

WRR

WETenschappelijk Raad voor het Regeringsbeleid

Peter Olsthoorn

Big Data voor Fraude- bestrijding

working paper 21

1894015

00451

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 vindt u op www.wrr.nl.

Wetenschappelijke Raad voor het Regeringsbeleid
Buitenhof 34
Postbus 20004
2500 ca Den Haag
Telefoon 070-356 48 00
E-mail info@wrr.nl
Website www.wrr.nl

Big Data voor Fraudebestrijding

Peter O'lsthoorn

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

Vormgeving binnenwerk: Textotera, Den Haag
Omslagafbedding: Textotera, Den Haag

Working Paper nummer 21

ISBN 978-94-90188-20-2

wrr, Den Haag 2015

Alle rechten voorbehouden. Niets uit deze uitgave mag worden vervaardigd, opgeslagen in een geautomatiseerd gegevensbestand, of openbaar gemaakt, in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of enige andere manier, zonder voorafgaandeschriftelijke toestemming van de uitgever.

Voor zover het maken van kopieën uit deze uitgave is toegestaan op grond van artikel 17B Auteurswet 1912 (het Besluit van 20 juni 1974, S. 6), 35f. (zoals gewijzigd bij het Besluit van 23 augustus 1985, S. 6), 47 en artikel 17 Auteurswet 1912, dient men de daarvoor wettelijk vastgestelde vergoedingen te voldoen aan de Stichting Reprorecht (Postbus 30 51, 2130 kb Hoofddorp). Voor het overnemen van gedeeltes (in bloemlezingen, readers en andere compilatiewerken) (artikel 17 Auteurswet 1912) dient men zich tot de uitgever te wenden.

inhoud

Ten geleide	9	
1	Inleiding	11
1.1	Wetsovertreder of brave burger	11
1.2	Politiekewens en controle	12
2	Omvang van defraude en beleid	19
	Inleiding	19
2.1	Deruwelbedragen	20
2.2	Minimale Geww-minimale 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	Overregulatie en uitdagingen	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	95
6	Syrië en Irak	99
	Inleiding	99
6.1	Wettelijke basis	99
6.2	Uitvoering Syrië	102

6.3	Toepassing in de praktijk	105
6.4	Privacy	108
7	Inspectie szw	111
	Inleiding	111
7.1	Beleiden 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 voorname	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	Privacywetgeving	149
10.6	Toekomst	152
11	bzk	159
	Inleiding	159
111	Doelen en uitgangspunten	161
112	Risicogestuurd onderzoek naar adresfraude	160
113	Landelijke aanpak adresfraude met risico-analyse	162
114	Toekomst: vervolglaan	167
115	Project Aanpak Fraude bij lotu	168
116	Basisregistraties: Heel veel data	170

117	Relatie Big Data en frauderegistratie	172
118	Privacykwasties	174
12	Veiligheid en justitie, en iCoV	177
	Inleiding	177
12.1	iCoV: doe 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	185
12.7	Toekomstige opties met Big Data	191
12.8	Risicomeldingen in strafrechtelijke dossiers	193
12.9	Slot: naar een nieuw wet	195
13	Conclusie	201
	Inleiding	201
13.1	Politiekewens	202
13.2	Zover mogelijk data	203
13.3	Bepaalde politieke invloed	204
13.4	Transparantie en verantwoording	204
13.5	Privacybehoefte	205
13.6	Kaderwet voor minder grenzen	207
Bijlage 1	Interventieteam projecten waarvoor met behulp van de techniek van Syr i bestanden zijn gekoppeld en vervolgens een risicoanalyse is gemaakt	211
Bijlage 2	Financiële resultaten uit 21 interventieteamprojecten waarvoor met behulp van de voorloper van 'Syr i' bestanden zijn gekoppeld en vervolgens een risicoanalyse is gemaakt	213

ten geliede

WIR WorkingPaper 21 is geschreven als achtergrondstudie voor het project 'Big Data, privacy en veiligheid'. In dit project verkent de WIR de implicaties van het gebruik van Big Data binnen het veiligheidsdomein. Deze achtergrondstudie *Big Data en fraudebestrijding* is uitgevoerd door onderzoeksjurist Peter Olschoorn. Hij beschrijft in deze studie wat zich in Nederland afspeelt op het terrein van dataverzameling, bestandsopstelling en gegevensanalyse om fraude te voorkomen en/of te detecteren. De studie omvat verschillende overheidsdomeinen als gemeentelijke uitkeringen, sociale verzekeringen, belastingen en toelagen, en criminaliteitsbestrijding. De in deze studie beschreven vormen van dataanalyse zijn nuttig maar het is wettelijk en de publieke en maatschappelijke wens om door bestandsopstelling 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 WIR tot stand zijn gekomen. De verantwoordelijkheid voor de inhoud berust bij de auteur.

