgeving. Een landelijk database zou veel gebundelde informatie bevatten na een risico-analyse, die eenvoudig tot een natuurlijke persoon te herleiden is. Dat is volgens de Wbp niet toegestaan. Anonimiseren vermindert de slagkracht van een analyse volgens Deloitte; je vergelijkt dan gemiddelden. Uiteindelijk gaat het in de data-analyse ten behoeve van fraudebestrijding om tot concrete verdenkingen te komen of die te ondersteunen met bewijs.
Wellicht kan een 'Data Darkroom' uitkomst bieden: individuele gegevens in een afgesloten omgeving koppelen, waarbij louter de resultaten van de analyses inzichtelijk worden. De opgebouwde profielen zouden dan weer landelijk gedeeld kunnen worden.

Afgelopen zomer is het onderwerp risicoanalyse opnieuw opgepakt door de regionale fraudeonderzoekers, nu onder de paraplu van de VNG. Daartoe was weer een iets andere term gevonden: Informatiegestuurd werken genoemd, kortweg IGW. Het moet gericht zijn op ingrijpen bij misbruik, maar ook op het voorkomen. Immers, staat de gemeente bekend om adequaat optreden, dan heeft dat invloed op de calculatie om te gaan frauderen. Om die reden wordt gesuggereerd betrokkenen die in een te onderzoeken doelgroep vallen, te blijven informeren.
Probleem is vooral het gebruik van eigen gemeentelijke data, zoals vergunningverlening of belastingsignalen zoals de OZB voor een pand dat wellicht wordt verhuurd. Maar ook hondenbelasting, buitenlandse vakanties, autobezit en thuiswonende studerende kinderen.
Gezien de ervaringen in de afgelopen vijf jaar wil VNG Kenniscentrum H&N het gebruik van systemen en software aanvankelijk minimaal houden. Gemeenten kunnen van een laag niveau (Incidentgestuurd) groeien naar een hoog niveau (Intelligencegestuurd), met gebruik van volledige klantenbeelden, dat wil zeggen persoonlijke profilering die actueel blijft door voortdurend gebruik van bestanden en risico-analyse. Onderzoek is behalve op deze signalen mogelijk op grond van gekozen themaprofiel (bijvoorbeeld waterverbruik, niet-erkende kinderen) of groepsprofiel (eenoudergezinnen, leeftijd, woningbezit).

Verder gaan analysegestuurd werken – de eerder besproken bulkvergelijkingen van data met risico-indicatoren en ook 'Big Data-onderzoek'. Onder dit laatste wordt geopperd alle beschikbare data te koppelen aan BSN-nummers van alle burgers. Dit staat echter op gespannen voet met privacyprincipes gezien de enorme omvang ('in strijd met proportionaliteit') en de twijfel aan de noodzaak ('subsidiariteit'). Maar veel vormen van IGW zijn zonder meer mogelijk binnen de voorwaarden van privacywet. Bestandskoppelingen ten behoeve van handhaving zijn toegestaan in

de Participatiewet, de Wet maatschappelijke ondersteuning (Wmo) en de Jeugdzorgwet.

Aanvullend op alle genoemde vormen van onderzoek kan internetonderzoek plaatsgrijpen. Het kan zeer verrijkend zijn op uitkomsten. Echter, zoeken naar persoonsgegevens kan personen wakker schudden. De optie wordt genoemd om gebruik te maken van een afgeschermde onderzoeksomgeving om dit risico te vermijden, bijvoorbeeld het IRN (internet recherche Nederland).[211]

I IGH in Amsterdam

Amsterdam werkt met een actieprogramma Informatiegestuurde handhaving. Het doel is om met onder andere informatieanalyse de capaciteit van de handhaving effectiever en efficiënter in te zetten: meer misbruik voorkomen en bestrijden door mensen en middelen slimmer in te zetten.
Behalve vergroting van de pakkans is het doel ook om met vergaarde informatie over de oorzaken en omstandigheden van ongewenst gedrag het nalevingsgedrag te bevorderen. Voorbeeld: foutparkeren beter aanpakken, maar ook parkeerbeleid ondersteunen zoals met verbetering van de bewegwijzering naar de P+R-plaatsen.
Aan de hand van een aantal thema's wordt deze fundamenteel andere werkwijze, die veel meer structureel dan op incidenten gericht is, stapje voor stapje geïntroduceerd in Amsterdam.
Een aantal (proef)projecten is ter hand genomen:

1. Aanpak logeerfraude
   Amsterdam had naar schatting tweeduizend illegale hotels en een onbekend aantal pensions zonder vergunningen. Met behulp van data-analyse tracht de gemeente in kaart te brengen waar de verdachte panden zich bevinden. De 'pakkans' was in het verleden, op grond van meldingen, zo'n 10 procent, waardoor capaciteit van handhaving inefficiënt werd ingezet. In dit project is 50 procent gehaald; op elke twee keer dat controle plaatsvond, is er één illegale exploitatie opgerold.
   Dat is bereikt door informatie op internet te bundelen, zoals over Airbnb, uit politiedossiers en van woningcorporaties met concrete meldingen van overlast, en verder aangevuld met informatie uit verschillende bestanden van de gemeentelijke handhaving. Die informatie is gecombineerd met adres- en pandinformatie, waarna de verdachte panden in beeld konden worden gebracht.
   Dit is zonder specifieke analysesoftware gedaan, dus het was arbeidsintensief. Vervolgens was ook menselijke slimheid een factor: verdachte panden werden op tijden bezocht dat de kans op aanwezige toeristen het grootst is: in de ochtend en de avond. Om een zaak tegen een illegaal hotel rond te krijgen werden aangetroffen toeristen geïnterviewd over hun boekingen.
   Deze informatie werd voorheen na het afronden van de zaak niet of nauwelijks gebruikt. Door deze informatie gestructureerd te analyseren en in te zetten, konden ook de boekingsorganisaties in beeld worden gebracht en worden aangepakt.

2. Aanpak horecaoverlast
   Gepoogd is meer patronen te ontdekken van de horecaoverlast om handhaving bij structurele problemen mogelijk te maken. Zo heeft de eenheid gepoogd om, letterlijk, de routes van de kroegentochten in beeld te brengen.

---

211 Nota Focus op IGW, VNG Kenniscentrum Handhaving en Naleving, Den Haag, augustus 2015.

De aanbieders van deze drinkgelagen, bijvoorbeeld aan groepen die vrijgezellenavonden vieren, zijn benaderd om informatie te verschaffen over vaste routes. In combinatie met politiemeldingen van overlast zou een meer structureel beeld ontstaan van ordeverstoringen in de openbare ruimte en in de kroegen.
Een succes is dit niet geworden, omdat de organisatoren van deze uitjes niet happig waren op het verschaffen van de noodzakelijke informatie. Wel heeft een analyse van horecaklachten op zich geleid tot een efficiëntere inzet van de inspectie. Zo werden zowel 'beroepsklagers' opgemerkt, als gelegenheden die het vaak te bont maken. Ook succes had de poging om geluidsoverlast bij evenementen te koppelen aan toekomstige vergunningverlening. Heel ingewikkeld was dit natuurlijk niet, maar tot op heden kwam niemand op het idee.

3. Aanpak taxioverlast
Voorheen werd de individuele taxichauffeur gecontroleerd en beboet, bijvoorbeeld voor het weigeren van ritten. De verantwoordelijkheid is verlegd naar de taxiorganisaties. Die worden aangepakt op grond van de informatieverzameling over hun chauffeurs. De risico-indicaties over de 'rotte appelen' worden verzameld per bedrijf, dat chauffeurs aan de regels moet houden.
Voor het 'handhavingsarrangement' vormt informatiegestuurd werken het uitgangspunt. Bestanden van verschillende diensten van de gemeente Amsterdam (Programmateam Taxi, Dienst Infrastructuur, Verkeer en Vervoer (DIVV), Directie Openbare Orde en Veiligheid (OOV), Dienst Stadstoezicht en Dienst Basis Informatie (DBI) en de stadsdelen) zijn daarvoor beschikbaar, alsmede die van de Inspectie Leefomgeving en Transport (ILT), Politie Amsterdam-Amstelland, het OM en wederom de Belastingdienst. Daarmee kunnen analyses met risico-indicatoren voor chauffeurs worden opgesteld met eventuele verkeersovertredingen, strafblad, belastingaangiften, woon- en familiesituatie. De IGH-aanpak beperkte zich tot de handhaving van het gedrag van de taxichauffeur op straat, al ontstaan er ook 'bijvangsten' als belastingontduiking.
Opvallend in dit project was de inzet van leerplichtambtenaren in Amsterdam als undercover taxicontroleurs. Ze lieten zich bij scholen afzetten en registreerden het gedrag van de taxichauffeurs bij de aanvraag van hun rit (al dan niet weigeren) en uitvoering.[212]

4. Parkeerdienst
Fiscaal Parkeren heeft de gemeente uitbesteed aan Cition. Dit bedrijf fotografeert voertuigen van parkeerders voor digitale controle. Rijdende camera's leggen de kentekens van stilstaande auto's vast met het oog op efficiënt parkeerbeheer. De kentekens worden ook bij het intikken van kentekens bij het betalen van het parkeren bij de palen of via de mobiele systemen zoals Parkmobile en YellowBrick al opgeslagen.
De geparkeerde en beboete kentekens worden opgeslagen in een landelijke database, het Nationaal Parkeerregister (NPR), opgetuigd door het Servicehuis Parkeer- en Verblijfsrechten (SHPV) en beheerd door de RDW. De database bevat ook tariefzones van gemeenten, eigenaren van een parkeervergunning, onder wie gehandicapten, bezoekers en professionele gebruikers, zoals hulpverleners.
Extra aandacht krijgen foutparkeerders en wanbetalers. Die kentekens worden vergeleken met de bestanden van de RDW met gestolen voertuigen en voertuigen die als uitgevoerd zijn gemeld. Foutparkeerders worden doorgegeven aan de handhaving.

212 Nota handhavingsbeleid Taxi', 4 september 2013 https://www.amsterdam.nl/parkeren-verkeer/taxi/taxibranche/handhavingsbeleid/ (laatst geraadpleegd 16 februari 2016).

Hinderpalen Amsterdam

IGH is gebaat bij bundeling van krachten en 'integraal beleid'. Dat was een belangrijke conclusie van bijvoorbeeld het project Emergo voor het 'schoonvegen' van de wallen in Amsterdam. Emergo werkte met bundeling en analyse van databestanden van de politie, het OM, stadsdiensten, de Belastingdienst, de Sociale Dienst, uitkeringsinstanties, kadaster et cetera om afwijkende profielen van panden, bedrijven en personen in beeld te krijgen.

Zowel technisch als inhoudelijk was dit problematisch. Een team van ICT-specialisten had bijna drie jaar nodig om tot eerste resultaten te komen. Methoden en uitkomsten waren niet transparant.

Belangrijkste aanbevelingen luidden:

– doorgaan met bundeling en analyse van informatiestromen;
– vereenvoudiging van de regelgeving voor de noodzakelijk geachte duidelijkheid over wat wel en niet kan op het gebied van informatie-uitwisseling.[213]

Over de problemen met de data schreef de betrokken criminoloog Cyrille Fijnaut: 'Het was niet mogelijk om op basis van het convenant dat was gesloten, onmiddellijk gegevens binnen Emergo uit te wisselen. Het duurde ruim een jaar voordat het juridische kader voor de verzameling, de uitwisseling en het gebruik van informatie volstrekt helder was gemaakt en de technische voorzieningen waren gerealiseerd om de onderlinge informatieve samenwerking te kunnen automatiseren.'[214]

Dit project is opgegaan in het RIEC, de regionale samenwerking voor criminaliteitsbestrijding. Ook de convenanten zijn voortgezet. Over de koppeling van bestanden in de uitvoering van het werk van RIEC's is nauwelijks iets bekend. Daarmee samen hangt het gebrek aan transparantie over de feitelijke werkwijzen. Met een beroep op de noodzakelijke geheimhouding in het kader van misdaadbestrijding door betrokkenen is het zicht hierop voor de buitenwacht gering.

Diverse factoren (ontbreken van eenduidige registratie, beperkte toegankelijkheid van informatiebronnen en sectorale opslag van informatie) zorgen ervoor dat informatie niet of niet optimaal wordt uitgewisseld. Daarnaast is er een veelheid aan data en informatie beschikbaar die op zichzelf bruikbaar is, maar niet direct tot effect op de handhaving leidt. Het maken van analyses is door de veelheid aan niet eenduidige gegevens lastig. Ook wat betreft het delen van informatie ten behoeve van bestrijding van uitkeringsfraude door de DWI bestaat deze onduidelijkheid in combinatie met gebrekkige transparantie.

Er is een potentieel van vele bestanden geschikt voor koppeling voor vele vormen van handhaving. Echter, de doelbinding van de privacywet – dat mogen enkele worden gebruikt voor het aanvankelijk bekendgemaakte doel – verhindert de koppeling van bestanden en massale inzet voor analyse indien data tot personen te herleiden zijn.[215]

---

213 http://www.hetccv.nl/instrumenten/bestuurlijke-aanpak/amsterdam---eindrapport-emergo
https://zoek.officielebekendmakingen.nl/blg-135298 (laatst geraadpleegd 16 februari 2016).
'Het project Emergo: meervoudig aanpakken van georganiseerde misdaad', Toine Spapens, uit 'Kennis in de frontlijn - Ervaringen met praktijkonderzoek in de politie', p 141-156 uitgever: Politieacademie
https://pure.uvt.nl/portal/en/publications/het-project-emergo%28245f4ce9-6f32-438d-bdcd-6fe15ccc4413%29.html (laatst geraadpleegd 16 januari 2016).

214 'De strijd tegen de zware misdaad', Cyrille Fijnaut, 2011 www.wbs.nl/system/files/fijnaut_-_de_strijd_ tegen_zware_misdaad.pdf (laatst geraadpleegd 16 januari 2016).

215 Interview met Ronald Kersbergen, projectleider IGH Amsterdam.

II Big data tegen fraude in Rotterdam

Ook het stadsbestuur van Rotterdam heeft zich recent op Big Data geworpen. In een artikel in iBestuur van maart 2016[216] wordt gewag gemaakt van de inzet van Big Data voor onder meer fraudebestrijding.

Het accent in het artikel ligt op het verzamelen van data door de gehele stadsorganisatie heen en het proberen om niet uit te gaan van IT-voorwaarden en beperkingen door software en dataspecialisten.

Wel is een externe adviseur ingeschakeld. Met hem is een test met data-analyse in het sociale domein opgesteld, teneinde effectievere indicatoren op te stellen die ertoe kunnen bijdragen sociale verzekeringsfraude te traceren.

Dankzij deze methode is de 'vinkjeslijst' die de Sociale Dienst gebruikt om fraude te detecteren, volgens betrokkenen 'veel kleurrijker' te maken: meer geschakeerde indicatoren die op fraude kunnen duiden.

De menselijke begeleiding moet foutieve gevolgtrekkingen uit data voorkomen. 'Een van de dingen die we in de data vonden, is dat als iemand ouder is dan 83, de kans groot is dat die persoon fraudeert. Dan is die persoon wel gehuwd, maar woont niet meer met de partner op hetzelfde adres. Maar dat gebeurt op die leeftijd natuurlijk best vaak, zonder dat dat betekent dat er sprake is van fraude, bijvoorbeeld omdat een van de twee in een bejaardentehuis is opgenomen. Dat maakt duidelijk dat je altijd inhoudelijke deskundigen nodig hebt om verbanden te duiden.'[217]

Aan een tweede probleem, privacy, werd volgens betrokkenen te zwaar getild uit angst voor politieke problemen. In de woorden van de adviseur: 'Er mag veel meer dan men denkt of wil. Er zit natuurlijk wel vaak een bestuurlijk afbreukrisico aan. Zo van: "Het mag niet, want ik denk dat ik anders gezeur krijg met mijn wethouder." '[218]

Vaak volstaat tijdig anonimiseren van data om vervolgens patronen te ontdekken die de controleurs kunnen helpen en niet a priori een lijst met te controleren mensen te genereren.

Denken in data helpt, bijvoorbeeld met een vroege signalering van schulden: 'Zie je bij wijze van spreken de abonnementen op de Donald Duck opgezegd worden? Het zijn hele eenvoudige dingen waar je naar kunt kijken. Huisartsen weten ook onmiddellijk waar de pijn zit. Ga dat dan met zijn allen anonimiseren en met elkaar delen om de patronen te leren herkennen.'[219]

216 Big data in Rotterdam: zonder 'silo's', Freek Blankena, 17 maart 2016 http://ibestuur.nl/nieuws/big-data-in-rotterdam-zonder-silo-s).

217 Idem.

218 Idem.

219 Idem.

11 BZK

INLEIDING

Het ministerie van BZK zette via zijn onderdeel ICTU, dat werkt aan de 'digitale overheid', een aantal projecten op met data-analyse. Het project Landelijke Aanpak Adreskwaliteit (LAA), verbetering van de Basisregistratie Personen (BPR), heeft onverwacht grote nadruk gekregen: voor fraudebestrijding breidt samenwerking zich immers steeds verder uit, met steeds meer data-analyse juist op adresbestanden.
De intrigerende wisselwerking tussen het op orde brengen van adressen en diverse vormen van fraudebestrijding van een aantal overheden vormt de hoofdmoot van dit onderzoek. Overigens is ook hier niet in letterlijke zin sprake van een Big Data-toepassing: er worden (nog) geen data-analyses toegepast op de BPR als geheel om risico's op fraude (verdenkingen) uit te distilleren. De BPR is onderdeel van een stelsel van elf basisregistraties, die in een omvangrijk project worden gekoppeld en beter toegankelijk gemaakt via knooppunten. Samen vormen ze de *very big data* van de overheden. De beschrijving hiervan vormt de opmaat naar de nog niet beantwoorde vraag: in hoeverre komt het stelsel in aanmerking voor data-analyse en profilering, ook ten behoeve van fraudebestrijding?

11.1 DOEL EN UITGANGSPUNTEN

Het kabinet gaat in de Rijksbrede antifraudestrategie uit van 'een goede balans tussen gerechtvaardigd vertrouwen, goede dienstverlening en fraudebestrijding'. Ictu is de ICT Uitvoeringsorganisatie, opgericht door het ministerie van BZK en de VNG 2001, die 'kennis en kunde op het gebied van ICT en overheid bundelt'. ICTU voert voor het ministerie van BZK een aantal projecten uit, waaronder het project Aanpak fraude algemeen en het project Landelijke Aanpak Adreskwaliteit (LAA).
Die vloeien voort uit de Rijksbrede anti-fraudestrategie, zoals gelanceerd in 2013. Het ministerie van BZK gebruikt bij een aantal initiatieven gegevens en analyses daarvan voor handhaving. De belangrijkste is gericht op het verbeteren van de kwaliteit en fraudebestendigheid van de Basisregistratie Personen (BRP).[220]

Het belangrijkste doel was om de BRP (voorheen GBA) op orde te krijgen. Ook voor fraudebestrijding is een juiste adressering van personen noodzakelijk. Veel fraude wordt gepleegd door gerommel met woonadressen, bijvoorbeeld voor uitkeringen,

220 Brief van minister Opstelten (VenJ) aan de Tweede Kamer over de aanpak van fraude met publieke middelen,19 december 2013 https://www.rijksoverheid.nl/documenten/kamerstukken/2013/12/21/rijks brede-aanpak-van-fraude
Interview met Mattie Blauw van BZK.

studiefinanciering en toelagen, maar ook voor zwaardere criminaliteit. De Tweede Kamer eiste een percentage van 99 procent juistheid van alle gegevens. Dat is door de regering vervolgens toegezegd met een actieplan.[221]

Uit de resultaten van een evaluatie bleken grote verschillen te bestaan tussen gemeenten in het bijhouden van de BRP: bij 15 gemeenten is geen enkele afwijking geconstateerd – alle 15 met een inwoneraantal van onder de 35.000. Er waren echter ook 31 gemeenten die onder de minimale norm van ten minste 90 procent juiste data presteerden.
Voor alle data tezamen was het percentage van 99 procent haalbaar, maar voor de factor adres maximaal 98 procent, zelfs met een steeds verfijndere controlemethodiek. De oorzaak daarvan zijn veranderingen die te laat worden doorgevoerd, vooral bij verhuizingen van personen voor korte of lange tijd, of definitief.[222]

11.2 RISICOGESTUURD ONDERZOEK NAAR ADRESFRAUDE

Officieel bleek in een kleine 3 procent van de gevallen het geregistreerde adres in de BRP niet het feitelijke woonadres van de betrokkene. Het controleren van namen bij adressen bij 17 miljoen inwoners en 7,5 miljoen huishoudens geeft via een willekeurige steekproef een kleine kans op resultaat. Om die reden is het nut van het opstellen van risicogestuurd adresonderzoek beproefd, om een hoger percentage onjuiste adressen te kunnen traceren.