Prof. dr. J.A. Knottnarus
Voorzitter WIR

Dr. F.W. A. Brom
Directeur WIR

1

iCov? Het Inlichtingenbureau? De meeste Nederlanders, en wellicht ook de meeste parlementarissen 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 spionage dienst National Security Agency (nsa) blijkt op grote schaal 'data' te verzamelen uit communicatie via de telefoon en internet met Google en Facebook.

'Ongevevenaard', 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.

Tervrij aan de ophof over de Snowden-affaire geen eind te komen, werd over onze 'eigen' Big Data-toepassingen nauwelijks iets bericht. Deze toepassingen zijn voor de Nederlandse samenleving – uit op Nederland – 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 i

Selecteer uit het bestand van het Justitieel Inzasssbureau (jib) personen met jaarlijks meer dan drie boetes wegens rijden door rood licht. Is het terechtvaardigen om specifiek van hen de belastingaangifteextra te controleren?

Hoeveel jaar jib-data mag je daarvoor gebruiken? Welke ander data zijn daarbij nog meer nuttig, welke bestanden kun je gecombineerd inzetten?

Of doktor nr. 10 met analyse van data al dan niet 'big' kun je van elke Nederlander een gedetailleerd fraudeprofiel opstellen? Van gezinnen, van families?

(13 maar geografin: fraudeprofielen van wijken, straten en van postcodes?)

Brabantse lijken met een pak kans op hennep teelt die vijftien keer zo groot is als in een gemiddeld dorp, zouden zo geïdentificeerd kunnen worden. Net zo goed overigens als bepaalde wijken in Wassenar, Blaricum en Amsterdam-Zuid zo het stampel brandhaarden van belastingontwijking of zelfs witte boorden criminaliteit opgedrukt zouden kunnen krijgen.

Dit alles is geen sciencefiction. De Belastingdienst blijkt daadwerkelijk de intentie te hebben om een dehand van data op nism 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 (Venz) (wiltwassen, 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 daarom 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 wensen en contr

De snelle toename van informatiebundeling ten behoeve van fraudebestrijding komt voort uit een uitdrukkelijke politieke en maatschappelijke wens; misbruik van voorzieningen moet prioriteit krijgen.

Het parlement verwoordde deze eis, aangevuld met bestuurlijke continuïteit begrip, als de noodzaak tot 'integratie in pan ningen' en 'het' heger gaan van versnippering'. De ambtelijke vertaling van deze politieke eels was fraudebestrijding vooral doorkrachtenbundeling; met onder meer tot het rijtje een bundeling van bestanden om daarin door analyse fraudepatronen en -risico's tekunnen 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 dat gebruik 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 kwestie, die ongevraagd is: de in de nood 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 bereikt we tussen noodzakelijke bestrijding van groeieender criminaliteit en het onzien van 'onschuldige burgers'. Ook in deze discussie open gevoelens, al dan niet onder invloed van lobbyisten en door 'framing', gemiddeld zijn op in (sociale) media tussen personen die bij het woord 'bestandskoppeling' alleen al de hooftok luiden over privacydending en personen die termen 'vertoedeling' en 'criminalisering' in de mond hebben en hebben liggen.

Voor beantwoording van deze kernvraag moet de onderliggende casestudy fraudebestrijding handvatten bieden. De bevindingen zijn verval in een grote hoeveelheid facten over toepassing van data analyse in fraudebestrijding.

De vragen die speelden voor dit onderzoek waren onder meer:

- Welke dataverzamelingen -analysesetien overheden en zelfstandig organen in om fraude te voorkomen en/of te detecteren?
- Wat speelt zich op dit terrein van dataverzameling, het combineren van bestanden en gezamenlijk analyseren 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 weerbaarheid van bij de opzet van systemen;
- de uitvoering van data analyse van grote bestanden en systemen;
- resultaten van data uitvoering;
- hinderbaarheid bij datatoepassingen en vraagstukken omtrent grenzen en rechten op privacy;
- toekomstige wensen en verwachtingen.

Op onderdelen spelen verder de volgende vragen:

- Vanuit welke interne en externe oep en bestaende bestanden en door worden de data verzameld?
- Hoe functioneren organisaties en systemen in data analyse?
- Waar liggen de grenzen voor gebruik van persoonsgegevens op nationaal niveau, zijn die dan niet onvoldoende personen te herkennen?
- Welke controle vindt er plaats op de toepassing van de systemen?
- Is er uiteindelijk ook politiek inzicht in en controle op het gebruik van data en de eventuele effecten?
- Welke expertise en ondersteuning zijn voorhanden voor controle op uitvoering?
- Hoe verhoudt de data toepassing zich tot de privacywetgeving en de Autoriteit Persoonsgegevens (ap) of van?
- Of samen vatend, hoe komen keuzes tot stand en hoe werkt de data vervolgens en waar willen organisaties heen?