De Rijksdienst voor Identiteitsgegevens (RvIG), voorheen Agentschap BPR en onderdeel van het ministerie van BZK, leidde het project voor verbetering van de BRP: de LAA, aanvankelijk bedoeld als proef. Daarbij wordt data-analyse ingezet om tot patroonherkenning te komen en op basis daarvan gericht te gaan speuren naar foutieve adressering. Dit leidt tot risicoprofielen: bij welke kenmerken is er gerede verdenking van foutieve adressering. Als er opzet in het spel is, dan legitimeert dit veelal de fraudebestrijding.
Binnen het project LAA werden op basis van een risicoprofiel verdachte adressen geselecteerd door de RvIG. Deze risicoadressen werden geselecteerd voor huisbezoeken door gemeenten. Soms volstond een louter administratieve controle. Een voorbeeld van risicogestuurd onderzoek vormt het nagaan van 'overbewoning': een groot aantal personen staat dan ingeschreven op een beperkt aantal vierkante meters. De vraag is of deze personen hier daadwerkelijk wonen, of alleen op het adres ingeschreven staan en elders woonachtig zijn. Ook andere risicofactoren

221 Motie Heijnen-Bilder, 29 november 2007 , Kamerstuk 31 200 VII, nr. 34
Actieplan Kwaliteit GBA, 11 juni 2008, staatssecretaris Bijleveld aan de Tweede Kamer.

222 Kamerstuk 30 985 Beleidsdoorlichting Binnenlandse Zaken en Koninkrijksrelaties Nr. 18
Lijst van vragen en antwoorden, 21 april 2015
https://zoek.officielebekendmakingen.nl/dossier/30985/kst-30985-18

werden opgesteld, zoals personen die briefadressen hanteren. Een derde indicator waren de 'verwonderadressen' van de Belastingdienst, die sterke aanwijzingen bieden dat gegevens van één of meer bewoners onjuist zijn. Bijvoorbeeld bij de combinatie van toeslagen, of onbestelbare brieven.
Ook het CJIB leverde selecties van verdachte adressen. Een belangrijke bron was uiteraard ook het adressenbestand dat bij gemeenten valt onder 'vertrokken onbekend waarheen' in de BRP. Niet minder dan ruim 400.000 personen waren begin 2014 geregistreerd als zogeheten VOW'er.

Gemeenten kregen ondersteuning. In het rapport 'Samen sterk tegen adresfraude' staat dat het fraudeteam van de RvIG tussen mei 2014 en januari 2015 124 gemeenten bezocht zowel om deze te informeren over fraudesignalen en de wijze waarop fraude het best aangepakt kan worden als om zelf inzicht te krijgen in de maatregelen die gemeenten al genomen hebben tegen adresfraude die de BRP treft.
Door vijf gemeenten werden risicoprofielen gebruikt in het proces van inschrijven aan de balie. Die gemeenten gebruikten een gedetailleerd processchema dat beschrijft hoe verschillende 'signalen van fraude' kunnen worden herkend en moeten worden afgehandeld. De overige bezochte gemeenten gebruikten een dergelijk processchema met risicoprofielen toen niet.
Zo'n 43 procent van de gemeenten gebruikte ook sociale media bij het adresonderzoek, 25 procent had (eveneens) een anoniem meldpunt. Het overgrote deel van de gemeenten let op overbewoning dan wel schijnbewoning, en pakt deze veelvoorkomende adresfraudes aan.

In het 'Eindrapport Samen werken aan Adreskwaliteit 2014' staat het effect van dit hanteren van risicosignalen beschreven: de meeste van de gehanteerde zes typen 'risicoadressen' leverden een meer dan tienmaal zo groot 'rendement' op van het uitvoeren van adresbezoeken in vergelijking tot willekeurig huisbezoek. In detail:

- Bij de kleine 6000 extra adresonderzoeken en huisbezoeken door de eerste 91 deelnemende gemeenten op grond van risicosignalen bleek bij 1 op de 3 adressen sprake van onjuiste adresregistratie: dus geen 3 procent trefkans, maar ruim tien keer zoveel!
- Vooral de verwonderadressen geleverd door de Belastingdienst bleken effectief: bijna 130 personen van wie de gegevens niet kloppen bij 100 gecontroleerde verwonderadressen. Oftewel: inzet van deze risicofactor uit data-analyse was bij controle van de BRP ruim 18 keer zo effectief dan met een aselecte steekproef.
- Bij de geleverde 'verdachte' adressen van het CJIB (detentieregistratie, boete-inning) traden bij 23 procent onregelmatigheden naar voren; vervolgens zijn bij huisbezoeken bij 100 CJIB-adressen gemiddeld 102 personen aangetroffen van wie de geregistreerde gegevens niet klopten.
- Een derde risicoprofiel is opgesteld aan de hand van signalen van de registratie 'vertrokken onbekend waarheen' (VOW) in de gemeentelijke BPR. Een indica-

tor was bijvoorbeeld of op deze adressen in de afgelopen vijf jaar een paspoort, identiteitskaart of rijbewijs was aangevraagd. Voor 7 procent van de 'VOW'ers' bleek dit het geval. Vervolgens zijn die adressen bezocht. Zo werd ook een ongewoon hoog geachte bewonersdichtheid (minder dan 12 m2 per bewoner) als risico-indicatie genomen. Een derde gedeelte van de adressen bleek niet correct gehanteerd, met gemiddeld 106 personen op de 100 adressen van wie de data onjuist bleken.
– Zo blijkt het briefadres zonder BPR-registratie een goede indicator te zijn dat er iets niet klopt op een adres. Het bezoeken van selectieve (verdachte) 100 briefadressen leverde gemiddeld 66 personen op van wie de geregistreerde gegevens niet klopten.

Conclusie: risicogestuurd handhaven, oftewel databestanden analyseren om tot gerichtere verdenkingen te komen van foutieve adressering, sorteert effect.
Gevolg: in december 2014 rapporteerde de Rijksoverheid dat het succes van de risicogerichte aanpak van adresfraude leidt tot landelijk uitrollen van het project LAA. Met een investering op jaarbasis van 13 miljoen euro worden baten van naar schatting 42 miljoen euro per jaar verwacht, te behalen met op te sporen fraude zoals minder uitkeringen, toeslagen et cetera. Oftewel een businesscase zoals dat is gaan heten: elke euro investering levert ruim 3 euro op.[223]

11.3 LANDELIJKE AANPAK ADRESKWALITEIT MET RISICO-ANALYSE

Uit de geslaagde proeven met risicogericht adresonderzoek vloeide in januari 2015 de Landelijke Aanpak Adreskwaliteit voort, waarbij gemeenten zich kunnen aansluiten. In deze aanpak zouden opgestelde risicosignalen gedeeld worden met gemeenten ten behoeve van gericht adresonderzoek.
Ter stimulans voor deelname ontvangen gemeenten van het ministerie van BZK een vergoeding voor een afgerond adresonderzoek ter hoogte van 70 euro. De RvIG

223 Samen werken aan Adreskwaliteit 2014, Eindrapport, 26 november 2014, http://www.rvig.nl/documenten/circulaires/2014/11/26/eindrapport-adresonderzoek-2014
Samen sterk tegen adresfraude, Rapport over de aanpak van adresfraude door de Rijksdienst voor Identiteitsgegevens (RvIG) en gemeenten, 20 april 2015 http://www.rvig.nl/documenten/rapporten/2015/04/20/rapport-samen-sterk-tegen-adresfraude
Interviews met Mattie Blauw, Judy Moester en Monique Barnhoorn van BZK.
Kamerstuk 30 985 Beleidsdoorlichting Binnenlandse Zaken en Koninkrijksrelaties Nr. 18 Lijst van vragen en antwoorden, 21 april 2015
https://zoek.officielebekendmakingen.nl/dossier/30985/kst-30985-18
Kabinet investeert 13 miljoen in aanpak adresfraude, verwachte opbrengst 42 miljoen, persbericht, 21 december 2014
https://www.rijksoverheid.nl/actueel/nieuws/2014/12/21/kabinet-investeert-13-miljoen-in-aanpak-adres fraude-verwachte-opbrengst-42-miljoen

produceerde op grond van data-analyse en risicoprofilering de 'Waaier fraudepatronen' voor gemeenten, met daarin '10 signalen voor mogelijke fraude'. Deze handleiding voor fraudedetectie wordt veel gebruikt door gemeenten en andere bij het bestrijden van adresfraude betrokken partijen. De risicoprofielen uit de waaier worden door de RvIG steeds verder gespecificeerd en aangevuld .
Bij het inzetten van bestanden van derden voor adrescontrole en vergelijken van data uit verschillende bestanden voor het voorkomen en bestrijden van adresfraude wordt vooraf een juridische toets uitgevoerd, met de vraag: is het qua privacy in de haak?

De risicoanalyses maken van gemeenteambtenaren ook speurders. Ze kunnen daartoe opleidingen volgen. De Ictu had het voornemen om gemeentelijk ambtenaren Burgerzaken te ondersteunen in het preventief signaleren van fraude-indicaties tijdens realtime transacties in de BRP. Doel was ook om bekende fraudepatronen zoals die van de fraudekaart (waaier) bij gemeenten te automatiseren, zodat een ambtenaar beter wordt ondersteund in zijn taak en aan de balie zoveel mogelijk op uniforme wijze wordt gewerkt.[224]

Het ministerie van BZK is in het kader van fraudebestrijding ook scherper geworden op het registreren van immigratie, al dan niet tijdelijk. In 2014 is begonnen met het registreren van tijdelijk verblijf in Nederland zoals van seizoenarbeiders, studenten en gepensioneerden. Zij moeten zich nu inschrijven in de BRP wanneer ze verwachten de komende zes maanden meer dan twee derde van de tijd in Nederland te zullen verblijven.
Maar er is eerder behoefte aan een burgerservicenummer onder meer voor de heffing van belasting en andere overheidstaken. Daartoe kunnen ze zich melden voor inschrijving als niet-ingezetene in de BRP (onderdeel RNI, registratie niet-ingezetene).

In Bestuurlijke Overleggen tussen kabinet en gemeenten over EU-arbeidsmigratie is door gemeenten aangegeven dat zij inzicht willen hebben in het eerste verblijfsadres van niet-ingezetenen in Nederland. Het eerste verblijfsadres kan door gemeenten worden gebruikt voor handhaving, bijvoorbeeld bij controle op overbewoning. Het ministerie van BZK heeft het initiatief van de gemeenten ondersteund, onder andere door een systeem te laten bouwen dat de inschrijving ondersteunt – Registratie Eerste Verblijfsadres (REVA) – en waarbij het eerste klantcontact bij het RNI-loket wordt gebruikt om aan persoon te vragen naar zijn/haar eerste verblijfsadres. Deze pilot is begin 2014 begonnen bij de gemeenten Rotterdam, Den Haag, Westland, Schiedam en Vlaardingen. Inmiddels doen ruim dertig

224 Waaier fraudepatronen, 10 signalen van mogelijke fraude, folder, 27 februari 2015 http://www.rvig.nl/documenten/brochures/2015/02/27/waaier-fraudepatronen

gemeenten mee en is de verwachting dat begin 2016 alle 19 RNI-loketten zullen meedoen aan de pilot.[225]

Het Algemene Rekenkameronderzoek was kritisch over het gebrek aan inzicht in de effectiviteit, efficiency en proportionaliteit van gegevensuitwisseling en -analyses.[226]
Daarop zijn maatregelen genomen, zoals de invoering van een werkgroep Batenberekening en een 'Batenmonitor', waarmee resultaten van het LAA-project uitvoerig worden bijgehouden. In een externe audit was nog niet voorzien. De participatiegraad van gemeenten is hoog, vindt de projectleiding: 160 deelnemers, samen goed voor 10 miljoen inwoners. Zo'n 240 gemeenten deden niet mee ondanks de financiële stimulans.
In 2015 zijn samen 7200 adresonderzoeken uitgevoerd, met 2500 onjuiste adresregistraties als resultaat. (stand december 2015).
Het project LAA is volgens de minister van VenJ 'lonend', zo rapporteerde hij eind 2015 aan de Tweede Kamer.[227] Bij 38 procent van de onderzochte adressen verschilden de inschrijving van personen met de werkelijke daar wonende personen. Tot en met oktober 2015 is voor ruim 7 miljoen euro aan baten berekend, die momenteel toenemen, tegenover ruwweg 6 miljoen euro aan kosten. Begin 2016 wordt een evaluatie uitgevoerd.[228]

Overigens vat het project LAA juist een aantal door de Rekenkamer geopperde problemen bij de horens, voor wat betreft de BRP. Het aantal terugmeldingen op de BRP waarbij afnemers van gegevens uit de BRP – veelal overheidsdiensten – melden dat zij gerede twijfel hebben bij een gegeven, steeg in de eerste helft van 2015 met 6 procent. Onderwijl daalde het aantal personen geregistreerd als vertrokken met onbekende bestemming (VOW'ers) in de BRP met 50.000 in de anderhalf jaar tussen begin 2014 en medio 2015.
Dankzij samenwerking met onder andere de Belastingdienst, de Nationale Politie, het CJIB, de RvIG en de SVB komen veel nieuwe signalen beschikbaar. Doordat de signalen steeds sterker worden, zal het rendement van de huisbezoeken verder toenemen.

---

225 Magazine Aanpak Adreskwaliteit, Nummer 3 en 4, november 2015
http://magazine.aanpakadreskwaliteit.nl/nl/magazine/10136/794712/cover.html

226 Rapport Basisregistraties, Algemene Rekenkamer, 29 oktober 2014
http://www.rekenkamer.nl/Publicaties/Onderzoeksrapporten/Introducties/2014/10/Basisregistraties

227 Kamerbrief over voortgang rijksbrede aanpak van fraude van minister van der Steur (VenJ) aan de Tweede Kamer, 21 december 2015
https://www.rijksoverheid.nl/documenten/kamerstukken/2015/12/21/tk-voortgang-rijksbrede-aanpak-van-fraude

228 Interview met Mattie Blauw van BZK.

De Belastingdienst zou na een beperkte start met LAA met 200 signalen nog 750 signalen leveren. Van de nieuwe deelnemer politie werden 'enkele honderden adressignalen' verwacht in de pilotfase, het CJIB na eerst 250 nog eens 1500. De SVB, DUO, ZiNL (Zorginstituut) en het UWV werken mee aan verificatie van signalen of hebben de intentie daartoe uitgesproken.
Ze gaan na hoe ze vanuit hun bestanden verdachte adressen kunnen selecteren. Ook wordt gesproken met partijen van buiten het overheidsdomein, zoals de Stichting Netwerk Gerechtsdeurwaarders (SNG), die onjuist geachte adressen kunnen doorspelen. Na succesvolle proeven met politiesignalen van openstaande boetes in enkele Utrechtse gemeenten en Almere volgde ook inbreng van de politie in andere gemeenten.[229]

De middelen die de RvIG inzet in het project LAA breiden zich uit. Zo hanteert ze sinds augustus 2015 het instrument *webcrawler* om frauduleuze online-advertenties te vinden in grote openbare bestanden. De webcrawler haalt content van vooraf bepaalde delen van advertentiesites binnen, bijvoorbeeld: marktplaats.nl/woningen, en selecteert hieruit de relevante advertenties.
Bijvoorbeeld 'Gezocht: inschrijfadres. Ik woon zelf bij mijn gezin, dus kom alleen langs voor mijn post.' Of: 'Woning te huur. Inschrijven als bewoner bij gemeente momenteel niet mogelijk'. Dit soort advertenties zijn vaak bedoeld om regelingen en uitkeringen aan te vragen (of te houden) die afhankelijk zijn van het woonadres, zoals bijstand, huurtoeslag of studiefinanciering.
Of omdat iemand zich onvindbaar wil maken vanwege bijvoorbeeld (belasting)schulden, uitstaande boetes of politievervolging. Met een toenemend aantal advertentiesites zijn afspraken gemaakt om het malafide aanbod te verwijderen en de adverteerder hiervan op de hoogte te stellen. Op Marktplaats.nl (waarmee als eerste afspraken zijn gemaakt) zijn in 2015 meer dan honderd advertenties verwijderd.
Malafide advertenties bevatten overigens weinig tot geen persoonsgegevens. Vaak een naam en soms een telefoonnummer. Het gaat de RvIG *niet* om analyse van persoonsgegevens van adverteerders. Dit instrument is volledig gericht op de advertentie zelf.[230]

Voorbeelden gemeenten
Enkele lokale projecten voor opschoning van adresbestanden liepen parallel, zoals van de Dienst Basisinformatie van de gemeente Amsterdam. Daartoe zijn grote bestanden gekoppeld, bijvoorbeeld de polisadministraties van het UWV en de SVB. In de werkgeversrelatie en in de pensioenregistratie komen vaker juiste adressen voor dan in de gemeenteadministratie. Ook de Belastingdienst, de Sociale Dienst, uitzendbureaus en woningcorporaties werkten mee met de vergelijkingen.

229 Idem.
230 Idem.

'Maar ook via de balie krijgen we meldingen, bijvoorbeeld omdat iemand zich laat inschrijven op een adres waar al twee gezinnen wonen. Daarnaast doen we risico-analyes op onze eigen bestanden, zoals op overbewoning. Stel dat drie gezinnen op één adres staan ingeschreven. Klopt dat? Ons systeem Key2Burgerzaken is gekoppeld aan de Basisadministratie Adressen en Gebouwen en via Atlas kennen we de grootte van de woning. Overigens doen we niet alleen query's op adres, maar ook op persoon. Bijvoorbeeld, wie heeft een uitkering en is per 1 juli verhuisd? Heeft dat soms met de huishoudtoets te maken?'[231]
In het project is onderscheid gemaakt tussen:
– 'onwetende burgers' (niet op de hoogte van wetgeving);
– 'gemakzuchtige burgers' (vergeet adreswijziging door te geven);
– 'calculerende burger': fraudeert om bijvoorbeeld uitkeringen, hogere toeslagen, studietoelage et cetera te ontvangen, of vanwege het maskeren van onderhuur.

Zo'n 30 procent van de 33.000 adressen waarvan de registratie van de polisadministratie anders was dan bij de gemeente, was dit onderzoekswaardig. De risico-indicatie was volgens de betrokkenen zinvol in fraudebestrijding. Echter, er volgde slechts zeventien concrete onderzoeken naar fraude, met tien keer het stopzetten van een uitkering.
Amsterdam zou zich zetten aan 'diepgaander onderzoek', onder meer via sociale media als Facebook, teneinde het aantal spookburgers – oorspronkelijk 85.000 – verder terug te dringen.[232]
Den Haag deed een eigen project om met risico-indicatoren grotere percentages onjuiste adressen af te vangen. Zo was het percentrage onjuiste adressen bij de risico-indicaties als volgt:
– administratieve leegstand: bijna 46 procent;
– wel ingeschreven, niet woonachtig: 33 procent;
– verdenking onregelmatigheid studiefinanciering (DUO): bijna 15 procent.

Den Haag zag mogelijkheden voor intensivering van datakoppeling, onder meer met data over gas- en waterlevering, internetdata ('sociale' media), Suwinet Services, speuren naar familieleden en ook de telefoongids.
Het begon met datakoppeling ten behoeve van adreskwaliteit, maar in de slipstream werd behalve fraude ook criminaliteit getraceerd, zoals hennepteelt en mensensmokkel.[233]

231 Magazine Aanpak Adreskwaliteit, november 2015, pagina 7-11.
232 Idem.
http://magazine.aanpakadreskwaliteit.nl/nl/magazine/10136/791119/de_ervaringen_van_amstelveen_en_amsterdam.html
Project Schoon Schip – roadshow BZK najaar 2013, presentatie, 9 december 2013
http://www.rvig.nl/documenten/publicaties/2013/12/09/workshop-4-presentatie-bestandsvergelijking-gebruik-uwv-polisadres-bij-gba
'Eindrapport pilot. Interventieproject. Schoon Schip. Een samenwerking van Gemeente Amsterdam met UWV, SVB, Belastingdienst en het RCF', Gemeente Amsterdam, 9 mei 2013
http://www.rvig.nl/documenten/rapporten/2013/06/25/eindrapport-schoon-schip (geraadpleegd 13 februari 2016).
233 Resultaten project Adresonderzoek en praktijkervaring gemeente Den Haag met o.a. leegstand, BPR roadshows 2013, 12 september 2013
http://www.rvig.nl/documenten/publicaties/2013/12/09/workshop-2-presentatie-adres onderzoek

Tilburg digitale gedragsanalyse
Tilburg begon met risico-analyse van digitale contacten met burgers, dat wil zeggen van 'vreemd gedrag van de inschrijver'. Aangezien dit via internet minder zichtbaar is dan aan de balie, heeft Tilburg in het project 'Adres op orde' 25 indicatoren verzameld om dan toch afwijkingen te herkennen, waarvan er nu 7 leiden tot een uitnodiging voor de inschrijver voor 'een persoonlijk gesprek', dat wil zeggen een verhoor.

11.4 TOEKOMST: VERVOLG LAA

In afwachting van een besluit van de ministeriële commissie-Aanpak Fraude in april 2016 om het LAA-project structureel te maken, gaat het tot die tijd door met 'risicogerichte adresonderzoeken' binnen hetzelfde budget.
Naar verwachting zijn eind maart 2016 ten minste 10.000 adresonderzoeken afgerond, in het eerste jaar na aanvang. Dat was het doel. Op basis van risicosignalen van beheerders en afnemers van adresgegevens zouden in 2016 zo'n 10.000 adressen worden bezocht voor controle en 5000 adressen administratief gecontroleerd; met naar verwachting circa 7500 adresgerelateerde fraudegevallen. Administratieve controle is geschrapt. Nu wordt nog geraamd dat 10.000 huisbezoeken 40 procent onjuist adressen zal opleveren.
De BRP wordt met de uitkomsten gecorrigeerd en de fraudeopbrengst wordt door de partners in beeld gebracht en verhaald. De baten daarvan worden landelijk geregistreerd en mede benut voor de financiering van het adresonderzoek.

De opbrengst is initieel als volgt gespecificeerd: de verwachte baten komen tot stand door jaarlijks 15.000 gevallen van adresfraude op te sporen. Eén opgespoord adresfraudeur levert gemiddeld 2800 euro aan adresfraude gerelateerde baten op, in totaal 42 miljoen euro per jaar. De investering is 13 miljoen per jaar.
Naar verwachting van het kabinet zal het percentage van gecontroleerde adressen met onregelmatigheden in adressen binnen het LAA-project in maart 2016 liggen tussen de 40 en 50 procent. In 2014 was dit nog 30 procent, in 2015 opgelopen naar 38 procent. De feitelijke percentages worden door het project op maandbasis bijgehouden. Deze realisatie blijkt in lijn met de verwachtingen.[234]
Samenwerking zal verder toenemen: DUO levert gemeenten verdachte adressen aan, waarna vervolgens de buitendienst van de gemeente onderzoek doet of een student thuis of uit huis woont. DUO betaalt 360 euro per aangeleverd dossier. Bij fraude zet de DUO de studiebeurs stop en kan de eerder uitgekeerde beurs worden teruggevorderd.

234 Kamerbrief over voortgang rijksbrede aanpak van fraude van minister van der Steur (VenJ) aan de Tweede Kamer, 21 december 2015
https://www.rijksoverheid.nl/documenten/kamerstukken/2015/12/21/tk-voortgang-rijksbrede-aanpak-van-fraude

VNG Kenniscentrum Handhaving en Naleving brengt bijvoorbeeld interne afdelingen van gemeenten en afnemers zoals de Belastingdienst samen binnen de structuur van de landelijke interventieteams. Zij vergelijken informatie over adressen die ze niet vertrouwen en gaan vervolgens op huisbezoek. Zo worden fouten in de BRP ontdekt en stuit men op onterecht verstrekte toeslagen of uitkeringen.

11.5 PROJECT AANPAK FRAUDE BIJ ICTU

Het deelproject Innovatie van ICTU in het kader van fraudeaanpak, aldus gepubliceerd in een vacature in januari 2015, zet in het veld van fraudebestrijding data-analyse c.q. 'business forensics' in. Met pilots wil de afdeling Burgerschap & Informatiebeleid (B&I) van het ministerie van BZK aantonen dat het mogelijk is om kleine en concrete stappen in de aanpak van identiteits- en adresfraude te zetten door middel van data-analyse in open bronnen.
Het project Aanpak Fraude van ICTU draagt in opdracht van het ministerie van BZK onderzoek, wetenschappelijke methodes en innovatieve ideeën en technieken aan die de huidige aanpak van ID- of adresfraude kunnen aanvullen of verbeteren. In 2015 begon BZK een 'proef' op gebied van analyse van databestanden, begeleid door ICTU. Samen met de gemeente Zaanstad wordt onderzocht of op grond van gecombineerde gegevens binnen de gemeente Zaanstad nog niet-bekende patronen van adresfraude te traceren zijn. Na onderzoek naar privacyaspecten zoals melding bij de Autoriteit Persoonsgegevens, is besloten om:

– de gecombineerde gegevens in eerste instantie volledig te anonimiseren;
– toestemming datagebruik beter te regelen.

De geanonimiseerde gegevens van Wmo en BRP worden gebruikt om te zoeken naar fraudepatronen waarvan de relevantie door ambtenaren van Zaanstad wordt bepaald. Door niet-relevante patronen weg te gooien worden alleen vermoedelijke vergissingen, fouten of fraude meegenomen. In deze fase zijn persoonsgegevens die verwijzen naar burgers op geen enkele wijze te herleiden.
De gevonden relevante fraudepatronen worden vervolgens gebruikt om in actuele niet-geanonimiseerde data die signalen te vinden die eventueel verder kunnen worden onderzocht op fraude, fouten en vergissingen. De experts binnen de gemeenten moeten de fraudepatronen nog beoordelen, aldus een woordvoerder van de gemeente.

Gemeenten willen ook fraudebestrijding in de hun toegewezen Wmo en Jeugdzorg zelf ter hand nemen in de stuurgroep fraude in de zorg. Onder voorzitter-

schap van de burgemeester van Hendrik-Ido-Ambacht zijn de gemeenten Schiedam, Gorinchem, Cromstrijen en de Drechtsteden begonnen.[235]
Eerst wordt vastgesteld waar de risico's liggen voor fraude, zowel door individuen maar ook door organisaties die meedingen in aanbestedingen voor pgb's. De grijze gebieden met 'creatief boekhouden' moeten in beeld komen. De gemeenten werken in het project samen met het Kenniscentrum Naleving & Handhaving van de VNG, het ministerie van VWS, twee zorgkantoren en de pgb-belangenvereniging Per Saldo.
De drijfveer is minimalisering van verlies van het krappe zorgbudget aan fraude. De resultaten zouden in het voorjaar van 2016 aan het ministerie van VWS worden aangeboden, ten behoeve van inzet voor alle gemeenten in Nederland. Erasmus Universiteit begeleidde het project en bracht begin 2016 het rapport 'Naar rechtmatige zorg in het gemeentelijke sociale domein' uit.
De EUR-onderzoekers stellen vast dat frauderisico's het grootst zijn aan de kant van zorgaanbieders en dat hier beter op gelet moet worden. Ze adviseren gemeenten om hun kennis beter te bundelen en uit te wisselen binnen de keten met zorgaanbieders, zorggebruikers en zorgverzekeraars. Ten tweede raden zij gemeenten aan de handhaving te versterken met nieuwe expertise, vooral gericht op financiële data-analyse in de zorg.[236]

Een vacature voor (big) data-analyst bij BZK

Vacatures geven doorgaans goede informatie over de richting van organisaties, zoals deze
'Data-analist cybersecurity ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Logius Functieomschrijving
Wil jij verder bouwen aan een veilige e-overheid?
Samen met jouw collega's van het Fraudeteam, dat de komende tijd wordt uitgebouwd, lever je een stevige bijdrage aan de veiligheid van de diensten van Logius, zoals DigiD en MijnOverheid.
Als data-analist cybersecurity bestrijd je cyberdreigingen zoals cybercrime (fraude en misbruik) en andere bewuste aantastingen van de diensten binnen de E-overheid. Enerzijds hebben jouw werkzaamheden een proactieve/preventieve zijde. Denk aan early detection, intelligente analyse van grote datasets en ondersteuning van security by design adviezen. Anderzijds hebben ze een meer reactieve zijde en werk je aan forensische en operationele analyse bij concrete signalen.
De (digitale) dreigingen, de voorzieningen en de methoden en technieken om dreigingen te onderkennen en beheersen zijn interactief en dynamisch. Snelle innovatie is daarom belangrijk. Het Fraudeteam wil nieuwe technische mogelijkheden snel kunnen toepassen. Naast het werken met, is ook het inrichten van nieuwe analyseomgevingen en applicaties onderdeel van jouw werkzaamheden. […]
Functie-eisen:

---

235 'Gemeenten werken samen bij aanpak fraude in de zorg', Persbericht gemeente Cromstrijen, 3 april 2015
http://www.cromstrijen.nl/actueel/gemeentenieuws_3355/item/gemeenten-werken-samen-bij-aanpak-fraude-in-de-zorg_6896.html

236 'Naar rechtmatige zorg in het gemeentelijke sociale domein', Erasmus Universiteit, Faculteit der Sociale Wetenschappen, januari 2016 http://www.eur.nl/fsw/bestuurskunde/nieuws-detail_bsk/article/81389-onderzoek-naar-rechtmatige-zorg-in-het-lokale-sociale-domein/

[…]
- Je hebt kennis en ervaring op het gebied van analyse van grote datasets (big data, profiling/predictive modelling) of van technisch-forensische analyse.
- Je hebt ervaring met één of meer programmeer- en/of scriptingtalen.
- Ervaring met werkgebieden als active monitoring en detectie, incident respons, computer network defense/investigations is een pre.
- Je hebt bij voorkeur kennis van en ervaring met malware, cybercrime, identity fraud, hacking en phishing.[237]

11.6 BASISREGISTRATIES: HEEL VEEL DATA

De belangrijkste data van de overheid zijn vervat in basisregistraties, elf in totaal. Het geheel wordt samengevoegd in een stelsel van basisregistraties. Dit stelsel moet voorzien in het borgen van onderlinge relaties en koppelingen alsmede gemeenschappelijke voorzieningen voor ontsluiting voor belanghebbenden en onderlinge uitwisseling.
Dit stelsel vormt één van de belangrijkste onderdelen van de Generieke Digitale Infrastructuur (GDI) van de overheid. Dit is geen organisatie of harde infrastructuur, maar het geheel van standaarden, producten en voorzieningen die gezamenlijk gebruikt worden door de overheden, vele publieke organisaties en in een aantal gevallen ook door private partijen.
Grof gezegd staan de basisregistraties nu nog op zichzelf, maar door samenvoeging moeten degenen met toestemming om de data in te zien veel efficiënter dan nu kunnen raadplegen en data overnemen.
Door gegevens onderling te delen, moet ook dienstverlening verbeteren. Hierdoor hoeft een burger of bedrijf bepaalde gegevens niet steeds opnieuw aan te leveren, maar is 1 melding voldoende. Provincies, gemeenten en waterschappen hebben toegang tot deze gegevens en kunnen ze bij hun eigen werk gebruiken.[238]

Het gaat daarbij om:
– BRP – Basisregistratie personen;
– NHR – Handelsregister;
– BAG – Basisregistraties Adressen en Gebouwen (tweevoudig *);

237 www.werkenvoornederland.nl, januari 2016 (inmiddels niet meer online).
238 'Stelsel van basisregistraties'
http://www.digitaleoverheid.nl/onderwerpen/stelselinformatiepunt/stelsel-van-basis registraties
'Stelsel van overheidsgegevens', bericht DigitaleOverheid.nl
http://www.digitaleoverheid.nl/onderwerpen/stelselinformatiepunt/stelsel-van-over heidsgegevens
'Efficiënter werken door samenvoegen basisregistraties', nieuwbericht Rijksoverheid.nl
https://www.rijksoverheid.nl/onderwerpen/digitale-overheid/inhoud/efficienter-wer ken-door-samen voegen-basisregistraties

- BRT – Basisregistratie Topografie;
- BRK – Basisregistratie Kadaster;
- BRV – Basisregistratie Voertuigen (kentekenregister);
- BLAU – Basisregistratie voor Lonen, Arbeidsverhoudingen en Uitkeringen;
- BRI – Basisregistratie Inkomen;
- WOZ – Basisregistratie Waarde Onroerende Zaken;
- BGT – Basisregistratie Grootschalige Topografie (voorheen GBKN);
- BRO – Basisregistratie Ondergrond (voorheen ook wel DINO).

*) De BAG bestaat uit twee basisregistraties: adressen en gebouwen. Daarom zijn er twaalf basisregistraties.

Het ministerie van BZK coördineert dit Stelsel van Basisregistraties. In een stelselcatalogus heeft Logius, ICT-onderdeel van het ministerie van BZK, de kenmerken en inhoud beschreven, en de koppelingen.[239] Er is ook een animatie beschikbaar van het stelsel. Een visiedocument schetst het beoogde toekomstige beeld en een kalender geeft de planning weer voor de hele beoogde digitale overheid inclusief de registraties.[240]
De uitgaven van de ministeries belopen tot 2021 grofweg 100 miljoen euro per jaar, in 2016 120 miljoen euro, de latere jaren iets minder dan 100 miljoen euro: totaal 600 miljoen euro. Daar komt een kleine 800 miljoen euro bij aan kosten – minus van de zbo's en agentschappen die de registraties beheren – minus een kleine 700 miljoen euro aan inkomsten.
Er worden knooppunten gebouwd, als voorziening of organisatie die het afnemers gemakkelijk maakt om aan te sluiten op beschikbare gegevensbronnen (waaronder de basisregistraties). Een knooppunt werkt als een intermediair tussen de houders van bronnen en de afnemende organisaties.
Informatiebeveiliging en privacy vormen samen belangrijk onderdeel van de dienstverlening van deze knooppunten. Een voorbeeld van een knooppunt is het BKWI (Bureau Keteninformatisering Werk&Inkomen), beheerder van Suwinet, dat gegevens deelt voor overheidspartijen binnen het domein werk en inkomen zoals het UWV, de SVB en de Belastingdienst.

Steeds meer sectoren overwegen of zetten stappen om een eigen knooppunt ontwikkelen, zoals gemeenten, onderwijs, provincies en andere partijen. Om een

239 Stelselcatalogus
http://stelselcatalogus.logius.nl/

240 Visie op het Stelsel van Overheidsgegevens
https://wiki.stelselvanbasisregistraties.nl/xwiki/bin/view/document/Visie+op+het+Stelsel+van+Over heidsgegevens
Releasekalender Basisregistraties
http://www.digitaleoverheid.nl/onderwerpen/voortgang-en-planning/releasekalender

indruk te krijgen van bestaande knooppunten is een overzicht opgenomen met doorverwijzingen naar bestaande knooppunten.[241] Dit overzicht geeft een indruk en pretendeert niet volledig te zijn.
Noodzakelijk is volgens De Digicommissaris de doorontwikkeling van het Stelsel van Basisregistraties naar een Stelsel van Overheidsgegevens (SvO).[242] Hiermee wordt beoogd meer samenhang aan te brengen in de manier waarop de overheid haar gegevens organiseert en deelt.
Het doel is de juiste informatie op de juiste plek en op het juiste moment. En daarnaast 'het bevorderen van de innovatiekracht in de samenleving en de overheid' door nieuwe toepassingen van data. De Visie op het Stelsel van Overheidsgegevens formuleert hiervoor verschillende principes die richting geven aan deze doorontwikkeling.

11.7 RELATIE BIG DATA EN FRAUDEREGISTRATIE

Dit stelsel voldoet niet aan de enge definitie van Big Data, namelijk dat het moet gaan om bakken vol ongestructureerde data. Echter, ze kunnen op heel veel manieren dienen om analyses op uit te voeren, om nieuwe patronen te ontdekken. Daar kunnen patronen uit voortkomen die duiden op een verhoogd risico van criminaliteit, bijvoorbeeld fraude.
Ook zijn de basisregistraties handig om snel in concrete bestrijding van fraude gegevens te vergaren. De grens tussen inzet van data voor casuïstiek en voor meer generieke opsporing is niet helder. De Big Data-mogelijkheden van de basisregistraties zijn verschillende keren aan de orde gekomen afgelopen jaren, ook in het kader van fraudebestrijding.
Op termijn levert het gebruik van basisregistraties voor opsporing, zoals voor de Inspectie SZW, het meest op indien alle (relevante) systemen centraal worden ontsloten. De basisregistraties tezamen vormen een datareservoir *à boire*, maar analyse daarvan op grond van de principes van Big Data-analyse vormen nu nog een 'stip op de horizon'.

---

241 Knooppunten
http://www.digitaleoverheid.nl/onderwerpen/stelselinformatiepunt/stelselthemas/knooppunten
'Stelsel van Overheidsgegevens', De Digicommissaris, Erik Jonker, 28 september 2015
https://digitaleoverheid.pleio.nl/file/download/34410462
Knooppunten en het Stelsel van Basisregistraties
https://wiki.stelselvanbasisregistraties.nl/xwiki/bin/view/document/Visie+op+het+Stelsel+van+Over heidsgegevens

242 'Notitie Stand van zaken financiering stelsel van basisregistraties', 16 januari 2016, Digicommissaris https://digitaleoverheid.pleio.nl/file/download/41536982

De mogelijkheid wordt geopperd voor analyse van grote hoeveelheden gekoppelde data. Voor deze massale analyses spelen vragen ten aanzien van privacy, zoals de bekende principes van proportionaliteit, subsidiariteit, doelbinding.[243]

Een groot deel van een kritisch rapport van de Rekenkamer over de basisregistraties uit 2014 is gewijd aan fraudebestrijding.[244] De Rekenkamer stelde vast dat te weinig helder was hoe basisregistraties voor fraudebestrijding ingezet zouden worden. Er waren wat afzonderlijke initiatieven en experimenten, maar een overkoepelende benadering ontbrak. Deze fragmentarische aanpak maakt het lastig om te leren van de ervaringen op dit gebied, aldus de Kamer.
Zonder heldere voorwaarden voor data-analyse volgen er te gemakkelijk valse verdenkingen. De Rekenkamer noemt als voorbeeld Schoon Schip in Amsterdam, dat na koppeling van bestanden van het UWV en tweeduizend verdachte burgers opleverde, met uiteindelijk 25 werkelijke fraudegevallen.
Juist gezien de mogelijkheden voor adequate opsporing moeten privacy- en beveiliging optimale aandacht krijgen. Zo moet ook transparant worden wie er welke gegevens opvraagt en verkrijgt.
Ook moet het correctierecht van burgers en bedrijven goed geregeld worden, omdat kleine fouten grote gevolgen kunnen hebben, niet zelden voor langere perioden. Kleine foutpercentages kunnen in absolute zin tot grote aantallen fouten leiden en kleine fouten kunnen grote gevolgen hebben door de verspreiding ervan naar vele verschillende (overheids)instanties. Een tip van de Rekenkamer: stel gegevens beschikbaar als open data, waar dit zonder bezwaren (zoals privacy) mogelijk is, mede om zo de gegevenskwaliteit breder toetsbaar te maken.

Al in mei 2012 en in januari 2013 zijn sessies over fraudebestrijding met basisregistraties georganiseerd met bestuurders, managers en informatiespecialisten van inspecties, uitvoeringsorganisaties, expertisecentra en politie. Zo lichtten een aantal sprekers toe hoe fraudesignalen uit de grote dataverzamelingen te destilleren en toe te passen zijn met uitkomsten op naam en op adres, in netwerken et cetera.
Een van de sprekers was van iCOV, Infobox Crimineel en onverklaarbaar vermogen, dat in hoofdstuk 12 in deze rapportage uitgebreid aan bod komt. Hij noemde als voorbeeld om uit bestanden van BPR NHR, WOZ en Kadaster verdenkingen te formuleren.

---

243 'Basisregistraties als fundament voor modernisering toezicht bij Inspectie SZW', Ruud Boot (ICTU) en Wimfred Grashoff (Servicepunt Basisregistraties), zonder datum http://www.digitaleoverheid.nl/images/stories/stelsel_van_basisregistraties/best-practice-iszw.pdf (geraadpleegd 8 februari 2016).