De afles concentrert zich rond de kernvraag van dit onderzoek: waar ligt de balans tussen de verwachte adequate bestrijding van fraude met data analyse en een voldoende 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 het huidige raam 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, bestellingen, uitkeringen/ toelagen en arbeidsmarkt.

Een eerste probleem dreigde op te treden bij de te gebruiken terminologie, te beginnen met de term 'Big Data's. Dit wordt gehanteerd door grote volumes data, veelal ongestructureerd, die met een hogesnelheid en betrouwbare verwerking leiden tot nieuwe inzichten die beslissingen ondersteunen.

In het zakelijk domein wordt al de term *Business Intelligence* als *Business Analytics*, of twee analyses gericht op toekomstig profijt uit voorspellingen. In fraudebestrijding betekent 'Big Data' vooral het voorspellen van kwade objecten en objecten naar verwachting het vaakst tot fraude leiden. Dit kan samengaan met profilering van situaties en personen.

Deze nauwe definitie is uiteindelijk van laten voor dit onderzoek. Ten eerste gaat Big Data uit van een compleet nieuw wereld. Ten tweede speelt data-analyse al jaren een groter 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 (geen garantie voor de toekomst) inhouden.

Betrokkenen spraken ook wel over *littledata*; daar meeweten ze behalve op een beperkte omvang, ook op zaken op persoonlijke data, veelal met een min of meer concrete verduidelijking.

Dit impliceert direct ook een van dit onderzoek: waar de term 'Big Data's 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.

Zelf zijn dus voorstander van het toepassen van Big Data, van grote hoeveelheden gegevens, maar daarbij vooral gericht op het behouden naar een of die frauderisico's en naar paknamen van fraudeurs en uiteindelijk het duiden op naam, opdat verdachten in de reageverval kunnen worden.

De huidige werkwijze van fraudebestrijders bestaat vaak uit het combineren van (Big) Data bestanden en 'littledata' voor het oplossen van concrete zaken. Het uiteindelijk doel van de huidige data-exercities is niet louter het ontharen van generieke patronen die tot fraude leiden – dat is een tussenstap – maar ook van patronen van fraude ontkenners of van zogenaamde *reddivisions*, oftewel 'beroepsfraudeurs'.

Hij nept patronen tussen subjecten, organisaties en personen op naam. Van belang is daarbij wel in hoeverre patronen voorspelende waarde hebben, en verder of ze tot profilering of zelfs stigmatisering leiden. Door de weerstand die dit oproept, neemt gedurende dit onderzoek de vraag of het mogelijk en goed is om deze ongewenste effecten compleet te verkleinen of uit te bannen.

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

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

De volgende betekenis en zijn:

- Datamining is zoeken naar opvallende zaken en verbanden in (grote) bestanden.
- Data-analyse is het analyseren van de bestanden als zodanig.
- Risicoanalyse is het onderzoeken en vaststellen welke risico's er zijn in het uitvoeringsproces (handmatig en geautomatiseerd) of in klant- en uitkeringsmarkten.
- Risicoprofielen zijn risicovolle kenmerken of verzamelingen klant-kenmerken die uiteindelijk leiden tot het uitsluiten (profielen) van groepen personen met deze kenmerken of zelfs individuele klanten.
- Bestandsvergelijking: vergelijken van data uit het ene bestand met data uit 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 gemeenschappelijke taal van verschillende handelingen met data die keuzes ondersteunen, in dit geval de voorkoming van fraude en de opsporing daarvan.

Waarvoor de opsporing zelf over zowel 'informatiegestuurd handhaven' (lijgt) als 'analysegestuurd handhaven' en bedrukt en daar hetzelfde met fraudebestrijding en voorkomen, met behulp van 'risicoprofielen' of indicatoren, of dat in de huidige taalgebruik ook wel genoemd wordt: verdenkingen scoren. En dat met behulp van data-gebruik.

Een derde keuze, en niet het geringste, betreft de structuur van dit onderzoek. In de onderzoeksjournalistiek die ik dagelijks bedrijf, zijn selecties en waargenomen duren medegericht op het boeien van lezers. Dat is onmogelijk met behoud van alle nuances.

Daarom door de bronnen in dit onderzoek niet gewaardeerd, uitgeraaid terzichte. Vaak gaat het juist bij dataverzameling en -gebruik voor fraudebestrijding door overheden om zeer bevoorrechte nuances en details.

Dit heeft mede geleid tot een veel grotere omvang van het onderzoek dan aanvankelijk was bedoeld. Die keuze is gemaakt voor een uitputtende weergave in een logische samenhang niet voor een journalistiek eselutie.