244 'Basisregistraties vanuit het perspectief van de burger, fraudebestrijding en governance', Rekenkamer, 29 oktober 2014. http://www.rekenkamer.nl/Publicaties/Onderzoeksrapporten/Introducties/2014/10/Basisregistraties

Bijvoorbeeld van personen met een laag inkomen en zeer dure huizen, mogelijk gefinancierd met buitenlandse hypotheken. 'Basisregistraties zijn hier van belang, in het bijzonder door ze met andere registraties te verknopen en in samenhang te bezien.
Het iCOV kijkt dan ook met belangstelling uit naar het leggen van verbindingen binnen het Stelsel van Basisregistraties […] Als Kadaster, Handelsregister en WOZ aan de BAG worden gekoppeld, ontstaan er nieuwe analysemogelijkheden.' Ook het IB, dat eveneens elders in dit stuk aan bod komt (hoofdstuk 5), zag mogelijkheden om met de BAG (Basisregistraties Adressen en Gebouwen) frauderisico's met bijstand te distilleren, zoals schijnverhuizingen, verdacht gebruikersdoel van panden en oppervlakte van een pand.[245]

11.8 PRIVACYKWESTIES

Zoeken op 'privacy' op het domein digitaleoverheid.plein.nl levert geen resultaat op.[246] Privacy lijkt inderdaad bij een aantal basisregistraties geen enkele rol te spelen, zoals van topografie en gebouwen. Het project Landelijke Aanpak Adreskwaliteit, gericht op verbetering van adresregistratie in de BPR toont aan dat ook op het oog eenvoudige bestanden zoals van adressen zich al goed lenen voor data-analyse en het genereren daaruit van 'risico's' in de vorm van verdachte adressen. Daarbij is ook een grens geslecht door VenJ. De minister van VenJ ging in september 2015 akkoord met een machtiging tot BRP-terugmelding voor de politie. Die machtiging behelst toestemming om bepaalde politiegegevens over adresbezoek te verstrekken aan (B&W van) gemeenten ten behoeve van de BPR-kwaliteit. Dat besluit verscheen in de Staatscourant 'om onduidelijkheid weg te nemen'. Immers, de wet politiegegevens staat niet toe dat opsporingsdata worden gedeeld buiten het justitiedomein.
Verbetering van adreskwaliteit gaat meer en meer hand in hand met fraudebestrijding. Dat werd evident met de samenwerking tussen het project LAA en de Landelijke Stuurgroep Interventieteams (LSI), geleid vanuit de Inspectie SZW. Diezelfde inspectie oppert meer mogelijkheden voor datagebruik vanuit basisregistraties. Bij koppeling van bestanden kan eenvoudige vergaande profilering van (rechts)personen ontstaan. Opsporingsdiensten kunnen met een goed werkend stelsel van basisregistraties, of met een nog op te bouwen stelsel van overheidsinformatie, sneller relevante gegevens verzamelen en bundelen om tot een verdenking te komen of een verdenking te ondersteunen.

245 Presentaties seminar BAG Fraudebestrijding http://wiki.stelselvanoverheidsgegevens.nl/index.php/Fraudebestrijding (Geraadpleegd 11 februari 2016).

246 Zoeken op 'privacy' bij De Digitale Overheid https://digitaleoverheid.pleio.nl/search?q=privacy (geraadpleegd 13 februari 2016).

Net als met het project LAA kunnen de basisregistraties vroeg of laat ook beschikbaar komen om analyses op los te laten om tot risicofactoren te komen zonder concrete verdenking, net zo goed als beleid gericht op verbetering van bijvoorbeeld leefomgevingen van analyse van deze 'Big Data'-gebruik kan gaan maken.

Voorbeelden op zich vormen het Handelsregister en het Kadaster. Aangezien steeds meer zelfstandigen thuis werken, moeten ze zich met hun privéadres registreren. Hun data, ook over omzet en vermogen, zijn voor iedereen beschikbaar. Ook data van het Kadaster zijn openbaar, zij het tegen betaling. De Autoriteit Persoongegevens heeft zich over het laatste kritisch uitgelaten. Voor 'een paar euro' is er inzage in naam, adres, burgerlijke staat, koopsom, WOZ, hypotheek en bouwvergunningen. Per 1 oktober wordt de WOZ openbaar met alle voor fiscale heffing geschatte waarden van woningen.[247]

247 Eigen Huis Magazine oktober 2015, vraaggesprek met Jacob Kohnstamm http://www.eigenhuis.nl/actueel/eigen-huis-magazine/

12 VEILIGHEID EN JUSTITIE, EN ICOV

INLEIDING

Het ministerie van VenJ begon met het grootschalig inzetten van data-analyse voor fraudebestrijding. Soms gaat dat gepaard met media-aandacht, zoals het geval was bij project Radar (fraudebestrijding bij bedrijven), waarbij zich IT-problemen voordeden. Maar veelal speelt zich dat in stilte af, wat vragen oproept over hoe betrokkenen verantwoording afleggen over hun werkzaamheden.
Het accent in dit hoofdstuk ligt op Infobox Crimineel en Onverklaarbaar Vermogen (iCOV), het grootste en belangrijkste samenwerkingsverband ten behoeve van de bestrijding van allerlei vormen van fraude, waaronder belastingfraude en witwassen. Dankzij de medewerking van de leiding van iCOV komen de werkzaamheden van dit samenwerkingsverband voor het eerst uitgebreid in de openbaarheid met deze rapportage.[248]
Daarna komen de werkzaamheden van Justis kort ter sprake, de screeningsautoriteit van het ministerie van VenJ, dat bij het grote publiek vooral bekend is van de Verklaringen omtrent het Gedrag.
Het hoofdstuk eindigt met de bespreking van de door een aantal in dit onderzoek aan bod komende partijen genoemde dringende noodzaak om de wettelijke kaders uit te breiden om de nieuwste ontwikkelingen van data-analyse mogelijk te maken.

12.1 ICOV: DOEL EN OPZET

iCOV is als samenwerkingsverband tussen het OM, de politie, de Belastingdienst, de Douane, het FIOD en de Financial Intelligence Unit in 2013 opgericht met de operationele doelen onder meer om crimineel en onverklaarbaar vermogen in kaart te brengen, witwas- of fraudeconstructies bloot te leggen, belastingontduiking tegen te gaan en verder de partners te helpen om overheidsvorderingen alsnog te innen.
Een meer structureel doel van het samenwerkingsverband is 'om de deelnemende partijen in staat te stellen betekenisvol te interveniëren dan wel gedrag te beïnvloeden'.
iCOV voert louter verzoeken uit voor deelnemende partijen. Dat is de reden van de grote belangstelling van organisaties om mee te doen. Recent sloten zich zo ook nog de opsporingsdiensten van de Nederlandse Voedsel- en Warenautoriteit

248 Compilatie van informatie over iCOV, waaronder een gesprek met Gees Grootscholten (Hoofd), Arjen Cuijpers (plv Hoofd iCOV/MT lid verantwoordelijk voor ICT) en Mieke van der Vegt (Senior beleidsmedewerker/privacy jurist). Citaten zijn eveneens van deze woordvoerders.

(NVWA), de Inspectie SZW en de Inspectie Leefomgeving en Transport (ILT) bij het samenwerkingsverband aan. Andere overheidsorganisaties tonen interesse in deelname, zoals toezichthouders en nog meer inspecties. iCOV, dat zijn onderkomen heeft in een gebouw van de Belastingdienst in Utrecht (en voorheen in Hoofddorp bij de Douane), bouwt deels voort op de inzichten die zijn opgedaan in het experimentele project Vastgoed Intelligence Center (VIC). VIC richtte zich primair op vastgoedfraude, terwijl iCOV alle typen van vermogensdelicten bestrijdt. Het gaat om *financial intelligence* in de volle breedte, die haar beslag krijgt in rapportages, criminaliteitsbeeldanalyses, risico-indicatoren en groepsprofielen. Om aan die brede iCOV-taak vorm te geven moest een professionele en resultaatgerichte samenwerkingsorganisatie worden gecreëerd, die op basis van een stevig juridisch fundament haar werkzaamheden verricht. iCOV is gestoeld op een convenant[249], gepubliceerd in augustus 2013, waaraan protocollen voor gegevensverwerking en onderzoek[250] zijn toegevoegd, evenals twee Mandaatregelingen voor beheer en voor privacy.[251]
iCOV kan snel benodigde informatie uit veel verschillende bronnen leveren en dat is de voornaamste reden voor partijen om deel te nemen. Er werken op dit moment zo'n dertig personen afkomstig uit de verschillende participerende organisaties.

Het bestaansrecht van iCOV is met name gelegen in het bijeenbrengen van informatie van partijen, opdat deze zo efficiënter hun eigen taak kunnen uitvoeren en/of om gezamenlijk bepaalde complexe maatschappelijke vraagstukken het hoofd kunnen bieden. Als legitimering van het belang van zijn bestaan noemt iCOV zelf dat de staat naar schatting jaarlijks 16 miljard euro schade lijdt door fraude.

249 Convenant iCOV 2013
https://zoek.officielebekendmakingen.nl/stcrt-2013-24607.html

250 Protocol gegevensverwerking iCOV productie 2013
https://zoek.officielebekendmakingen.nl/stcrt-2013-24608.html

251 Regeling tot mandaat, volmacht en machtiging Hoofd iCOV Beheerszaken 2013, Staatscourant Nr. 24635, 29 augustus 2013
https://zoek.officielebekendmakingen.nl/stcrt-2013-24635.pdf
Regeling tot mandaat, volmacht en machtiging Hoofd iCOV Wet bescherming persoonsgegevens 2013, Staatscourant Nr. 24636, 29 augustus 2013
https://zoek.officielebekendmakingen.nl/stcrt-2013-24636.pdf

De overheid heeft een fors begrotingstekort, staat voor grote bezuinigingen in bijvoorbeeld de zorg (circa 16 miljard) en wordt tegelijkertijd voor die broodnodige miljarden opgelicht en daardoor ernstig benadeeld, aldus iCOV.[252]

Als samenwerkingsverband werkt iCOV op zijn beurt op kennis- en expertiseniveau samen met weer andere samenwerkingsverbanden, zoals Regionale Informatie- en Expertisecentra (RIEC's), het Anti-Money Laundry Centre (AMLc) en het Financieel Expertise Centrum (FEC).

12.2 OPBOUW EN UITVOERING VAN HET SYSTEEM

iCOV is een dienstencentrum en geen casusoverleg zoals het RIEC, dat meer op grond van een concrete casus en daarbij behorende (rechts)personen informatie uit verschillende bronnen bundelt.
Teneinde witwassen en fraude goed in kaart te brengen is het noodzakelijk heel veel data uit heel veel verschillende bronnen te combineren. Het voordeel daarvan is dat verbanden tussen een groot aantal (rechts)personen zichtbaar worden, die anders niet dan wel op basis van toeval zouden zijn gevonden.
Op basis van hun eigen wettelijke bevoegdheden kunnen alleen deelnemende partijen producten opvragen bij iCOV. Alle opdrachten en verzoeken aan iCOV worden 'juridisch getoetst' op rechtmatigheid van onder meer gegevensgebruik. Per product is er per mogelijke aanvrager een algemene rechtmatigheidsbeoordeling opgesteld in samenspraak met de juristen van de deelnemende partijen, verenigd in de zogenoemde Rechtmatigheidscommissie.
Daardoor is duidelijk onder welke voorwaarden wie welk product met welke gegevensbronnen kan aanvragen. Deze voorwaarden zijn opgenomen in de aanvraagformulieren, waardoor de aanvrager alle voorwaarden zelf moet doornemen vóór die specifieke aanvraag.
Daarbij valt te denken aan de vraag of er een vordering van de officier van justitie is bijgevoegd en of het verzoek past binnen de doelen van iCOV. iCOV controleert of het formulier volledig is ingevuld en of aan de voorwaarden is voldaan op grond van het door de aanvrager ingevulde formulier.
iCOV is '100 procent vraaggestuurd'. Daarmee is altijd duidelijk voor welke partij iCOV een product maakt en op grond van welke bevoegdheid. De politie moet bijvoorbeeld altijd een vordering van een officier van justitie tonen om fiscale gegevens te verkrijgen, omdat anders de fiscale geheimhoudingsplicht de aanvraag in de weg staat.

252 'Fraude kost Nederland jaarlijks 30 miljard. Aanpak loont.', Schalke & Partners, zonder datum http://www.schalke.nl/pdf/FRAUDE-totaaloverzicht%202014.pdf (geraadpleegd 17 februari 2016).
Deze zeer ruwe en ook relatief schatting van Schalke & Partners die iCOV als bron noemt is niet gefundeerd door valide onderzoek.

Alleen aanvragen vanuit de Belastingdienst hebben die dekking niet nodig, omdat de belastinginspecteur eigen bevoegdheden heeft (m.n. om belastingdata te raadplegen). De Belastingdienst kan echter niet alle gegevens van de politie krijgen, omdat daarop geheimhouding vanuit de Wet politiegegevens rust dan wel het opsporingsbelang in een concrete zaak aan verstrekking in de weg staat.
Ook de onderzoek- en ontwikkeling (R&D)-activiteit is vraaggestuurd: deelnemers kunnen vragen onderzoek te doen naar volgens hen belangrijke aspecten voor hun taken, die zien op toezicht, handhaving en opsporing. Die onderzoeken moeten passen binnen de doelen van iCOV. Dat staat in die bewoordingen beschreven in jaarplannen en in projectvoorstellen.

iCOV werkt met legio bestanden van de deelnemers. Het gaat op dit moment om specifiek de volgende databestanden:
– bestanden over vermogensposities van de Belastingdienst;
– informatie uit het Kadaster, RDW en van de Kamer van Koophandel;
– verdachte transacties en handhavings- en antecedenteninformatie van de politie.

iCOV werkt met de kopieën van de bestanden van de deelnemers, waaronder bestanden met data van alle belastingplichtigen, en beheert die zelf. Ze staan op een apart deel van de rekencomputer van het OM.
Er is een 'gedeelde verantwoordelijkheid' voor de juistheid van de data. In eerste instantie berust die bij de aanleverende partner. Nadat data concreet zijn overgedragen, is de aanvrager hiervoor vervolgens verantwoordelijk.
Door deze werkwijze met kopieën van dumps (oftewel databases) zijn de producten die bij iCOV worden gemaakt, niet altijd even actueel. Dit hangt onder meer af van de frequentie waarmee de bestanden of gegevens daaruit worden aangeleverd; soms zijn de data niet actueler te verkrijgen (de belastingaangifte bijvoorbeeld doet men slechts één keer per jaar).
Intelligenceproducten helpen dus te prioriteren en te sturen, maar voor werkelijk juridisch bewijs moet de aanvrager te rade gaan bij de bronbestanden. Hij weet dan inmiddels wel in welke bestanden hij de grootste kans heeft om doel te treffen.
iCOV laat steeds verfijndere combinaties van indicatoren los op deze databases en beschikt over steeds verfijndere *tooling* om alle bestanden in één keer te ontsluiten, en daarmee snel vastgoed, ander vermogen en transacties van personen in kaart te brengen.

Banken leveren geen bestanden met transacties aan iCOV. De verdachte transacties waarover iCOV beschikt, zijn afkomstig van de Financial Intelligence Unit-Nederland (FIU). Banken en andere instellingen zijn wel verplicht om ongebruikelijke transacties te melden aan de FIU. Het is de taak van de FIU om deze transacties te analyseren en de transacties die verdacht zijn, beschikbaar te stellen aan de opsporingsdienst.

Ook het CJIB levert geen bestanden aan. Het CJIB vraagt wel producten op om betalingsregelingen te kunnen treffen, beslag te kunnen leggen en om beter te prioriteren. Voor dat laatste wordt bijvoorbeeld een lijst van personen aangeleverd met openstaande ontnemingsvorderingen. iCOV kan heel snel laten zien bij welke personen de meeste verhaalmogelijkheden zijn.

De techniek om data bijeen te brengen is nauwkeurig vastgelegd en belangrijk. iCOV en deelnemende partijen moeten samen bestanden technisch aanpassen voor verwerking tot de formaten die iCOV hanteert voor bundeling van data tot een informatief geheel.
De datastroom begint bij de bronbestanden vanuit de Belastingdienst, opsporing, et cetera. Deze worden samen opgeslagen in een *staging database,* waarop bewerkingen worden uitgevoerd voor een 'slimme opslag', oftewel zodanig gebundeld dat ze functioneel zijn. Dit resulteert in een bronnendatabase, die de basis vormt voor de productvervaardiging.
Hier vindt het selecteren, transformeren en aggregeren van data plaats. Op dat moment zijn de verschillende datastromen nog steeds gescheiden.
Wanneer er een productaanvraag komt die rechtmatig is, vindt er vermenging plaats en koppeling op naam (BSN), oftewel analyse met verschillende tools. Daaruit volgt dan bijvoorbeeld een rapportage vermogen en inkomen, een veelgevraagd product waarin data vermengd en gekoppeld zijn. Sommige data worden sec geleverd, andere data worden gewogen en verklaard. Daartoe zijn er twee soorten van verwerking van data: voor productie op naam en toenaam (BSN) en anoniem.
Dat laatste is specifiek bedoeld voor onderzoek en ontwikkeling met de data, bijvoorbeeld voor *prototyping* voor de ontwikkeling van nieuwe producten. Als deze nieuwe producten na het testen werkend zijn, worden deze als kennistools in de productieomgeving geplaatst.
iCOV maakt geen gebruik van open-internetdata van bijvoorbeeld LinkedIn, Facebook en Google. Het eventuele gebruik van deze bronnen wordt overgelaten aan de participanten, oftewel de klanten van iCOV die data opvragen. iCOV heeft ook geen grote ongestructureerde internetbestanden waarin het *random* zoekt naar specifieke patronen. iCOV werkt met grote hoeveelheden gestructureerde data, die grotendeels afkomstig zijn van de deelnemende partners.

12.3 DATA-ANALYSE IN DE PRAKTIJK

iCOV hanteert drie productgroepen of rapportages:

1. Vermogen en Inkomsten, met de varianten: object, subject, hypotheek per subjecten, bulk. De aanvrager vraagt een Rapportage Vermogen en Inkomen aan op een subject, een object of op een grote hoeveelheid subjecten (bulk). In een

dergelijke rapportage staat informatie over onder andere loon, vastgoed en vermogen.
Op dit moment zijn in dit overzicht opgenomen: (eventueel) loon, bezit vastgoed, bedrijven, stichtingen, hypotheken, box 3-vermogen, winsten, alimentatie, auto's, aandelen, toeslagen en verdachte transacties. Handzame ordening en weergave vinden plaats in excelbestanden op A3-formaat. Het komt voor dat de aanvrager dit product opnieuw aanvraagt na verloop van tijd om veranderingen in vermogen in de tijd waar te kunnen nemen (bijvoorbeeld om met 'nieuw' vermogen de oude vordering alsnog te laten voldoen).

2. Relaties: relatienetwerk rondom of tussen personen en/of organisaties. In 'duizelingwekkende snelheid' wordt in de systemen zakelijke contacten, vastgoed et cetera in kaart gebracht en grafisch weergegeven. In drie tot vier lagen diep kunnen binnen een minuut relaties op niveaus van adres, werkgever en collega's, vastgoed, Kamer van Koophandel in kaart worden gebracht. Crimineel verkregen vermogen is vaak elders ondergebracht, bij (rechts)personen in het netwerk van verdachten en veroordeelden.
Deze dienst kan technisch gezien 'oneindig diep' en 'oneindig breed' gaan, maar uit praktisch oogpunt en uit privacyoverwegingen is de informatiegaring beperkt. Iedereen is op verschillende wijze met anderen verbonden. Denk bijvoorbeeld aan werkgevers met duizenden werknemers, waarbij niet iedereen elkaar persoonlijk kent. Om die reden is bij dit product ingebouwd dat de computer bij een specifiek aantal werknemers een 'stopvlag' plaatst.
De aanvrager komt bij iCOV langs om samen met experts van iCOV te kijken naar de 'brutoversie' van de relatiescan: daarbij kan de aanvrager aangeven welke relaties wel, en niet van belang zijn voor zijn onderzoek. De niet-relevante (juridisch gezegd: niet-noodzakelijke) relaties worden dan verwijderd, zodat er uiteindelijk een nettobestand (een opgeschoond relatienetwerk) overblijft.
Dat bestand wordt verstuurd aan de aanvrager, zodat alleen de noodzakelijke en betekenisvolle relaties worden verstrekt. De brutorelatiescans worden wel bij iCOV bewaard. Dat is noodzakelijk om eventuele rechtmatigheidsvragen die later kunnen rijzen in bijvoorbeeld een rechterlijke procedure of bij een onderzoek door de Autoriteit Persoonsgegevens, te kunnen beantwoorden.