Nadere inleiding volgt in hoofdstuk 2 een uiteenzetting over de geschiedscomvang van het fraudeprobleem. Hoofdstuk 3 heeft het onjuist dedaren 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 demaest gav uide partij, in samenwerkingen vanwege zijn hoeveelheid relevante data.

Deze gaan onder meer naar het Inlichtingenbureau (ib), besproken in hoofdstuk 5, dat vele initialen beslaan dank u koppelen en analyse en, en aan omvredesignalen 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 wetsvrijzingen geëigtmardesysteem 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 u w v, dat verregaande plannen en werken met data-analyse openbaar (hoofdstuk 8), gevolgd door 'zuster' Sociale Verzekeringsbank (svb), die zich na de nodige tegenslag bochelden opstelt (hoofdstuk 9).

Niet als het u w v en de svb pogen gemeenten misbruik van voorzieningen krachtiger aan te pakken met inzet van data, na aanvankelijke mislukkingen (hoofdstuk 10). Zauw en samen met het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (bz), besproken in hoofdstuk 11, aan betredesbestanden waar mee veel fraude en data-analyse samenhangen.

Tot slot komt in hoofdstuk 12 het ministerie van Veiligheid en Justitie aan bod (Vnu), met het samenwerkingsverband dat grote hoeveelheden data voor werkt voor de opsporing van vooral financiële fraude. De aemstudy eindigt met conclusies en de beoogde Kaderwet Gegevensuitwisseling, waar veel instanties die fraude bestrijden, hun hoop op gevestigd hebben voor ruimer bevoegdheden.

Dan rest me nu dank te zeggen aan de voortreffelijke woordvoerders van de organisatie die aan dit onderzoek hun bereidwillige medewerking verleenden, vaak met aanzienlijke inspanningen en uiteindelijk ook de nodige flexibiliteit om zich te plooiën naar de onderzoeksoopdracht.

Transparantie aan fraudebestrijding zijn immers geen natuurlijke eisen en geboden. De woordvoerders hadden niet slechts aan een hogelw diltet van informatie over hun werk te rein diet een nog nader diepgaand overzicht van de fraudebestrijding heeft geleid. Bovendien konden ze een kritische instelling en verslaglegging waarderen en besloten ook hun onzekerheden te delen, zoals de spanningevelden 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 opbehoed voor het vallen in de nodige valkuilen.

Pieter Oltshoorn

2

inleiding

Fraude is bedrog. Dat is de kortste definitie. Van de opgesomde definities op Enqdy.nl is deze verreweg het helderste: "Het misleiden, bedriegen of schenden van vertrouwen met als doel een oneerlijk of onrechtvaardig voordeel of materiële winst te verkrijgen." Hoe omvangrijk is het fraudeprobleem in Nederland?

En hoels dat verdeeld over de verschillende beleidsdomeinen? 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, zelfs landelijke organen en samenwerkingsverbanden niet van dezelfde cijfers uitgaan. Ook ontbreekt historisch inzicht.

Soms wordt daarvan gebruik gemaakt in de lobby vanuit opsporingsinstellingen: er draaieft altijd wel ergens een hoog bedrag dat een eigen leven kan gaan leiden. Aan de ene kant is die onwetendheid – gevolg van niet-opgespoorde misdaad is de omvang onbekend. Fraude is veelal administratief, en daardoor niet zo zichtbaar.

Maar ten minste zou de overheid een opsporingkinnen maken van jaarlijks vastgestelde fraude. Ook dat sluit echter op problemen: onbekende regelmatig heden duiden niet altijd op opzet. Vooral in de zorg (hoofdstuk 3) is er een enorm verschil in omvang van vastgesteld en juist dedarom on fraude.

Deze voorzichtigheid omgedrag als 'frauduleus' te bevestigen betreft vooral artsen. Bij uitkeringgeachtigen heeft deze voorzichtigheid jarenlang ontbroken. Daar zijn teveel geleide bedragen wel standaard als 'frauduleus' gecorrekert.

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. Hier 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 hooggedachte fraude rechtvaardigt – en noodzaakt tot – daadkracht. Er kwam een ministerieel commissie-Aanpak Fraude, waarvan nauwelijks iets is vernomen.

Ondertussen 'vrandworit' de overheid in hoog tempo, tot in de afgewenste intensievere samenwerking in fraudebestrijding tot stand te brengen. En om de veelvuldig gewaste vermindering van versnippering van inspanningen – een man-traven het parlement – in praktijk te brengen.

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, 65 procent van de in totaal 30 miljard euro geschatte fraude in Nederland.

Dit fraaieronde bedrag is echter een ruweschatting van een adviesbureau, dat publiek dit getoonde met een natuvingeronderzoek: uitkrijngs/fraude per jaar 3 miljard euro en belastingfraude 10 miljard euro (maar wellicht 23 miljard euro).⁵

Hoedan ook: het bedrag aan uitkrijngs/fraude van 135 miljoen (obs-dijfers) of 3 miljard euro, waarvan de ordeheft met Wet Werk en Bijstand (wwb)-uitkeringen, vormt minder dan 10 procent van de totale bedragen die met fraude gemoeid zijn. Of schoon bijstandsfraude een relatief gering deel uitmaakt van de totale fraude, is de aandacht hiervoor het grootst.

Zoligt het zwartepunt in de eerste resultaten van het zoeken op het woord 'fraude' bij zowel via Google.nl als op de wnl op tijdschrift fraude. (Ook dat is vreemgens een gevolg van toepassing van Big Data en algoritmes).

Wel werd in het voorjaar van 2016 bekend dat er bij gemeenten voor 14 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-

In 2013 werd besloten tot de oprichting van een ministeriële commissie Aanpak Fraude, onder voorzitterschap van de premier en de minister van V en J als coördinator. Ook de ministers van szw, Economische Zaken (ez), Volksgezondheid, Welzijn en Sport (vws), ozk, Onderwijs, Cultuur en Wetenschap (ocw), W en en en Rijksoverheid 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 om motie vanuit de Tweede Kamer, van de leden Gesthuizen (sp) en Bandson (D66) voor de oprichting van een nationale fraudeautoriteit en het aanstellen van een nationale fraudecommissaris zoals in Engeland eerder genoemde—inmiddels opgeheven—National Fraud Authority.

Het kabinet verkoopt daarbij de weg van coördinatie boven de oprichting van een fraudeautoriteit en/of de aanstelling van een nationale fraudecommissaris. De toenmalige minister Opstelten van Verkeersdijsten daarbij de verdeling van ver-

⁵ 'Fraudekosten Nederland jaarlijks 30 miljard. Aanpak loont', Schalk & Partners, zonder datum <http://www.schalk.nl/pdf/FRAUDE-totaal%20kosten%202014.pdf> (Geradpleegd 17 februari 2016).

⁶ <http://www.trouw.nl/tr/14482/Nederl-miljard-aan-bijstandsfraude-nog-niet-gelnd.html> (Geradpleegd 19 april 2016).

antwoordelijkheden tussen bewindspersonen als helder.⁷ De commissie leidt de uitvoering van een Rijksbreed actieplan, dat eind december 2016 werd gepresenteerd.⁸

De oprichting van een commissie leek een nieuwe benadering, maar in de praktijk wordt fraudebestrijding periodiek met een maatregel opnieuw in beschijningeperget. Zowel 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 'ministeriecommissie-fraudebestrijding'. Behalve Lubbers namen ook de ministers Hirsch Ballin (Justitie), De Vries (sz) en Kok (Financiën) zitting in de commissie-fraudebestrijding, die de taak kreeg om het frauderen sociale fraudebeleid te coördineren. En dat in werd gesteund door een ambtelijke stuurgroep onder leiding van W. Imke 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 taken en samenstelling Stuurgroep fraudebestrijding' van, inmiddels, minister W. Imke 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 'Misbruiken oneigenlijk gebruik op het gebied van belastingen, sociale zekerheid en subsidies', minister Opstelten van Veiligheid en Justitie aan de Voorzitter commissie Veiligheid en Justitie, Nummer 0060-491, 21 november 2014, http://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2014Z2410&did=2014D4322 (geraadpleegd 19 april 2016).

8 'Misbruiken 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/downloaddocument?id=5028d05-5018-450b-aad1-4a02f5b33f18&titel=Rijksbrede%20aanpak%20van%20fraude.pdf> (geraadpleegd 19 april 2016).

9 <http://www.nrc.nl/handelsblad/1992/09/16> fraude-769006, (geraadpleegd 19 april 2016).

10 'Regeling taken 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 mogelijk fraudulente dooverheid of andere organisaties beschikbaar hebben. Het is cruciaal om (real-time) 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 overtradingen aan de digitale poort¹²:

- Hij zegde toe om in een aantal dossiers te inventariseren aan welke gegevensuitwisseling het uofficijs, (indusrief)bedrijf en (indusrief)bedrijf, ook in de vorm van mogelijk bestaande privacy protocollen voor samenwerkingsverbanden:
- gefingeerde dienstverbanden;
 - faillissementsfraude;
 - identiteitsfraude;
 - notoire fraudeurs (subjectgericht 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 op wils zouden daarin meegenomen kunnen worden. Daarover meer in het althoofdstuk.