3. Thema: door bestandsvergelijking kan het gekozen thema met risico-indicatoren casuïstiek in kaart worden gebracht. Het gaat hier om onderzoek naar bijvoorbeeld groepen, sectoren of een geografisch gebied.
Aan de hand van scenario's en verschijningsvormen worden bijbehorende risico-indicatoren toegepast op de toegestane bronnen (open, gesloten en privaat, alleen voor zover die voor die aanvrager gebruikt mogen worden).

Het beeld dat hieruit ontstaat, biedt mogelijkheden voor nadere analyse en het bepalen van interventiestrategieën. Dit is het tijdrovendste product van iCOV, dat alleen gemaakt kan worden in samenspraak met de aanvrager.
Soms wordt een vermoeden dat bestaat bij de aanvrager, juist uitgesloten door het maken van een themascan. Er kan bijvoorbeeld blijken dat er geen sprake lijkt te zijn van witwassen met vastgoed.
Een voorbeeld van themaonderzoek: het 'geld lenen van jezelf' kan (maar hoeft niet te) vallen onder een typologie van witwassen die de Financial Action Task Force (FATF) onderscheidt. Om die reden wordt dit gegeven gecombineerd met diverse andere indicatoren, waaronder informatie dat een particulier in 'risicolanden' gestalde grote bedragen heeft ingebracht als zekerstelling bij banken voor het verkrijgen van een hypotheek. Op deze manier kwam een bepaalde groep in beeld. Een team van de FIOD is hierop nader onderzoek gaan doen.

12.4 RESEARCH & DEVELOPMENT

Naast het leveren van producten (vermogen en inkomen, relaties en thema) doet iCOV ook aan Research & Development (R&D; Onderzoek & Ontwikkeling).
Deze afdeling binnen iCOV kent vier taken, te weten het toetsen van de betrouwbaarheid van de data, het ontwikkelen van nieuwe producten en tools, het ontwikkelen en valideren van nieuwe indicatoren en (toegepast) wetenschappelijk onderzoek (criminaliteitsbeeldanalyses).
Deze afdeling kent een eigen regime dat is gebaseerd op de uitgangspunten die gelden voor het doen van wetenschappelijk onderzoek (regime voor Wetenschap en Statistiek) en werkt in een afgescheiden data-omgeving. Uit deze afdeling kunnen nooit persoonsgegevens worden verstrekt. R&D levert alleen anonieme rapportages, nieuwe indicatoren, nieuwe kennisregels, nieuwe tools en dergelijke.

Wetenschappelijk onderzoek

De laatstgenoemde taak van R&D, het wetenschappelijk onderzoek, betreft 'fenomeenonderzoek'. Dit levert anonieme gegevens op. Dit fenomeenonderzoek is wetenschappelijk van aard, waarbij wordt samengewerkt met het WODC en/of universiteiten.
Bij het ontwikkelen en valideren van indicatoren wordt onderzocht wat elders al bekend is, bijvoorbeeld bij de Financial Action Task Force (FATF), waarin 34 deelnemende landen zich bezighouden met de bestrijding van witwassen en de financiering van terrorisme. In het project Operationaliseren Witwasindicatoren FATF worden de indicatoren afkomstig uit de typologieën van de FATF, geoperationaliseerd in de data die bij iCOV al beschikbaar zijn.
Deze indicatoren kunnen vervolgens worden gebruikt om bijvoorbeeld een themascan te maken (al blijft telkens de vraag wie over welke gegevens mag beschikken).

Alle projecten voor R&D staan vermeld in het jaarplan, dat wordt vastgesteld door de opdrachtgevers. Op die manier is voor die projecten aan de 'vraagsturing' van de deelnemers voldaan. Er is echter wel veelal opnieuw toestemming van de houder van de bronbestanden nodig om deze te mogen gebruiken.
Doorgaans wordt toestemming niet geweigerd, aangezien iCOV hoofdzakelijk de gegevens gebruikt van de opdrachtgevers zelf. Ook kunnen externe bronnen aan een specifiek R&D-project worden toegevoegd. In een aantal gevallen zijn externe wetenschappers bij de projecten betrokken in de hoedanigheid van een klankbordgroep.
Daarnaast zijn er momenteel twee promovendi werkzaam bij iCOV. De onderzoekers werken in een gescheiden omgeving. Eén of twee bijna-afgestudeerde criminologen en/of recherchekundigen kunnen gelijktijdig stage bij iCOV lopen; voor meer stagiaires (en hun begeleiding) heeft iCOV geen ruimte.
Een voorbeeld van fenomeenonderzoek is het onderzoek dat in samenwerking met de Landelijke Recherche is gedaan naar de kenmerken van Outlaw Motorcycle Gangs, in vergelijking met driehonderd andere mannelijke motorrijders uit dezelfde leeftijdscategorie. Uit het onderzoek kwam naar voren dat 82 procent van de clubleden een JDS-registratie (justitiële documentatie, voorheen: strafblad) had, tegen 33 procent gemiddeld binnen de controlegroep. Binnen de Outlaw Motorcycle Gangs zijn er veel vaker dubieuze debiteuren – met een schuld bij de Belastingdienst – en is ook veel vaker sprake van verdachte transacties. De motorbendeleden zijn verder gemiddeld vaker werkloos, hebben een uitkering en vaker een inkomen onder modaal. Opvallendste factor: ruim 20 procent bezit geen motorrijbewijs.
Dit zijn statistische uitkomsten. Daarna wordt de vervolgvraag gesteld of de samenwerkende partners op basis van deze informatie de motorbendeleden anders benaderen. Het helpt volgens iCOV om deze groep beter te duiden. Dit duidt de groep als een probleemgroep ten opzichte van een willekeurige andere groep motorrijders.
Hierbij moet echter wel rekening worden gehouden met het feit dat er een vertekend beeld kan ontstaan, doordat er sprake is van een bevooroordeelde selectie: de namen van motorbendeleden kwamen exclusief uit politiesystemen, wat ongetwijfeld invloed heeft gehad op het grote percentage JDS-registraties.
Vanuit Big Data-oogpunt blijft de cruciale vraag: welke praktische betekenis heeft dit? 'Je kunt zo'n groep nader onderzoeken en inzoomen op details.'

12.5 RESULTATEN

In 2014 heeft iCOV ruim duizend verzoeken omtrent vermogen en inkomen van de deelnemende organisaties in behandeling genomen. 52 procent van de aanvragen was afkomstig van de politie (incl. de Rijksrecherche), 14 procent van de FIOD, 11 procent van de Belastingdienst en 23 procent van het OM (incl. het CJIB).

Per aanvraag gaat het doorgaans om meerdere (rechts)personen, subjecten en/of objecten tegelijk. In een enkel geval is een aanvraag geweigerd. Weigering vindt bijvoorbeeld plaats omdat de aanvrager (nog) geen lid is van het samenwerkingsverband, de juiste vordering ontbreekt of omdat de vraag niet overeenkomt met de doelen waarvoor ICOV in het leven is geroepen.

Levering van een rapportage vermogen en inkomen vindt binnen twee dagen plaats. Van relatienetwerken zijn er in 2014 ruim driehonderd gemaakt. Levering vindt plaats binnen ongeveer een maand, dat gaat immers in overleg met het team dat erom vraagt en daarvoor ook persoonlijk naar ICOV toe moet komen. 43 procent van de aanvragen was afkomstig van de politie (incl. de Rijksrecherche), 20 procent van de FIOD, 33 procent van de Belastingdienst en 10 procent van het OM (incl. het CJIB).
Deze dataverzameling en -verwerking levert een tijdwinst op van weken/maanden ten opzichte van traditioneel rechercheren en verzamelen van data. De slagingskans van de opsporing neemt dankzij deze 'levering aan één loket' verder aanzienlijk toe. Organisaties kunnen in principe hetzelfde resultaat bereiken, maar dan in veel langere tijd: weken of maanden, tegenover een 'druk op de knop' en andere analyse bij ICOV.
Een rapportage is een 'snel intelligenceproduct', dat volgens ICOV te beschouwen is als 'sturingsinformatie', maar niet als bewijsvoering. In rechtszaken levert ICOV-informatie alleen waarschijnlijk niet afdoende bewijs. Voorbeelden van op deze manier inbeslaggenomen criminele vermogens zijn niet voorhanden.
Dat komt deels omdat het intelligenceproduct een schakel in een veel groter geheel en deels omdat er relatief veel tijd verstrijkt tussen de beslaglegging en de uiteindelijke veroordeling/executie: ICOV bestaat pas sinds 2013.

Uit tevredenheidsonderzoek onder de deelnemers blijkt dat ICOV in het algemeen wordt gewaardeerd met een 7,5. Vooral de snelheid wordt zeer gewaardeerd. ICOV is in de loop van anderhalf jaar wel relatief meer bij complexe zaken betrokken geraakt, zoals ondermijnende criminaliteit van de XTC-productie en hennepteelt, en terrorismefinanciering.
Het aantal aanvragen is nu nog goed te behappen, maar bij voortgaande groei kan er een probleem ontstaan en zal ICOV bij gelijkblijvende capaciteit de aanvragers/deelnemende organisaties mogelijk moeten gaan bewegen selectiever te worden in hun aanvragen.

De waardering voor themaonderzoeken blijft achter, wat ICOV zelf ook onderkent: de themaonderzoeken zijn nog onvoldoende ontwikkeld en tijdrovend. Daardoor brengen ze (nog) niet altijd de gehoopte uitkomsten en aansluiting bij behoeften, omdat er te lang op moet worden gewacht.

iCOV voert hooguit tien tot vijftien themascans per jaar uit, want ze zijn arbeidsintensief. Voor iCOV is dit het product waarvoor nog het meest te ontwikkelen valt en daarmee wordt in 2016 een aanvang gemaakt.
Overigens meldde het kabinet in een brief aan de Kamer dat een investering vanaf 2013 in de strafrechtketen van 20 miljoen euro voor de beslagname op crimineel vermogen moet leiden tot 60 miljoen meer inbeslaggenomen crimineel vermogen. De doelstelling is dat er vanaf 2016 jaarlijks ruim 100 miljoen aan crimineel vermogen in beslag wordt genomen; in 2013 was dat bijna 90 miljoen euro volgens het OM, in 2014 al 136 miljoen en in 2015 143,5 miljoen.[253]

12.6 HINDERPALEN EN VRAAGTEKENS

iCOV is een jong samenwerkingsverband, dat vooral worstelt met juridische grondslagen: er kan ontzettend veel, maar wat is toegestaan op grond van vooral privacyregels? De vraagstukken op een rij:

- Complexe maatschappelijke vraagstukken vereisen een multidisciplinaire oplossing;
- Complexe maatschappelijke vraagstukken (waaronder fraude, ondermijnende criminaliteit, problematiek in het zuiden van het land etc.) kunnen niet door één enkele overheidspartner alleen worden opgelost; ze vergen een multidisciplinaire en gezamenlijke/afgestemde aanpak, aldus het hoofd iCOV. Daartoe werken verschillende overheidsorganisaties verregaand samen vanuit verschillende disciplines/expertises en met behulp van verschillende databronnen die binnen de overheid voorhanden zijn. De huidige wetgeving biedt echter geen grondslag voor een dergelijke verregaande vorm van samenwerking en gebruikmaking van gecombineerde data (en Big Data); gegevensuitwisseling kan slechts plaatsvinden op basis van de bevoegdheden die door een van de organisaties wordt aangewend.

Zo werkt iCOV in de praktijk ook: een aanvrager van een iCOV-intelligenceproduct mag alleen die informatie ontvangen die hij op basis van zijn wettelijke bevoegdheid mag aanvragen. Binnen iCOV worden alleen gegevens verwerkt als daar door een deelnemende organisatie om wordt verzocht (100 procent vraagsturing), zodat helder is op grond van welke taak, welke bevoegdheid en met welk doel de gegevens verwerkt worden.
De doelstellingen van veel participanten overlappen wel, maar zijn meestal niet eensluidend. Gechargeerd: de politie is niet of minder geïnteresseerd in belastingontduiking of zwart geld, de Belastingdienst niet in de crimineel verkregen inkomsten, zolang er maar belasting over wordt betaald.

253 Voortgang Rijksbrede aanpak van fraude http://www.tweedekamer.nl/vergaderingen/commissieverga deringen/details?id=2015A00838)

Daardoor is er geen toereikende, eenduidige grondslag om complexe problematiek in zijn geheel (bijvoorbeeld de aanpak van illegaal geld en fraude) te omvatten en via samenwerking en informatie-uitwisseling het hoofd te bieden.

Doelbinding

Partijen die deelnemen en willen deelnemen, moeten aantonen dat hun taak aansluit bij het doel van ICOV, te weten het opsporen van crimineel en onverklaarbaar vermogen dan wel het blootleggen van witwas- en fraudeconstructies of het alsnog innen van overheidsvorderingen. Anders kunnen ze niet toetreden tot het convenant.
ICOV zelf beschouwt deze doelbinding op zich niet als een probleem. Wel de 'niet-eenduidige doelstellingen' van de samenwerkende partners, waardoor een toereikende, eenduidige grondslag ontbreekt om complexe problemen als geheel aan te pakken.

Proportionaliteit en dataminimalisatie

Behalve doelbinding is ook proportionaliteit een punt waarover veel gediscussieerd is: van de enorme hoeveelheid beschikbare data wordt maar een fractie gebruikt in de rapportages. Het is noodzakelijk om wel alle gegevens te hebben, omdat anders de verbanden tussen de gegevens niet gelegd kunnen worden en van tevoren ook niet gezegd kan worden van wie gegevens moeten worden opgevraagd. Dat weet je pas bij de aanvraag van het product. Van elke Nederlander zijn veel data voorhanden.
Het aantal 'productieopdrachten' van ICOV dat wordt aangevraagd door de deelnemende partners, bedraagt circa vijftienhonderd per jaar. Minder dan een promille van de personen van wie grootschalig data bijeengebracht zijn, zijn ook onderwerp van onderzoek.
Het is dus enerzijds noodzakelijk om alle gegevens klaar te hebben staan onder verantwoordelijkheid van de aanleverende partij, maar anderzijds worden deze zeker niet allemaal gebruikt. Als gezegd, worden alleen die vragen beantwoord die op basis van de juiste wettelijke bevoegdheid mogen worden beantwoord.

Wellicht ten overvloede: er is dus eerst een verdenking nodig en een vordering van de officier van justitie om fiscale data te kunnen ontsluiten en te mogen verstrekken aan de politie. Deze toestemming van het OM is een afdoende juridische dekking en de inzet van deze wettelijke bevoegdheid wordt getoetst door de strafrechter. Met de toename van de hoeveelheid databestanden wint deze bevoegdheid aan belang.

Juridische voorzichtigheid

Juristen worstelen met de grenzen van de regelgeving en kiezen snel voor voorzichtigheid, wellicht te snel volgens de uitvoerende diensten. Maar, zo redeneert ICOV, vertrouwen komt te voet en gaat te paard.

En daarom zeggen de deelnemende partners binnen iCOV te kiezen voor zorgvuldigheid en het wikken en wegen van de inzet van middelen.
Ook vereisen de juiste werking van het juridisch kader en nieuwe juridische vragen continue scherpte en aandacht. iCOV valt onder de ministeriële verantwoordelijkheid van de ministeries waaronder de deelnemende organisaties vallen.
De wetgever ontvangt geen periodieke rapportages over de voortgang. Door het hoofd iCOV wordt twee tot drie keer per jaar over de voortgang en activiteiten van iCOV verantwoording afgelegd aan de opdrachtgevers in een besloten opdrachtgeversoverleg; de hoogste leidinggevenden van de participerende overheidsorganisaties die aan iCOV deelnemen, hebben hierin zitting.
Als toezichthouder kan de Autoriteit Persoonsgegeven besluiten tot een onderzoek naar privacy bij iCOV, net als bij alle andere overheidsinstellingen. iCOV heeft op eigen initiatief eind 2013 een presentatie gegeven bij de AP over de opzet van de productieomgeving. De AP had daarbij vooral aandacht voor de gedeelde verantwoordelijkheid in de productieomgeving. Sindsdien is binnen iCOV verder nagedacht over de mogelijkheden van datamining.

Transparantie
iCOV wil de exacte werkwijzen voor zich houden om te voorkomen dat verdachten en criminelen aan de weet komen hoe ze digitaal speurwerk kunnen ontlopen. Openbaarmaking van deze 'keukengeheimen' staan op gespannen voet met het recherchewerk. Slagvaardigheid en succes komen dan in het gedrang.
iCOV vreest dat verdachten en veroordeelden het vastleggen van relevante data zullen ontwijken, zodra ze kennis hebben van de methoden. Zo zijn van de drie producten de beschikbare en gebruikte data van participanten exact beschreven, maar niet openbaar.
Vanzelfsprekend kan iCOV desgewenst gevraagd worden tekst en uitleg te geven in bijvoorbeeld een strafzaak waarvan iCOV-producten gebruik is gemaakt. De processen zijn nog niet extern gecontroleerd of getoetst.
In 2016, doorlopend in 2017, zal een audit plaatsvinden. Deze toets richt zich per kwartaal achtereenvolgens op a) werken volgens het juridisch kader; b) informatiebeveiliging en c) professioneel proces. De audit wordt gehouden door de auditdienst van het Parket Generaal van het OM.

Het convenant, de protocollen en mandaatregelingen zijn wel openbaar. De daaruit voortvloeiende praktische criteria per soort product zijn vastgelegd in een productenoverzicht dat vertrouwelijk is. Ook de beschikbare bestanden, waarvan een aantal is genoemd, zijn niet openbaargemaakt. iCOV valt onder de Wet openbaarheid van bestuur (WOB), de beantwoording daarvan loopt via de ministeries van Financiën en Veiligheid & Justitie).
Afstemming om tot (R&D-)onderzoek te komen vergt soms (te) veel tijd. Als voorbeeld kan dienen het project Subjectgerichte Aanpak Beroepsfraudeurs, dat onder meer tot doel heeft om typologieën van beroepsfraudeurs op te stellen. Alle

betrokken partijen onderschrijven dit doel, maar juridische vragen over levering en gebruik van data zorgen voor vertraging.

Vertraging in levering van data

Begrensd wordt het samenwerkingsverband bovendien door praktische problemen. Zo liep/loopt de levering van data door deelnemende partijen, bijvoorbeeld politiedata, onder meer als gevolg van een brede reorganisatie van de politie en samenhangend vele juridische vragen, vertraging op. Ook speelt bij sommige partijen koudwatervrees om de data beschikbaar te stellen, een rol.

Doorspelen van informatie

Goede rechercheurs halen hun informatie op tal van plaatsen. Zo komt het voor dat onderzoekers werken met (overzichts-)informatie uit verschillende bronnen verkregen (eigen systemen, open bronnen, FIU, Justis/track, etc.). iCOV heeft een beperkte scope van partijen met wie zij samenwerkt en aan wie zij intelligenceproducten mag verstrekken. Tegelijkertijd nemen de deelnemers aan iCOV ook aan andere samenwerkingsverbanden deel. Dat maakt de kans op het doorspelen van informatie van een iCOV-product – zonder dat opnieuw goed getoetst is of die informatie wel met al die andere partners gedeeld mag worden – niet ondenkbeeldig. Zo kan een FIOD-ambtenaar of een medewerker van de Belastingdienst de verkregen informatie ook in een andere context inbrengen, bijvoorbeeld in een Regionaal Informatie en Expertise Centrum (RIEC).
iCOV kan voor doorverstrekking geen verantwoordelijkheid dragen; het is aan degene die de iCOV-rapportage op basis van zijn eigen bevoegdheden heeft verkregen, om te bepalen of hij die informatie kan/mag delen met anderen (bijvoorbeeld op basis van de regels van dat andere samenwerkingsverband).
iCOV waarschuwt bij verstrekking wel voor oplettendheid op dit punt. Uiteindelijk is het aan de rechter om te toetsen of het doorspelen van informatie rechtmatig was. Uiteraard houdt AP ook hierop toezicht en hebben alle organisaties privacyfunctionarissen in dienst, die adviseren over informatie-uitwisseling en informatieverstrekking.
Er wordt daarbij getrapt gewerkt: een brokje verkregen informatie met een concrete verdenking wordt gemengd met eigen onderzoek en keert terug in een uitgebreider vervolgvraag, bijvoorbeeld omdat daarmee een verdenking sterker is geworden of zich heeft uitgebreid tot andere personen.

Gebrekkig kader

Het samenwerkingsverband worstelt ook met de vraag of en, zo ja, in hoeverre de huidige regelgeving allerlei typen van gegevensverwerking toestaat. Dat geldt vooral voor het gebruik van geavanceerde analysemethoden met gekoppelde bestanden. Onduidelijkheid belemmert de ontwikkeling van Big Data-toepassingen. Zie ook de hinderpalen/vraagtekens hierboven.

Big Data-analyse is weinig gereguleerd door daarop toegespitste heldere wet- en regelgeving. Deze wetgeving is geschreven in een tijd dat deze technische mogelijkheden er nog niet waren en dat maakt deze moeilijk toepasbaar daarop. Grondslagen zijn nu te vinden in de specifieke aanvragen die bij ICOV worden gedaan en dat leidt tot belangrijke informatie, maar niet tot een totaalplaatje. Voor het oplossen van complexe (ondermijnende) maatschappelijke problematiek bestaat bij samenwerkingsverbanden als ICOV grote behoefte aan een meer generieke grondslag waarmee ook complexe fraude- of witwasproblemen gezamenlijk aangepakt kunnen worden. Ook de op handen zijnde Kaderwet zal daarin – op basis van de huidige uitgangspunten – vermoedelijk niet voorzien.
Dat brengt het risico mee, aldus ICOV, dat de informatieproducten losse puzzelstukken blijven, die niet of slechts deels in elkaar passen. Daarmee kan het doel om tot een beter inzicht te komen in de problematiek en tot een gezamenlijke aanpak, niet worden bereikt. Nu moet steeds weer de specifieke grondslag van de aanvrager als uitgangspunt dienen.
Elke deelnemende organisatie is gebonden aan specifieke restricties in gegevensuitwisseling. Vanuit zijn taakstelling is ICOV er vooral in geïnteresseerd dat er wel een generieke grondslag komt, zodat het de deelnemers aan het samenwerkingsverband beter van dienst kan zijn.
ICOV is nu beperkt in de mogelijkheden om bijvoorbeeld de vraag in een politieonderzoek om data van de Belastingdienst te beantwoorden in de fase waarin een concrete verdenking nog ontbreekt. In hoeverre kan dan de fiscale geheimhouding worden opgeheven?
Voor een verkennend onderzoek (themaonderzoek op grond van aanwijzingen bestaat geen juridische titel, behalve voor terrorisme (Artikel126gg/hh Sv), waarvoor wel bestanden gevorderd kunnen worden. Voor ernstige vormen van (grootschalig) witwassen of fraude bestaat zo'n grondslag niet.

Over waar die grondslag een plek zou moeten krijgen (bijvoorbeeld in opsporingswetgeving of in wetgeving voor handhaving en toezicht etc.), bestaat nog geen duidelijkheid. Er zijn verschillende mogelijkheden om zo'n grondslag, uiteraard met voldoende waarborgen, vorm te geven.
Gedacht kan worden aan uitbreiding van het verkennend onderzoek in het Wetboek van Strafvordering, het opnemen van nieuwe mogelijkheden in de Algemene Wet op de Rijksbelastingen of opname in een nieuwe wet die fraude en witwassen tegen moet gaan.
Met een generieke grondslag wordt het mogelijk om verschillende soorten gegevens (van de overheid) te kunnen gebruiken om problematiek integraal te kunnen aanpakken (zie hierboven). Het voert hier te ver om aan te geven hoe dat er precies uit zou moeten zien.

Het kabinet meldde in april 2015 aan de Kamer: 'Om gesjoemel effectiever te kunnen aanpakken wil het kabinet de informatie-uitwisseling verbeteren. Samenwer-

kingsverbanden als de Regionale Informatie en Expertise Centra (RIEC's) en de Infobox Crimineel en Onverklaarbaar Vermogen (iCOV) kunnen hier baat bij hebben. Het kabinet denkt eraan om een nieuwe wet te maken die de gegevensuitwisseling voor de aanpak van fraudebestrijding moet versoepelen […] Nieuwe wetgeving kan de gegevensuitwisseling vergemakkelijken, zodat bijvoorbeeld politie en justitie gegevensuitwisseling niet meer per samenwerkingsverband hoeven te regelen.'[254]
Naast het aanpakken van een aantal bekende beroepsfraudeurs wordt in het kader van dit rijksbrede project medio 2015 ook een verkenning afgerond naar een meer innovatieve manier van data-analyse met als doel
breder bruikbare indicatoren van beroepsfraudeurs in het Nederlandse publieke domein vast te stellen. Het doel van de verkenning is om risicoprofielen op te stellen die tot nieuwe inzichten en een meer effectieve aanpak van beroepsfraudeurs kunnen leiden.[255]

12.7 TOEKOMSTIGE OPTIES MET BIG DATA

iCOV heeft een 'potentieelverkenning R&D' laten uitvoeren om mogelijke ontwikkelrichtingen in kaart te brengen. Daarbij is gesproken met universiteiten, onderzoeksinstituten, met de eigen participerende organisaties in het samenwerkingsverband, waaronder met betrokkenen bij SyRI, E-Law (Universiteit Leiden), TU Twente, de Vrije Universiteit Brussel, NFI (Kecida), het Rathenau Instituut en de IND.

Deze verkenning leverde een aantal inzichten op:
- Het potentieel van datamining op de bij iCOV beschikbare data wordt enorm geacht door de experts.
- De technieken kunnen zowel beschrijvend als voorspellend worden ingezet.
- Fraudebestrijding vraagt om dynamische modellen, gezien de voortdurend veranderende kenmerken van dit fenomeen.
- Op hoofdlijnen zijn er twee analysemethoden te onderscheiden waarmee meer informatie uit de data gehaald kan worden, te weten één waarbij met beslisregels en beslisbomen wordt gewerkt, de andere waarbij in neurale netwerken gebruik wordt gemaakt van kunstmatige intelligentie. Deze methodieken kunnen elkaar aanvullen.

254 Deze op handen zijnde Kaderwet gegevensuitwisseling zal er wellicht in voorzien dat samenwerkingsverbanden gegevens mogen doorgeven aan de politie en aan het OM zonder gerechtelijke vordering. De Autoriteit Persoonsgegevens is kritisch, evenals privacyorganisaties. Ze willen betere waarborgen en restricties.

255 Voortgang Rijksbrede aanpak van fraude http://www.tweedekamer.nl/vergaderingen/commissieverga deringen/details?id=2015A00838

- Het is verder mogelijk om door het gebruik van technologie vooroordelen te reduceren. Op dit moment gebruiken de opsporingsinstanties vaak 'de criminele achteruitkijkspiegel' (meer onderzoek doen rond groepen waarvan je al weet dat ze crimineel zijn). Door het gebruik van nieuwe technieken is het ook mogelijk nieuwe fenomenen/groepen in beeld te krijgen. Door gebruik te maken van Privacy Enhancing Technologies kunnen de privacyrisico's daarbij worden beperkt.
- Geautomatiseerde besluitvorming is verboden volgens de Wet bescherming persoonsgegevens.
- Uitkomsten van toepassing van nieuwe technologie kunnen ook gebruikt worden om juist een *green lane* te creëren: dat betekent het met rust laten of belonen (bijvoorbeeld door een snellere behandeling/toekenning van middelen aan of) van degenen die aan de indicatoren voldoen. Bijvoorbeeld door bij de Belastingdienst/toeslagen de aanvragen die 'groen' zijn, versneld te behandelen en de aanvragen die 'rood zijn' allemaal extra te bekijken. Aangezien iCOV juist tot doel heeft om crimineel en onverklaarbaar vermogen te traceren, ligt het meer in de rede om de inrichting van een dergelijk systeem bij de deelnemende organisaties (en dan met name de Belastingdienst) te laten.
- Op geaggregeerd niveau (geanonimiseerd) kunnen analyses meer inzicht geven in witwas- en fraudeconstructies. Die kennis kan door de deelnemende organisaties worden ingezet om opsporing, handhaving, toezicht en bedrijfsprocessen te verbeteren.
- Op subjectniveau zouden dergelijke analyses kunnen bijdragen aan een hogere pakkans, slimmere selectie van zaken en ook om anderen in beeld te krijgen dan diegenen die te zien zijn in de 'criminele achteruitkijkspiegel'.

Op dit moment is het echter juridisch niet mogelijk om dit met deze data op subjectniveau te doen: de bevoegdheden van de organisaties zijn hiervoor in het algemeen niet toereikend. Om dit mogelijk te maken is eerst een goede wettelijke grondslag nodig. Daarvoor is een politieke en maatschappelijke discussie over het gebruik van dit soort technieken in een combinatie van verschillende databronnen vereist. Vandaar dat iCOV dit niet doet op subjectniveau.
Dit probleem doet zich niet voor bij het verkrijgen van nieuwe kennis uit R&D op grond van geanonimiseerde data die op geen enkele wijze tot personen herleidbaar zijn. Ook dit kan leiden tot betere efficiency en keuzes in opsporing en uiteindelijk tot toename van terug te vorderen vermogen.

iCOV onderzoekt, in opdracht van zijn opdrachtgevers, op dit moment wat nodig is om een pilotproject te starten om op geaggregeerd niveau analyses te maken. Deze pilot zou moeten gaan plaatsvinden in een afgescheiden omgeving met beperkte data en leidt dus tot anonieme resultaten.
De opdrachtgevers van iCOV zijn voorzichtig, omdat ze zich realiseren dat negatieve beeldvorming over deze pilot een negatieve weerslag kan hebben op de pro-

ductieomgeving die zich al bewezen heeft. ('Denk aan SyRI, waarbij beeldvorming op de loop ging met de methode.')
De benodigde expertise zal ICOV vermoedelijk – deels – buiten de deelnemende organisaties moeten halen door bijvoorbeeld samen te werken met een onderzoeksinstituut. Aangezien ICOV zich nu nog aan het oriënteren is op de mogelijkheden, valt op dit moment nog niet te zeggen hoe deze pilot verder vormgegeven zal worden.

Kortom, deze mogelijke toekomstige ontwikkelingen verkeren nog in het stadium van verkenning en gedachtevorming. Het is nog niet duidelijk hoe een en ander daadwerkelijk vorm zal krijgen.

12.8 RISICOMELDINGEN MALAFIDE BEDRIJVEN EN JUSTIS

Op 1 juli 2011 trad de Wet controle op rechtspersonen (Wcr) in werking. Hiermee is het stelsel Verklaring van geen bezwaar (VVGB), verplicht bij de oprichting van rechtspersonen, vervangen door doorlopend toezicht op onder meer bedrijven en stichtingen. Voor handhaving werd in een het justitieprogramma Herziening Toezicht Rechtspersonen (HTR) het systeem Radar opgetuigd: Risicoprofielen, Automatische analyse, Distributie naar afnemers en Aanvragen op verzoek. Radar produceert risicomeldingen over mogelijk malafide bedrijven en stichtingen op grond van data uit de volgende bestanden:
– Nederlands Handelsregister (NHR);
– Basisregistratie Personen (BRP);
– Centraal InsolventieRegister (CIR);
– Justitieel Documentatie systeem (JDS).

Bij verdenking doet screeningsautoriteit Justis van het ministerie van Veiligheid en Justitie nader handmatig onderzoek naar de rechtspersoon, met aanvullende informatie uit (gesloten) bronnen, zoals van de Belastingdienst, het Kadaster en de Rijksdienst Wegverkeer. Justis en de leverancier van Radar formuleren en verfijnen risicoprofielen.
Van de meldingen duidt 80 procent op risico op faillissementsfraude, de rest betreft verdenkingen van witwassen, belastingfraude (ook btw), beleggingsfraude, drugs- en mensenhandel.
Justis zegt niet te weten wat de resultaten van deze exercities zijn, omdat de afnemers van risicomeldingen die niet willen of kunnen terugmelden. Er is alleen bekend dat de Belastingdienst, de Politie, het OM, de DNB, curatoren en andere partners (mede) mede dankzij de tips van Justis 'de nodige acties' verrichten, zoals vervolging van drugsproducenten, intrekking van vergunningen of onderzoek naar witwassen en Europese geldstromen.

Ook is bij de oprichting van bedrijven onwettige belastingteruggaaf voorkomen, zijn verdachte netwerken en bestuurswisselingen in beeld gebracht, en/of verdachten van fraude aangehouden en vervolgd.
Radar haalde de media door IT-problemen en een geschil met de toepassing van het systeem Alert.[256]
Het project mislukte daardoor aanvankelijk en leverancier Capgemini werd vervangen door zusterbedrijf Sogeti. In een brief aan de Tweede Kamer van augustus 2015 meldt de staatssecretaris van Veiligheid en Justitie dat Radar dan 'naar volle tevredenheid' werkt.[257] De exploitatie is in handen van de dienst Justis.
Al in de evaluatie van de Wet controle op rechtspersonen van januari 2014 is verslag gedaan van de aantallen verstrekte risicomeldingen en gevolgen.[258]

1 juli 2011 tot 1 juli 2013:
- Toezicht op circa 1 miljoen rechtspersonen;
  - 1,5 miljoen wijzigingen Handelsregister gedurende twee jaar;
  - 200.000 wijzigingen in automatische analyse door Radar;
  - 1368 systeemmelding;
  - 37 risicomeldingen verstrekt aan één of meer afnemers.

Daarnaast op verzoek van afnemers:
- 28 risicomeldingen;
- 1158 netwerkanalyses verstrekt.

Justis verstrekte cijfers over 2013 en 2014:[259]
- Ruim 1 miljoen rechtspersonen;
  2013:
  - 359.669 wijzigingen Handelsregister in Radar;
  - 1342 zaken door Justis opgepakt;
  - 145 risicomeldingen aan partners verstrekt.

256 Alert van Capgemini wordt ook genoemd als niet goed aangeslagen toepassing voor data-analyse bij bestrijding van uitkeringsfraude in het hoofdstuk over gemeenten.

257 29 911. Bestrijding georganiseerde criminaliteit, Nr. 116 brief van de staatssecretaris van veiligheid en justitie aan de Tweede Kamer, 27 augustus 2015
https://zoek.officielebekendmakingen.nl/dossier/29911/kst-29911-116

258 Evaluatie Wet controle op rechtspersonen, 23 januari 2014
https://www.rijksoverheid.nl/documenten/rapporten/2014/01/23/evaluatie-wet-controle-op-rechtspersonen
'Toezicht op rechtspersonen verstevigd', Nieuwsbericht Justis, 2 april 2015
https://www.justis.nl/Nieuws/2015/toezicht-op-rechtspersonen-verstevigd.aspx

259 Lijst van vragen en antwoorden over het Jaarverslag Ministerie van Veiligheid en Justitie 2014
https://www.tweedekamer.nl/kamerstukken/detail?id=2015Z10800&did=2015D21964

2014:
- 365.000 wijzigingen Handelsregister in Radar;
- 2094 zaken door Justis behandeld;
- 282 risicomeldingen aan partners;
- + 1110 'netwerktekeningen' geproduceerd.

'Justis verstrekt risicomeldingen efficiënter, sneller en meer op maat. Hierdoor kunnen samenwerkingspartners sneller en gerichter optreden', meldt de staatssecretaris in de brief aan Kamer. Zijn bron is Justis zelf echter en het is niet helemaal duidelijk wat de maatstaf was voor het meten van genoemde verbeteringen. Als resultaten werden genoemd: '[…] concrete vervolging door het oprollen van een drugslaboratorium voor amfetamine, intrekking van vergunningen of nader onderzoek naar witwassen en Europese geldstromen. Verder zijn nieuwe oprichtingen geblokkeerd om omzetbelastingfraude te voorkomen, verdachte netwerken in beeld gebracht, niet eerder waargenomen bestuurswisselingen bij de Belastingdienst verwerkt, beslagleggingen uitgevoerd of verdachten van fraude aangehouden en vervolgd[…].'
Ook Hans Blokpoel, Algemeen Directeur Belastingen, is naar zeggen van Justis lovend over Justis: 'De samenwerking met Justis draagt bij aan onze eigen aanpak om risico's zo vroeg mogelijk te detecteren. Ons doel blijft tenslotte om fraudes snel te stoppen en liefst zelfs voor te zijn.'

12.9 SLOT: NAAR EEN NIEUWE WET

Er zijn diverse Kamervragen gesteld over wat er aan data-uitwisseling tussen overheden plaatsvindt. Zo helder en eenvoudig als deze vragen zelf zijn, zo complex bleek het echter om daarop een antwoord te formuleren.
In maart 2015 stuurde minister Van der Steur een overzicht van koppelingen van databestanden door overheden naar de Tweede Kamer.
Het is een, ook letterlijk, zeer omvangrijk overzicht van 57 pagina's met tabellen.[260] Behalve dat het ontoegankelijk is en moeilijk leesbaar, ontbeert het overzicht ook informatie. Zo is niet duidelijk welke bestanden met welke doeleinden door welke organisaties zijn gekoppeld. De vermelding van een koppeling biedt evenmin een indicatie over de gebruikte techniek of de frequentie van de uitwisseling. Het overzicht is verder beperkt gebleven tot de rijksoverheid.
Er zijn koppelingen met basisregistraties uit het overzicht weggelaten, volgens de minister zijn deze 'al genoegzaam uit de vigerende wet- en regelgeving zijn af te leiden'. En ook zijn er koppelingen van bestanden weggelaten, als de nationale vei-

260 Bijlage bij Kamerbrief over gekoppelde databestanden van Minister van der Steur: Inventarisatie gegevensbestanden en koppelingen
http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2015/03/25/tk-inventarisatie-gegevensbestanden-en-koppelingen.html

ligheid of andere vitale belangen, zoals opsporingsbelangen, erdoor geschaad konden worden.
Bovendien hadden niet alle ministeries tijd genoeg gehad om hun lijstje in te leveren voor het overzicht. Kortom, dit overzicht, biedt niet het door de Kamer gevraagde inzicht in datakoppelingen.

In de Kamerbrief bij dit overzicht zet de minister uiteen dat het delen van data noodzakelijk is voor handhaving, aangezien 'het volume aan data, de variëteit aan data en de snelheid waarmee deze kunnen worden verwerkt, enorm toenemen'.[261]
Dat delen door overheden en het daartoe optuigen van samenwerkingsverbanden vormen een absolute noodzaak, aldus de minister, aangezien 'maatschappelijke problemen zich niet storen aan de reikwijdte van de taken van individuele overheidsorganisaties. Daarom is het wenselijk dat deze organisaties, waar nodig en mogelijk, steeds meer als een georganiseerd geheel optreden.'
De in 2013 opgerichte iCOV noemt hij een succesvol voorbeeld van data-uitwisseling en data-analyse. Dit orgaan kwam in dit hoofdstuk al uitgebreid aan bod. Volgens de minister mag een uitzondering op het recht op privacy – zoals vervat in Artikel 8 van het Europees Verdrag van de Rechten van de Mens (EVRM) – worden gemaakt, als er een wettelijke grondslag is, deze een in artikel 8 genoemd doel dient en nodig is in een democratische samenleving.
Volgens hem is daarvan sprake en wordt verder voldaan aan de vereisten van proportionaliteit en subsidiariteit van de privacywet (Wbp). De burger kan voor de verwerking van zijn persoonsgegevens toestemming hebben verleend, maar er kan ook aan voldaan worden met het uitoefenen van een wettelijke plicht of als de dataverwerking (en daarmee koppeling) noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak.
Ook aan de vereiste van doelbinding, het louter verstrekken van te koppelen data als dit niet onverenigbaar is met het doel waartoe ze aanvankelijk zijn verzameld, wordt volgens hem voldaan. De organisaties moeten het doel van de samenwerking onderschrijven en aan de verwerking moeten strakke voorwaarden zijn verbonden, zoals bijvoorbeeld in de Wet Suwi voor SyRI is vastgelegd.
In deze overheidsbrede datakoppeling – dat niet in het overzicht stond – speelt volgens de minister het Stelsel van Basisregistraties wel een cruciale rol voor de kwaliteit en transparantie van uitwisseling van gegevens en koppeling van bestanden binnen de gehele overheid.