Tevens versterkte de minister het systeem van Toelicht op Rechtspersonen (track) van de dienst Justis van zijn ministerie met een 'vraagrijdige signaleringsfunctie', gecombineerd met meer verfijnde risicoprofielen van beroepsfraudeurs¹³; personen die met verschillende regelingen fraude plegen. De laatste genoemd de analyse en profilering betreffen niet de vormen van fraude, maar verdacht personen. Ook hier gaat het, aldus de minister, om een verkenning van de mogelijkheden voor analyse van gecombineerde databestanden om verdachten te overnemen. Daartoe werd ook een 'combinatie 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 financiële economische criminaliteit (Finco) krijgen van 160 fte. De Dienst Regionale Recherche zou ook "Finco / fraude teams" krijgen.

11

¹¹ 'Rijksbrede aanpak van fraude', Brief van de regering, Nummer 11050-450, 20 december 2013, LW, Opstelten, minister van Veiligheid en Justitie aan de Voorzitter van de Tweede Kamer, (geraadpleegd 19 april 2016)
http://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=15225339&did=201501034 (geraadpleegd 1 februari 2016).

2.3 **slim voorkomen, vlot herstellen**

Op verschillende terreinen zou intensieve samenwerking fraude moeten terugdringen, bijvoorbeeld identiteitsfraude. Verschillende kabinetleden uitten de boodschap van dat dedden op uniform wijze. Al eerder is de minister van sz uitgesproken geestd.

Eind december 2018 stuurde de minister Plasterk van bzk, dekabinetsvisie op de aanpak van identiteitsfraude: 'Slim voorkomen, vlot herstellen' getiteld, aan de Kamer. Dit beoogde een modus operandi te zijn bij onder meer illegale grenspassages, illegale arbeid, mensensmokkel, drugshandel, terrorisme, witwassen en vele soorten fraude.

Daarmee wordt de kiem gelegd voor een brede uitwisseling van data van overheiden onderling, van publieke en private databanken onder meer de landregisterkruis, waarvoor ook Europol, de Europese opsporingsinstantie, al een warm pleidooi hield.

Minister Plasterk: 'Voorkomen en herstellen van identiteitsfraude vraagt om een integrale, informatiegestuurde aanpak waar in partners in publieke en private sector de krachten samenballen. Grote organisaties en zware ketens zijn kwetsbaar tegenover de kleine, creatieve, wendbare cadagrepen die hen bestoken en die makkelijk van aanvalsbasis wisselen van andere'.¹²

Dit was conform de wens van de Tweede Kamer voor een 'Integrale visie en het toegaan van versnippering van overheidsdaden.' Het antwoord op identiteitsfraude komt van moderne netwerken die snel en adequaat reageren. Van bolwerken naar netwerken. De sterk toegenomen aandacht voor fraude in meer betrokken partijen tot samenwerken: zowel op regionaal, als landelijk niveau. Met succes: door gebruik te maken van elkaars kennis en informatie worden fraudeurs geïdentificeerd en nieuwe maatregelen tegen fraude snel geïmplementeerd', aldus de minister.

2.4 **'vernetwerking' als doelen**

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 uuv, de Belastingdienst, het ock, het obs, het Centrum Indicatiestelling Zorg (oiz), het Centraal Justitieel Inzakebureau (cijb), Zorginstituut Nederland, Dienst Justis, de Rijksdienst voor Ondernemend Nederland (rvn), Dienst Uitvoering Onderwijs (duo), de Immigratie- en Naturalisatielendienst (ind), het Kadaster, de Kamer van Koophandel (kvk), de Rijksdienst

¹² Kabinetsvisie aanpak identiteitsfraude: 'Slim voorkomen, vlot herstellen', minister Plasterk van bzk, 20 december 2018 <http://www.tweedekamer.nl/kamerstukken/detail?id=201805829&id=201805829> (geraadpleegd 1 februari 2019).

voor het Wegverkeer (rdw) en de Sociale Verzekeringsbank (svb) samen (zie onderdeel Belastingdienst samenwerking).

Ook de partijen in de 'vreemdelingenketen' gingen intensiever datauitwisselen, 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 (ciop). Met deelname van 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 (rcof) en de Landelijk eBureau Groep Inlichtingen (laig), deze 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. Plattek:

"De samenwerking van de overheidsinstellingen in informatie, althans de integrale aanpak van identiteitsfraude mogelijk, zoals bedoeld in de visie."¹³

Dit sluit ook aan bij de afspraken voor samenwerking tussen publieke en private sector van het Nationaal Platform Criminaliteitsbestrijding. De aanpak van fraude noodzaak 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> (gearchiveerd 1 februari 2019).

¹⁴ Idem.

3

inleiding

De invoering van het nieuwe zorgstelsel begin 2006 leidde tot hernieuwde aandacht voor bestrijding van fraude. Deze fase deed in de eerste jaren. Op aandrang van het parlement is vervolgens een uitbreidingsamenwerking opgezet 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 problemen als het samenwerken in de zorgfraudebestrijding.