261 Kamerbrief over gekoppelde databestanden – Minister van der Steur (VenJ) informeert de Tweede Kamer over de koppeling van databestanden bij de overheid. 23 maart 2015 http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2015/03/25/tk-gekoppelde-databestanden.html

Naar een nieuw regime

Enkele maanden eerder lag er wel een inzichtelijk overzicht van samenwerkingen met het delen van data, zij het beknopter van omvang. Het is een bijlage in de verkenning voor een nieuwe 'Kaderwet gegevensuitwisseling'. Aangezien de uitbreiding van het delen van data steeds meer spanningsvelden oplevert met bestaande wetgeving, zet het kabinet in op een nieuwe wet die gegevensuitwisseling eenvoudiger moet maken. Daartoe is een verkenning uitgevoerd, die eind 2014 openbaar werd. De verkenning is opgesteld door een ambtelijke werkgroep, bestaande uit vertegenwoordigers van de ministeries van VenJ, SZ en Financiën, het OM en de gemeente Tilburg.[262]

Het intrigerende stuk werd niet opgemerkt door de parlementaire pers. Het handelt over de vraag of legitimering mogelijk is over een breed terrein voor 'allerlei samenwerkingsverbanden die gegevens binnen en tussen het bestuursrechtelijke en strafrechtelijke domein willen uitwisselen'. De doelstelling is het wegnemen van knelpunten die optreden bij de uitwisseling van data, met name opgeworpen door de Wet bescherming persoonsgegevens (Wbp) en de op handen zijn Europese privacyverordening.[263]
Het gaat vooral om het inrichten van een 'zorgvuldig proces' voor data-uitwisseling tussen instanties en toepassing voor analyses, zoals is gebeurd voor het onderdeel SyRI van de Wet Suwi. Ingezet wordt op een wet die de algemene principes, verantwoordelijkheden en procedures regelt, maar die geen gedetailleerde regels bevat.
Een kaderwet moet een raamwerk bieden waarbinnen de deelnemers aan een samenwerkingsverband hun samenwerking nader uitwerken in een convenant en in een informatieprotocol, dat de nodige waarborgen voor de bescherming van persoonsgegevens bevat. De beoogde kaderwet 'legitimeert, faciliteert en normeert' de data-uitwisseling. Vooral de randvoorwaarden moeten benadrukt worden waarbinnen overheden en samenwerkingsverbanden hun gebruik van data zelf kunnen invullen zonder verder met regels in botsing te komen.

Volgens de verkenning creëert een kaderwet een 'ja, tenzij' in plaats van een 'nee, tenzij', die de beoogde samenwerkingen in data nu te veel remt. Door geheimhou-

---

262 Kennis delen geeft kracht – Naar een betere én zorgvuldigere gegevensuitwisseling in samenwerkingsverbanden', Rapport van de Werkgroep Verkenning kaderwet, 5 december 2014, verzonden door minister Opstelten aan de Tweede Kamer, 19 december 2014
https://www.tweedekamer.nl/kamerstukken/detail?id=2014D48109&did=2014D48109

263 Algemene wet inzake rijksbelastingen (Awr), Wet politiegegevens (Wpg)
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.
http://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:31995L0046&qid=1397211648283

dingsbepalingen en andere beperkingen 'buiten toepassing' te verklaren moet ruimte ontstaan voor data-uitwisseling in samenwerkingen. Regelgeving voor opsporing moet transformeren van 'nee, tenzij' naar 'ja, tenzij'.
De geheimhoudingsbepalingen worden in feite vervangen door een algemene grondslag voor dataverstrekking in een kaderwet. Wel moeten partijen die data uitwisselen dan nog een convenant opstellen, waarbij ze zich beroepen op de ruimte in de kaderwet. 'Accountability', later rekenschap geven c.q. verantwoording afleggen is belangrijk. Dus moet de beoogde kaderwet ook voorschrijven dat de samenwerkingsverbanden vastleggen wat ze aan data gebruiken en waarom. Volgens de werkgroep kan in 'accountability' worden voorzien door in het openbare informatieprotocol de databescherming vast te leggen door de inrichting van het proces te beschrijven en aan te geven dat dit voldoende waarborgen biedt voor deze bescherming.
Een eigen doelbinding van de data-uitwisseling in een samenwerkingsverband voorkomt dat deze niet verenigbaar is met de doeleinden waarvoor de gegevens oorspronkelijk zijn verkregen. Immers, de vereiste van doelbinding blijkt nu in de praktijk bij tijd en wijle een rem te zetten op (de bereidheid om) gegevens uit te wisselen. Volgens de verkenning nemen partijen daarbij 'soms een te krampachtige houding' aan.

Alle deelnemers aan een samenwerkingsverband moeten de data kunnen gebruiken, ook private partijen. Immers, publiek-private samenwerking bij fraudebestrijding en de aanpak van andere vormen van wetsovertreding leveren alle partijen voordeel op.
De beoogde kaderwet zou de beperkingen die er nu zijn vanuit de Wet bescherming persoonsgegevens, kunnen wegnemen. Overigens lijkt de nieuwe Algemene verordening gegevensbescherming van de Europese Unie meer ruimte te geven om in de toekomst ook ingeval van onverenigbaarheid van doelen in een samenwerkingsverband toch gegevens te kunnen verwerken.

Ook de verstrekking aan opsporingsinstanties en het OM wordt eenvoudiger. Daarmee worden barrières weggenomen voor de samenwerking tussen bestuurlijke en strafrechtelijke instanties, wat 'bij uitstek meerwaarde zal hebben bij fraudebestrijding en andere activiteiten op het terrein van de rechtshandhaving en criminaliteitsbestrijding'.
Nu nog vormt het Wetboek van Strafvordering en het systeem voor het vorderen van informatie door opsporingsinstanties en het OM barrières voor een 'efficiënte vorm van gegevensuitwisseling' in samenwerkingsverbanden, aldus de werkgroep. Het College van procureurs-generaal van het OM wees eerder op dit probleem. Door de bepalingen ingeval van data-uitwisseling in samenwerkingsverbanden buiten toepassing te verklaren, zou onder een kaderwet een juridische vordering voortaan niet meer nodig zijn.

Andersom moet de beoogde kaderwet het mogelijk gaan maken dat strafrechtelijke gegevens door de politie, bijzondere opsporingsdiensten en het OM ook aan andere partijen binnen het samenwerkingsverband ten goede komen. De bestaande mogelijkheden zijn te beperkt.
Zo moeten voor bijvoorbeeld de verstrekking van politiegegevens aan de Regionale Informatie- en Expertisecentra (RIEC's) vier schakels worden doorlopen: een machtigingsbesluit op grond van de Wet politiegegevens, een wijziging van het Besluit politiegegevens, plus de opstelling van een convenant en protocol. Op basis van de kaderwet zal volstaan kunnen worden met vastlegging van de verstrekking van politiegegevens, strafvorderlijke gegevens en justitiële gegevens bij convenant en nadere uitwerking daarvan in een informatieprotocol, zo meent de werkgroep.

Tevens zal de beoogde kaderwet voorzien in een betere legitimatie van het gebruik van moderne analysetechnieken. Samenwerkingsverbanden worstelen met de vraag of en, zo ja, in hoeverre de huidige regelgeving geavanceerde analysemethoden toestaat. Zo moet ICOV voor de bestrijding van 'beroepsfraudeurs' data van personen en gelieerde bedrijven en netwerken verregaand kunnen matchen.
Ook komt dan van pas dat de kaderwet de informatieplicht van de privacywet en -verordening afzwakt. Immers, verplicht informeren van personen over verwerking van hun data leidt uiteraard tot calculerend gedrag bij verdachten en daarmee vermindering van de pakkans.

Ter compensatie van het wegvallen van de verplichting de burger individueel te informeren, denkt de werkgroep aan een passage in de kaderwet die algemene informatie over de gegevensverwerking door samenwerkingsverbanden voorschrijft en op de website publiceert. Dan weet iedereen te voren dat die gegevens onderwerp van onderzoek en data-uitwisseling kunnen zijn.
De noodzakelijke bepalingen over noodzakelijkheid van uitwisseling en de beginselen van proportionaliteit en subsidiariteit van de privacywetgeving alsmede transparantie moet geborgd worden met een Privacy Impact Assessment, een privacy-analyse per samenwerking en convenant om grenzen te bepalen.
In het slotwoord stelt de werkgroep dat de beoogde kaderwet een expliciete legitimatie zal geven aan gegevensverwerking in de vorm van data-analyse en profilering teneinde intelligence te verbeteren. Zo 'kan met een kaderwet het signaal worden afgegeven dat er meer mogelijk is dan wordt verondersteld'.

Tegenover betere mogelijkheden tot gegevensverwerking staan ook betere waarborgen voor een zorgvuldige verwerking en bescherming van persoonsgegevens dan nu het geval is met ad-hoc samenwerkingen, belooft de werkgroep. Aanvankelijk zou de Tweede Kamer in de huidige samenstelling nog moeten stemmen over nieuwe wetgeving om meer veel data-analyse mogelijk te maken.

Voltooiing van het concept-wetsvoorstel is verschoven van eind 2015 naar eind 2016. Op dat moment zullen het politieke en het maatschappelijke klimaat door de naderende verkiezingen in 2017 ongetwijfeld een rol spelen tijdens de stemming over het nieuwe wetsvoorstel.
Dit is niet de plaats om te speculeren of dat klimaat dan gunstiger is voor de handhaving en voor de opsporing van fraude. Nog minder voor de suggestie dat de hoop wordt gevestigd op een gunstiger klimaat voor samenwerkingsverbanden zoals iCOV om de mogelijkheden voor data-analyse en daarmee de bestrijding van criminaliteit aanzienlijk uit te breiden.
Het is niet uit te sluiten dat politieke partijen zich bij een stemming juist vóór de verkiezingen zullen keren tegen zo'n wet vanwege maatschappelijke zorgen om privacy die in de mediacratie doorgaans ruime aandacht krijgen.
Het uitstel biedt wel de mogelijkheid om langere tijd te besteden aan het maatschappelijke debat over het evenwicht tussen bestrijding van fraude, criminaliteit en terrorisme enerzijds en privacy anderzijds. En om voorwaarden te formuleren waarmee een adequaat oordeel mogelijk is over de effectiviteit van de – al dan niet verruimde – mogelijkheden voor data-analyse.

13 CONCLUSIE

INLEIDING

Ten minste 2,5 miljard aan onjuiste declaraties in de zorg, bijna een half miljard jaarlijkse belastingwinst nu plus een miljard verwachte toekomstige extra 'winst', 100 miljoen aan crimineel vermogen en honderden miljoenen minder uitkerings- en toeslagenfraude per jaar. O ja, ook 50.000 minder spookburgers. Analyse van data, al dan niet 'big', levert veel op.

Het combineren van databestanden ligt hieraan meer en meer ten grondslag. Het aantal samenwerkingsverbanden en hun activiteiten in fraudebestrijding groeien gestaag. Met toenemende bundeling van informatie voor gezamenlijke analyse, ook door koppeling van databestanden.
Er ontstaat, nog los van het officieel ontwikkelde Stelsel van Basisregistraties en daaruit mogelijk voortvloeiende Stelsel van Overheidsgegevens, reeds een enorm en snel groeiend datacomplex van de diverse overheden en bestuursorganen tezamen.
Ofschoon het veelal gestructureerde data zijn met analyse gericht op concrete zaken, gaat het meer en meer richting 'Big Data'. Dit geschiedt grotendeels onopgemerkt, zowel een gevolg van het gebrek aan transparantie als door het gebrek aan aandacht van media en politiek voor dit fenomeen.

Deze casestudy beschrijft als eerste uitvoerig de data-analyse van en met overheden voor fraudebestrijding. En doet dat in een grote hoeveelheid feiten en details, die tot op heden vaak onbekend, dan wel versnipperd en verspreid aanwezig waren in nauwelijks opgemerkte verslagen en Kamerstukken.
Dit relaas is niet uitputtend, maar toont de belangrijkste terreinen van de inzet van analyse van data, in grote en minder grote hoeveelheden, ten behoeve van fraudebestrijding.
De noodzaak bij instanties om diverse vormen van fraude te bestrijden is groot, want ten aanzien van fraude circuleren grote bedragen, uiteenlopend van 5 tot 16 miljard euro per jaar, met zelfs op nattevingerwerk gebaseerde uitkomsten als 30 miljard fraudeschade, die als bron wordt genoemd voor speurzin.
Een bedrag van 11 miljard euro aan fraude is het meest genoemd, ofschoon 'je weet niet wat je niet weet' ook voor fraude geldt. 'Fraude' is in onderhavig rapport overigens een ambigu begrip. Het gaat op de eerste plaats om risico's en verdenkingen die vanuit analyse van data ontstaan. De vervolgens werkelijk vastgestelde fouten kunnen een gevolg zijn van onwetendheid, slordigheid en pure opzet. In het laatste geval volgt meestal geen strafzaak, mede gezien de te groot geachte inspanningen en tijdsbeslag.

13.1 POLITIEKE WENS

De Tweede Kamer legde de afgelopen jaren de nadruk op de 'integrale inspanning' voor fraudebestrijding en op minder 'versnippering'. Het kabinet antwoordde met 'rijksbrede anti-fraudestrategie' van een ministeriële commissie-Aanpak Fraude; onder voorzitterschap van de premier en de minister van VenJ als coördinator. Ook de ministers van SZW, EZ, VWS, BZK, OCW, Wonen en Rijksdienst en de staatssecretaris van Financiën zijn vaste deelnemers aan de ministeriële commissie-Aanpak Fraude. Van verslaglegging van dit gezelschap is overigens niets meer vernomen. Er kwam een reeks domeinoverschrijdende voornemens.
Dit leidde in de praktijk tot het steeds sterker inzetten op de toepassing van gezamenlijke data-analyse door overheden en zelfstandige bestuursorganen, eventueel aan te vullen vanuit de private sector. Met name de ministeries van Financiën (vanuit de Belastingdienst), BZK (identiteits- en adresfraude), SZW (uitkeringsfraude) en VenJ (criminaliteit, witwassen) smeden verbanden voor gezamenlijk gebruik van databestanden.
In het private domein leiden de zorgverzekeraars de datadans voor fraudebestrijding, een gevolg van de ingezette marktwerking.
Data-analyse ten behoeve van het speuren naar fraude met uitkeringen van het UWV en de SVB zijn heden minder omvangrijk en intensief dan voor de bijstand (WWB), maar de mogelijkheden voor grootschalige analyse zijn aanzienlijk. Vooral het UWV heeft verregaande, gedetailleerde plannen om data in te zetten voor fraudebestrijding en daar ook kennis voor in huis. De SVB is een stuk bescheidener met haar ambities en komt op achterstand door problemen met uitvoering (pgb) en mislukte IT. De SVB waarschuwt ook voor te hoge verwachtingen van opbrengsten van risico-analyse met data.
Overigens belopen de winsten in het sociale domein naar verwachting eerder in de tientallen miljoenen per jaar, veel minder dan bijvoorbeeld de (potentiële) miljardenopbrengsten met behulp van onder meer data-analyse die in de zorg, met het witwassen en al dan niet bewuste belastingontwijking en –ontduiking haalbaar zijn.
Dit in weerwil van de publieke opinie, waarin de verontwaardiging over fraude met uitkeringen het grootst is. Direct betrokkenen wijzen op de gevolgen van deze maatschappelijke onvrede over het 'trekken' van uitkeringen. In relatie tot de omvang van de fraude is de data-inzet voor bestrijding van bijstandsfraude volgens hen verreweg het meest intensief.

Echter, welke bijdrage de data-analyse en koppeling van bestanden aan de fraudebestrijding levert, is moeilijk hard te maken. Voorlopers als Belastingdienst, zorgverzekeraars en iCOV (financiële criminaliteitsbestrijding) spreken van enorme bijdragen. Die nauwelijks te specificeren zijn wat betreft het succes van data-analyse, omdat ze een onderdeel vormen van processen. Eerder genoemde bedragen worden er (groten)deels aan opgehangen.

13.2 ZOVEEL MOGELIJK DATA

Teneinde fraude en risico's daarop in beeld te krijgen, willen fraudebestrijders en hun organisaties over zoveel mogelijk relevante dataverzamelingen beschikken. Gecombineerd gebruik vergroot de mogelijkheden voor bepaling van verdenkingen van gepleegde en nog te plegen fraude aanzienlijk.
Er is een beweging gaande naar één overheid wat betreft gebruik van databestanden. De domeinen van SZW (uitkeringen) en Financiën (belastingen en toeslagen) raken verweven met criminaliteitsbestrijding, het domein van VenJ. Dit wordt gevoed door maatschappelijke onrust.
Meest recente voorbeeld vormt de strijd tussen openbaar bestuur en criminaliteit in gemeenten in met name het zuiden van Nederland, zoals geschetst in de media. Samenwerkingsverbanden voor lokale en regionale criminaliteitsbestrijding (RIEC's) moeten alle zeilen bijzetten en krijgen daartoe inzage in uitgebreide databestanden.
Zowel direct als indirect; ze kunnen gebruikmaken van organisaties die data-analyse uitvoeren en van samenwerkingsverbanden die sluizen creëren tussen verschillende vormen van opsporing met data-analyse. Analoog aan deze aandacht zijn er twee dataorganisaties met de grootste verzameling van databestanden voor fraudebestrijding: het Inlichtingenbureau, dat gemeenten helpt om uitkeringsfraude te bestrijden en iCOV, dat vooral vermogenscriminaliteit helpt bestrijden. Samenwerking voor fraudebestrijding mislukt ook meer dan eens, zoals bijvoorbeeld in de zorg het afgelopen decennium. De introductie van marktwerking in de zorg heeft ook in de fraudebestrijding geleid tot het zoeken naar de juiste verhouding tussen publiek en privaat, versnippering van belangen en sub-optimalisatie.

Voor veel fraudebestrijding vormen bestanden van de Belastingdienst een voorname bron. Deze dienst zelf ontwikkelt zich in hoog tempo tot de verst gevorderde data-analist binnen de overheid. Koppeling met externe bestanden groeit. Profilering, expliciet en impliciet, is een logisch gevolg daarvan. Zo werd zeer recent bekend dat vanuit data-analyse honderd belastingadviseurs met hun 75.000 klanten in het vizier kwamen die voor meer dan 400 miljoen euro aan onterechte aftrekposten hadden geclaimd. Dit is één van de grootste successen tot nu die wordt toegeschreven aan analyse van grote databestanden die leidden tot verdenkingen van fraude.
De grootste post vormden vals gedeclareerde zorgkosten. Hier openbaart zich een mogelijke behoefte om bestanden van zorgverzekeraars en Belastingdienst te koppelen. Zo is er steeds meer denkbaar, tot de ultieme data-analyse mogelijk is; afgezien van de wenselijkheid.

13.3 BEPERKTE POLITIEKE INVLOED

De directe politieke invloed op de toename van zowel toepassing van data-analyse, koppeling van bestanden als van het bundelen van expertise is gering. Spaarzaam en globaal neemt het parlement kennis van handhaving met behulp van verdenkingen op grond van data-analyse. Stemmingen over concrete toepassingen en koppelingen waren niet traceerbaar, met uitzondering van wetgeving aangaande SyRI die unaniem instemming kreeg.
Exemplarisch voor de besluitvorming is de zaak over gebruik van parkeerdata door de Belastingdienst. Deze kwam niet in het parlement maar voor de rechter. In hoger beroep won de Belastingdienst van een privacy-organisatie.
Het tumult dat in de media hierover ontstond kreeg een zelfstandige invloed, wederom buiten het parlement om. 'Dit was voor mij persoonlijk ook over de grens', vond de directeur van de dienst en staakte dit 'programma'.
Eerst de rechter, vervolgens een persoonlijke opvatting van de dienst als grondslag voor een belangrijk besluit. Zowel het parlement als toezichthouder AP stonden hier buitenspel.
Echter, persoonlijke beoordeling van vraagstukken aangaande data-analyse en privacy in de praktijk van de fraudebestrijding speelt een grote rol. Dit treedt naar voren uit gesprekken met tientallen betrokkenen bij data-analyse in fraudebestrijding. Ze ervaren een gebrek aan houvast en proberen een evenwicht te vinden tussen vereisten van opsporing en van privacy.

Wetgeving voor fraudeopsporing wordt incidenteel en veelal onopvallend verbreed. Het treffendste voorbeeld was de uitbreiding van bevoegdheden in opsporing in het sociale domein (wijken, arbeidsmarkten, uitkeringen) met Systeem Risico-Indicatie of SyRI. De wetswijziging ten behoeve van SyRI is bekritiseerd als de introductie van de Big Brother staat.
Echter, het instrument is jarenlang toegepast zonder wettelijke dekking – wel met instemming van de AP -en dat onttrok zich aan de aandacht. SyRI werd pas als voorbeeld van flagrante inbreuk op de privacy beschouwd, nadat ze tot wet was verheven - overigens zonder politiek of maatschappelijk verzet.
Aandacht voor koppeling van bestanden en toepassing van data-analyse hangt nauw samen met geroffel op de mediatrom, vaak in de vorm van verontwaardiging.

13.4 TRANSPARANTIE EN VERANTWOORDING

Transparantie verhoudt zich volgens de fraudebestrijders slecht met de noodzakelijke slagkracht. Terughoudendheid – die bij andere partijen vaak nog groter was – is aan de ene kant begrijpelijk: de wetsovertreders die de overheid wil en moet vangen, hoeven niet gewaarschuwd te worden welke mazen in de wet en opsporing open en dicht staan.

Zeker de introductie van 'business cases', projecten waarbij de investering tenminste terugverdiend moet worden, noodzaakt tot opbrengstmaximalisatie.
iCOV, het IB en vele andere verbanden en instanties die fraude opsporen met data-analyse, beroepen zich op zowel hun snelheid en efficiency van werken als op hun zorg voor de omgang met bestanden. Hoe dat in de praktijk uitpakt, is echter veelal onbekend.
Transparantie over procedures en gebruikte bestanden neemt incidenteel toe, niet vanwege politieke druk maar vanuit een besluit van betrokken ambtenaren. Bijvoorbeeld met de website met ruime informatie van het Inlichtingenbureau.

Van iCOV is daarentegen weinig openbaar, teneinde de grote wetsovertreders die het doelwit vormen, niet wakker te schudden. Elke openbare aandacht kan het werk in de wielen rijden. Gebrekkige transparantie is deels veroorzaakt door een wettelijk vacuüm.
Zo is er voor SyRI wel een uitdrukkelijke wettelijke ondergrond maar veel andere data-uitwisseling wordt gedekt door convenanten dan wel eenmalige publicaties in De Staatscourant, die nimmer een parlementaire toets doorliepen.
Zo zijn de jaarverslagen van het IB niet openbaar, iCOV kent het fenomeen verslaglegging en openbare verantwoording in het geheel niet. De Interventieteams (SyRI-toepassing) rapporteren wel helder, maar geen details over toegepaste data-analyse.
Van veel organisaties die fraude bestrijden met data is niet duidelijk hoe ze precies te werk gaan en wat de uitkomsten zijn. Terugkoppeling met beleid is niet of nauwelijks zichtbaar. Openbaarheid is gering.
Zo werd van het genoemde gebruik van vastlegging van kentekens bij parkeergarages noch de aanvang van het vastleggen noch het stopzetten aan de belastingplichtige autobezitters meegedeeld.
Zelfs met de meest in de publiciteit geraakte Big Data-zaak voor misdaadbestrijding, de 'Bewaarplicht' van telecom- en internetdata, namen de Europese Commissie, de wetgever in Den Haag en uiteindelijk ook de rechter besluiten voor het invoeren en opheffen. Zonder enig zicht op het werkelijke resultaat; op de baten van het vergaren en inzetten van grote databestanden noch op de werkelijke privacyschendingen die hiervan het gevolg waren of konden zijn.

13.5 PRIVACYBOTSING

Fraudebestrijders en hun chefs banen zich op de tast een weg tussen de snel groeiende mogelijkheden van analyse en profilering en de als streng ervaren privacyregels.
Vooral de doelbinding en in minder mate proportionaliteit worden wellicht in de praktijk met voeten getreden: er bestaat gerede twijfel of de steeds bredere inzet van bestanden zich verhoudt tot de privacyvereiste dat data louter gebruikt worden voor het doel waartoe ze zijn verzameld.

Is bovendien het bundelen van tientallen databestanden in nieuwe domeinen, zoals van iCOV, nog proportioneel? De bestanden worden letterlijk overgedragen naar andere systemen voor data-analyse. Het risico op ongewenste praktijkgevallen neemt toe. Het 'shoppen' in data door individuele beambten wordt als een groeiend risico gezien. Een voorbeeld: bij sommige samenwerkingsverbanden moet een opdracht voor data-analyse van de kant van de politie juridisch gedekt zijn, maar van een belastingambtenaar niet. In een samenwerking ligt het dan voor de hand wie de data-analyse aanvraagt.

Fraudebestrijders toonden allen hun goede bedoelingen. Privacyregels vormen hun belangrijkste grenzen. Niet dat ze die moedwillig aan hun laars lappen, maar ze achten logischerwijs vanuit hun taakopvatting de privacyregels een belemmering.

Eigen privacyofficers bepalen grenzen, die niet transparant zijn. Voor hoelang geldt bijvoorbeeld het getraceerde risico c.q. de verdenking vanuit de data-analyse? Welke persoonsgegevens worden voor welke periode verzameld, gebundeld en blijven beschikbaar voor onderzoek? Dat weten de instanties zelf niet.

'Eens een dief, altijd een dief' is een spreekwoord dat van toepassing was en is. Dit strekt zich niet alleen uit in tijd, maar ook over grenzen van domeinen. Daarvoor raakt het begrip 'beroepsfraudeur' in zwang: de fraudeur op het ene terrein is vaak ook een wetsovertreder op een ander terrein.

Ook zijn er grote verschillen in het hanteren van privacyregels. Zo heeft de VNG voor gemeenten een uitgebreid protocol opgesteld voor het speuren op het open internet. Maar het online speuren door andere instanties, zoals de Belastingdienst dat zeer intensief doet, valt niet onder bekende regels of toetsing.

Ook voor de Autoriteit Persoonsgegevens (AP) lijkt het dweilen met de kraan open. Bij wetsvoorstellen toont de AP een uitgesproken en voor iedereen zichtbare invloed met advisering. Die vindt meer dan eens steun in de advisering van de Raad van State.

Echter, een aantal gesproken woordvoerders voor deze casestudie had contact met de privacywaakhond en vernam min of meer informeel over de toelaatbaarheid van de methoden in relatie tot privacyregels. De AP geeft dan de kaders aan. Officieel advies is dit echter niet, en ook zijn de deelnemers aan de dialogen noch de vragen en uitkomsten transparant. Vragen die we stelden over overleg met de AP dat had plaatsgevonden volgens vrijwel alle woordvoerders in deze studie, kregen dus geen concreet antwoord.

Ook velt de AP geen ad-hoc oordelen over privacygrenzen. Zoals de AP liet weten op vragen op een verzoek om commentaar op een zeer uitgebreid overzicht van

alle uitwisseling van informatie c.q. bestanden tussen verschillende overheden en zelfstandige bestuursorganen waarvan sprake is in paragraaf 12.9:[264]
'Als toezichthouder doen wij gericht onderzoek naar ernstige overtredingen die structureel van aard zijn, die veel mensen treffen en waarbij de AP door de inzet van handhavingsinstrumenten effectief verschil kan maken. Over welke informatie we precies hebben en waar we wel of geen onderzoek naar doen, kunnen we in verband met de zorgvuldigheid geen uitspraken doen. Zonder onderzoek gedaan te hebben, kunnen we ook geen uitspraken doen over wat er volgens de wet wel en niet mag.'[265]
Het behoort niet tot de taken van de toezichthouder op de privacy of zich met deze essentiële zaken bezig te houden, zonder dat er een besluit is voor onderzoek van bijvoorbeeld een concrete klacht, of verzoek om advies voor een wetsvoorstel is. Daar ontbreken ook tijd en capaciteit voor, aldus de AP.
Op grond van tips en aandacht voor incidenten verricht de AP soms nader onderzoek naar datagebruik. Ook voor nieuwe wetgeving wordt de AP uitgebreid geraadpleegd. Kritiek en suggesties worden serieus genomen, ofschoon die soms stuiten op de gewenste praktische uitvoerbaarheid van fraudebestrijding.
Er is echter geen structurele aandacht op de vele bestandskoppelingen van de toezichthouder. Die evenmin etaleert dat de deskundigheid c.q. capaciteit in gelijke mate groeit met de mogelijkheden voor toepassing van grote hoeveelheden data. Ondertussen neemt de toepassing van Big Data in de praktijk nieuwe horden. Zo publiceerde het FD op 9 mei jl. over grootschalig Big Data-onderzoek in het gebied Rotterdam-Zuid.[266] Onder leiding van het OM bundelden overheden, banken, (zorg)verzekeraars en andere private ondernemingen hun data voort risicoanalyse. Grootschalige fraudepatronen kwamen aan het licht.
De datareeksen waren al geanonimiseerd maar zijn ook na het onderzoek direct vernietigd vanwege privacyregels. Ook leverde de Belastingdienst geen data. Het OM kan dus resultaten uit het onderzoek concreet niet gebruiken voor misdaadbestrijding. Dus wil het OM ruimere mogelijkheden voor toepassing van Big Data-risicoanalyse.

13.6 KADERWET VOOR MINDER GRENZEN

De bedoeling is dat er met de komst van een Kaderwet Gegevensuitwisseling, waarvoor de minister in december 2014 een verkenning naar de Kamer stuurde, helderheid wordt gebracht waar partijen die speuren naar fraude behoefte aan heb-

264 Bijlage bij Kamerbrief over gekoppelde databestanden van Minister van der Steur: Inventarisatie gegevensbestanden en koppelingen
http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2015/03/25/tk-inventarisatie-gegevensbestanden-en-koppelingen.html
265 Woordvoerster AP, Merel Eilander.
266 http://fd.nl/economie-politiek/1150701/big-data-legt-onzichtbare-criminaliteit-bloot

ben. En of daar een data-autoriteit bij hoort die de afwegingen van baten en lasten breder maakt dan louter op grond van privacyregels.
Maatschappelijk zou een toetsing van de Kaderwet de politieke controle van data-analyse door overheden kunnen vergroten. Nu wordt er wel regelmatig over fraudebestrijding gerapporteerd aan de Kamer, maar een helder, transparant beeld over lasten en baten van verschillende methoden waaronder het groeiend gebruik van databestanden, levert dit niet op. De aandacht is navenant.
Wel treffen de partijen die bestanden en data uitwisselen elkaar op het hoogste niveau. Zo fungeert al sedert 2003 een Manifestgroep met directeuren van het UWV, de Belastingdienst, CAK, CBS, CIZ, CJIB, Zorginstituut Nederland, Dienst Justis, RVO.nl, DUO, de IND, Kadaster, KvK, de RDW, de SVB, CBR, BKWI en RSJ om onderlinge data-uitwisseling te bespreken. Toepassing van verdergaande analyse van bestanden, ook als Big Data bestempeld, is onderwerp van gesprek.
Net als in vrijwel alle tientallen samenwerkingen die zijn opgetuigd en met dwarsverbanden ook onderling data kunnen delen. Daarbij rijst de vraag of bestanden juist centraal gebundeld moeten worden, teneinde de effectiviteit van fraudebestrijding te vergroten. Maatschappelijk verzet tegen een 'datamoloch' van de overheid kan het gevolg zijn, maar de vraag is of de trein naar bundeling nog te stoppen is gezien de snel uitdijende samenwerking.
En in hoeverre dit kan doorgaan zonder wettelijke en maatschappelijk gevoelde privacygrenzen te tarten? Met overigens steeds weer de vaststelling in dit onderzoek dat het noodzakelijke evenwicht tussen fraudebestrijding en privacybescherming moeilijk generiek vast te stellen is. Immers, de verantwoording van de baten en lasten van de grootschalige data-analyse, de zogeheten 'accountability' ontbreekt.
Instanties die bijdroegen aan dit onderzoek, wensen uiteraard veelal graag een verruiming van mogelijkheden om data in te zetten voor speurwerk. Echter, een aantal van de geïnterviewden bepleit ook striktere regulering voor verantwoording. Ze zouden meer houvast willen hebben, want ze tasten nu vaak in het duister over hun grenzen.
De huidige versnippering met houtjetouwtje-overeenkomsten of 'convenanten' blijkt in de praktijk tot een niet meer te overzien woud van data-analyse voor fraudebestrijding te hebben geleid.

Fraudebestrijding met patroonherkenning vanuit data vereist een brede toepassing volgens fraudebestrijders. Velen willen daarin ook de stap zetten richting profilering van (rechts)personen. De vraag is in hoeverre deze profilering tot voorspellende en daarmee ook stigmatiserende normen en waarden zal leiden.
Bijvoorbeeld voor bestrijding van fraude met WWB-uitkeringen wordt het stoplichtmodel gehanteerd: rood, oranje en groen voor hoog, gemiddeld en laag risico op fraude. De Belastingdienst werkt met een 'green lane': degenen met een laag risicoprofiel voor belastingontduiking worden met rust gelaten bij controles. Dit

beschouwt de Belastingdienst als een gunst voor degenen die bereidwillig data laten analyseren en 'niets te verbergen' hebben.
De komende jaren kunnen bepalend worden hoe de samenleving in de hierna volgende decennia de voordelen van datagebruik plukt zonder daarvan blijvende schade en nadelen te gaan ondervinden.
De oplossingen waarnaar gedachten uitgaan lopen uiteen van technologie voor anonimisering en pseudonimisering gedurende processen – zoals met SyRI wordt gedaan. Tot en met volledig eigen beheer van data door burgers die dan mede zelf bepalen wie er over mag beschikken, voor welke periode en welk doel, zoals in de zorg wordt geopperd.
Ook de technologie Blockchain biedt wellicht mogelijkheden voor dataverzameling en uitwisseling met behoud van meer privacy, maar wordt gebracht als Haarlemmerolie voor veel digitale vraagstukken.

Het is echter zeer de vraag of technische oplossingen afdoende zullen zijn om principiële vraagstukken op te lossen, zonder diepgaande politieke afwegingen aangaande het evenwicht tussen fraudebestrijding en privacybescherming.
Door de recente terroristische aanslagen is er meer aandacht voor het fundamentele vraagstuk: in hoeverre zijn veiligheidsmaatregelen die de vrijheid beperken, zoals dataverzameling, gewenst ter vergroting van – al dan niet vermeende – veiligheid en vermindering van fraude?
We beschouwen jaarlijks een kleine 600 doden en ruim 20.000 zwaar gewonden als een aanvaardbare maatschappelijk tol voor vrije doorstroming van verkeer. Zo zal de samenleving ook een afweging moeten en kunnen maken van de voor- en nadelen van uitbreiding van data-analyse en profilering van burgers ten behoeve van het opsporen van wetsovertreders en ter voorkoming van criminaliteit en misbruik van voorzieningen.
Bovendien is een historische benadering mogelijk: privacy is een typisch 20e-eeuws product, waarvan de opkomst samenviel met onder meer verregaande verstedelijking en individualisering. Het belang dat individuen aan privacy hechten, lijkt aanzienlijk verminderd met het intensieve gebruik van onlineplatforms die – onterecht? – 'sociale media' worden genoemd. Zowel de expliciete als impliciete – betaling voor 'gratis' diensten – bereidheid om persoonlijke data af te staan in ruil voor voordelen lijkt aanzienlijk toegenomen te zijn.
Zo aanschouwen we eveneens in de 21e eeuw een snelle toename van het etaleren van medische kwalen, onder meer in vele televisieprogramma's. Dit werpt de vraag op: in hoeverre zijn mensen bereid om hun medische privacy op te offeren in ruil voor aandacht in grotere kring, zelfs openbaar, maar ook voor medisch onderzoek? En op beperkte schaal voor fraudebestrijding om de – ook eigen – medische kosten te beperken?
En willen we belastingaangiften transparant maken, zoals een bekende Nederlander deed in de media? En daarmee fraude en ontwijking met 'sociale inbreng' van burgers en data-analyse beter bestrijden? Het maatschappelijk denken over privacy

is aan verandering onderhevig en wat betreft Big Data nog lang niet uitgekristalliseerd.
Juist nu is dringend meer aandacht nodig voor met name de verwerking van data en combineren van bestanden en plegen van nieuwe vormen van (big) data-analyse, waar nu in wetgeving en handhaving voor privacy de nadruk nog vooral ligt op de verzameling ervan.
De politieke afwegingen aangaande het evenwicht tussen fraudebestrijding en privacybescherming zijn louter mogelijk met een reële berichtgeving van feiten aangaande datagebruik in de media. Niet aan de hand van incidenten en roeptoeters komen de beste maatregelen voor toepassing van data-analyse tot stand, maar vanuit geobjectiveerde afwegingen tussen potentiële vóór- en nadelen.

BIJLAGE 1 21 INTERVENTIETEAMPROJECTEN WAARVOOR MET BEHULP VAN DE TECHNIEK VAN SYRI BESTANDEN ZIJN GEKOPPELD EN VERVOLGENS EEN RISICOANALYSE IS GEMAAKT

Project	Onderwerp	Periode van controles
Kadastercheck	Detectie van verzwegen vermogen	Maart 2008-December 2009
Middengebied, Vlissingen	Wijkgerichte aanpak	Februari 2010-December 2010
Kanaleneiland, Utrecht	Wijkgerichte aanpak	Maart 2010-december 2011
De Vergt Zaltbommel	Wijkgerichte aanpak	Maart 2010-oktober 2010
Merwestein, Nieuwegein	Wijkgerichte aanpak	Augustus 2010-maart 2011
Donderberg, Roermond	Wijkgerichte aanpak	September 2010-juli 2012
Vrieheide/De Stack/Passart/Maria Gewanden, Heerlen	Wijkgerichte aanpak	Maart 2011-september 2012
Hambaken/Barten, 's Hertogenbosch	Wijkgerichte aanpak	Maart 2011-maart 2012
Terweijde/Achter de Poort /Nieuwstadt, Culemborg	Wijkgerichte aanpak	April 2011-december 2013
De Riet, Almelo	Wijkgerichte aanpak	Mei 2011-december 2011
Baarle-Nassau	Recreatiepark	September 2011-februari 2012
Soesterkwartier/Isselt, Amersfoort	Wijkgerichte aanpak	Oktober 2011-mei 2012
Stokhasselt/Vlashof, Tilburg	Wijkgerichte aanpak	Januari 2012-oktober 2012
Westwijk, Vlaardingen	Wijkgerichte aanpak	Januari 2012-juli 2012
Vlissingen-noord	Wijkgerichte aanpak	Mei 2012-maart 2013
Latus Spectare, Utrecht	Wijkgerichte aanpak	Mei 2012-juli 2013
Kern Vaals	Wijkgerichte aanpak	November 2012-mei 2014
Tongelre, Eindhoven	Wijkgerichte aanpak	Januari 2013- februari 2014
Schiedam-oost	Wijkgerichte aanpak	Januari 2013-oktober 2013
Meerzicht, Zoetermeer	Wijkgerichte aanpak	Maart 2013-april 2014
Dauwendaele, Middelburg	Wijkgerichte aanpak	Mei 2013-juni 2014

BIJLAGE 2 FINANCIËLE RESULTATEN UIT 21 INTERVENTIETEAMPROJECTEN WAARVOOR MET BEHULP VAN DE VOORLOPER VAN 'SYRI' BESTANDEN ZIJN GEKOPPELD EN VERVOLGENS EEN RISICOANALYSE IS GEMAAKT

Project	Bedrag belasting-aanslagen + boetes	Correcties op toeslagen	Uitkeringsfraude: Terugvorderingen en beëindigde uitkeringen + boetes (gemeenten, UWV en SVB)	Geconstateerde gevallen van overtreding Wav en Wml
Kadastercheck	3.521	2.356	820.144	N.v.t.
Middengebied, Vlissingen	1.921.696	522.570	40.830	308.000
Kanaleneiland, Utrecht	1.310.793	3.591	724.818	68.000
De Vergt Zaltbommel	765.914	---	142.297	16.000
Merwestein Nieuwegein	145.213	---	150.958	Geen financiële resultaten
Donderberg, Roermond	876.366	59.529	22.061	4.000
Vrieheide/De Stack/Passart/ Maria Gewanden, Heerlen	180.096	n.b.	5.802	Geen financiële resultaten
Hambaken/ Barten, Den Bosch	611.364	23.294	191.811	Geen financiële resultaten
Terweijde/Achter de Poort/ Nieuwstadt Culemborg	420.842	Geen financiële resultaten	459.467	84.000
De Riet, Almelo	Geen financiële resultaten	Geen financiële resultaten	Geen financiële resultaten	Geen financiële resultaten
Baarle-Nassau	81.727	Geen financiële resultaten	46.060	n.v.t.
Soesterkwartier/ Isselt Amersfoort	1.321.834	52.292	503.226	92.000
Stokhasselt/ Vlashof, Tilburg	1.322.702	3.176	110.878	8.000
Westwijk, Vlaardingen	5.694	61.800	18.242	24.000
Vlissingen-noord	479.916	70.558	31.149	580.000
Latus Spectare, Utrecht	489.927	1.603.567	555.384	361.125
Kern Vaals	236.567	81.676	155.676	Geen financiële resultaten
Tongelre, Eindhoven	1.918.042	2.950	533.746	Geen financiële resultaten
Schiedam-oost	95.487	604.000	98.103	Geen financiële resultaten
Meerzicht, Zoetermeer	313.336	46.376	132.497	Geen financiële resultaten
Dauwendaele, Middelburg	24.051	79.279	46.475	Geen financiële resultaten
Totaal	12.344.992	3.397.110	4.789.624	1.545.125