Wel werd er overigens jaarlijks voor miljarden aan 'onregelmatigheden' van medisch dedareren 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 toekomstig beheer van hun zorgdata, individuele inzage in dedaraties. Privacyafwegingen komen daarmee bij het individueel toelagen, zeker indien er financiële prikkelers bij zullen komen. Deze spanningen velden 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

bel eid en mislukkinge

Vlaamse art

Fraudebestrijding in de zorg kwam jarenlang moeilijk van de grond. In de media werd gesproken over een falen van het kabinet. Rusttel op dit punt. Zoals de beoogde inning van een relatief bescheiden bedrag van jaarlijks 47 miljoen euro aan onterechte dedaraties mislukte aanvankelijk, ofschoon de omvang ervan groot werd geacht: in een (concept)rapport van 2012 dat gedeeltelijk ingaat op wijzen van frauderen, staat bijvoorbeeld dat zich onthulden op privé in de onthulden al jaarlijks voor 50 tot 100 miljoen euro aan behandelingen dedareren zonder medische noodzaak.

Het betrof een conceptrapport van de C&G (Project Intensivering Controle en Toezicht), dat Rutte in zijn bezit kreeg, maar dat de minister van vva niet naar de

Tweede Kamer had gestuurd. Volgens haar was het gebrek aan eensgezindheid bij de deelnemende partijen over de eindvaste reden geweest om het niet te starten.¹⁵ De Kamer eiste daarop maatregelen voor zorgfraudebestrijding, wijzend op 'hjoemelende zorginstellingen, frauderende ziekenhuizen en malafide pgbemiddelingsbureaus'.

De Kamer drong aan op intensivering samenwerking tussen alle partijen betrokken bij 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 in geval 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 zetten en dus bestreden dient te worden. Onder leiding van VWS tekenden ook de volgende partijen:

- Nederlandse Zorgautoriteit (Inspectie voor de Gezondheidszorg)
- Zorgverzekerders Nederland
- Centrum Indicatie- en Stelling Zorg
- Inspectie Sociale Zaken en Werkgelegenheid (Inspectie Fiscale Inlichtingen en Opsporingsdienst)
- Belastingdienst
- Openbare Ministerie

¹⁵ Rapport in Call: Project Intensivering Controle en Toezicht op de rechtmatige uitvoering van de Zorgverzekeringswet (versie 25-03-2013); procebaschrijving en verbeteringen <http://www.tweedekamer.nl/kamerstukken/detail?id=2013D0160&did=2013D0160> (geraadpleegd: 9 april 2016).

'Fraude in de zorg veel groter dan gedacht', rti Nieuws, 16 mei 2015, <http://www.rtinieuws.nl/nieuws/fraude-de-zorg-veel-groter-dan-gedacht> (geraadpleegd: 19 april 2016).

Tijdslijn: waarom aanpak zorgfraude mislukte, rti Nieuws, 23 mei 2015, <http://www.rtinieuws.nl/nieuws/binnenland/tijdslijn-waarom-aanpak-zorgfraude-mislukte> (geraadpleegd: 9 april 2016).

¹⁶ Debat over Fraudebestrijding in de zorg, Tweede Kamer 28-828 Nr. 40, Nummer 20 13D21131, 24 mei 2013, <http://www.tweedekamer.nl/kamerstukken/detail?id=2013D21131&did=2013D21131> (geraadpleegd: 3 februari 2016).

steuning (Wmo) en de Wet en Marktordering 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 fors extra inzet tegen fraude en oneigenlijk gebruik [...] vermoedens bestaan dat het van een substantiële omvang kan zijn.'⁹

De opsporingsfunctie in de zorg werd versterkt en legdevw's grotendeels bij de Inspectiesw, die daartoe een budget kreeg voor investeringen in een nieuw werkhoud opsporing van zorgfraude, met name pgb- en declaratiefraude.

Door de investeringen in het toezicht van de zaken de opsporing bij de Inspectiesw zou ook het Openbaar Ministerie (om) te maken krijgen met een groeiend aantal fraudezaken, zo was het vermoeden. Het omkreeg dus vanaf 2010 interveringselden voor capaciteitsuitbreiding voor vervolging van fraude in de zorg. v.w.s stelde extra gelden menselijk recht 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 Inspectiesw versterkt met extra inspecteurs, die zich volledig gingen richten op zorgfraude met de focus op pgb-fraude. Vermoedens van grote omvang van fraude bleven zich opsignaleren, vooral nieuwberichten.¹⁰

Zorgverzekerders konden vanaf 2010 aan het Kenniscentrum Fraudebeheerding in de Zorg. Ook is vanuit genoemd Convenant vanaf 2010 een Verzamelpunt Zorgfraude actief, dat het Expertisecentrum Zorgfraudebestrijding (ezb) van fraudesignalen ging voorzien.

Bij elkaar ontstond – voor de buitenwereld – een ondoorzichtig web van samenwerking en verbanden om de omvangrijk geachte zorgfraude te bestrijden. Met welnig doeltreffend. Het ontmoetbaar door op 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-

⁹ Schippers en Van Rijn, 'extra geld en speciale inspecteurs voor aanpak zorgfraude', Nieuw se bericht v.w.s, 16 september 2013 <https://www.rijksoverheid.nl/actueel/nieuws/2013/09/16/schippers-en-van-rijn-extra-geld-en-speciale-inspecteurs-voor-aanpak-zorg-fraude> (geraadpleegd 20 januari 2016).

¹⁰ 'Fraudebestrijding in de zorg', Brief van de minister en staatssecretaris van v.w.s aan de Tweede Kamer, 28 oktober 2015, 27 maart 2016 https://www.tweedekamer.nl/kamerstukken/brieven_lagering/detail?id=201520160558&did=201601059 (geraadpleegd 20 januari 2016). 'Programmaplan Richtmatige Zorg: Aanpak van Fouten en Fraude 2015-2018', 27 maart 2015 http://www.tweedekamer.nl/kamerstukken/brieven_lagering/detail?id=201520160558&did=201601059 (geraadpleegd 20 januari 2016).

autoriteit (niet) als respectievelijk de walvis of de walvis inhouder, een de economische bestuursrechtelijke toezichthouder.²¹

Daarnaast funktioneert de strafrechtelijke lijn, met twee opsporingsinstellingen, Inspectie SZW en de . . . Dat is extra ingewikkeld. Vandaar ook zoveel plannen en rapportages op dit vlak; zo bevestigt de zadelindruk van complexiteit. Dit is volgens den zainhrent aan het Nederlandse systeem of model, dat zich ook op andere domeinen manifesteert:

'Niet één partij heeft de leiding, maar elk partij brengt expertise en bevoegdheden mee. In de zorg is dat extra ingewikkeld, omdat een belangrijk deel van de controle- en bijstand (dwingt) bij private verzekeraars. Zij moeten optreden, terugvorderen of stoppen met een contract.'²²

3.2

gemen de resultaten

Miljoenen geraamd

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

- vooraf aan betaling uit ~~de~~fraudebestrijding: 350 miljoen;
 - controle betaalde declaraties: 329 miljoen;
- onjuistheden in ~~de~~fraudebestrijding:
 - daadwerkelijk aan fraude vastgesteld: 9 miljoen;
 - vermoeden, onvoldoende bewijs: 8 miljoen;
 - administratieve fouten: 0 miljoen;
- gemiddelde fraudebedrag:

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

- vooraf aan betaling uit ~~de~~fraudebestrijding:
 - 449 miljoen;
 - controle betaalde declaraties: 329 miljoen;

²¹ Interview met Daan Molenaar, hoofd toezicht zorgaanbieder, bij de nza-Idam.

²² 'Zorgverzekeraars besparen 300 miljoen euro door controles', nieuwsbericht zn, 15 juli 2014 <http://www.zn.nl/338067458/Nieuwsbericht?navitemid=2954211> (geraadpleegd 20 januari 2016).

²³ 'Fraudecijfers 2013, toelichting persbericht juli 2014', nieuwsbericht zn, 15 juli 2014 <http://asas.zn.nl/pr/32768/Nieuw-Fraudecijfers%202013%20toelichting%20persbericht%20juli%202014.pdf> (geraadpleegd 20 januari 2016).

- onjuistheden ~~risicofactoren~~ **dedarates**:
daadwerkelijk aan fraude vastgesteld: 9 miljoen;
vermoeden, onvoldoende bewijs: 7,5 miljoen;
administratieve fouten: 25 miljoen;
- ~~gemiddeld~~ **fraudebedrag**:

Opvallend is de relatief hoge afwijking van dedarates in de categorieën 'Mondzorg' en 'Hulpmiddelen' vooraf en het zeer hoge percentage van de specialistische zorg in de bestrijding van onjuist geachte dedarates achteraf: 81 procent (van die 44,9 miljoen euro) tegen een aandeel van 59 procent in het totaal gedaraarde zorgbedrag (van de 37,7 miljard euro).

Van de daadwerkelijk afgedragen vond 70 procent plaats in de wvz (nu Wlz), en dan nog voornamelijk in de Omschakelings- en Secundaire Zorg (vgz) 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 onbekend.

Er is 69 keer een 'verzoek' gedaan om een fraude via het bestuursrecht, strafrecht of toezicht te sanctioneren. Zorgverzoeken zijn hiërarchisch inhoudend, aan gezien de oorsprong en tijdinvesting omvangrijk zijn.²⁴

Totaal gedaraard voor de basisverzekering in de Zvw in 2013:
40 miljard euro, met 2,6 miljard euro aan correcties is 6,6 procent.

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

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

Zorgverzekeraars Nederland (zn) verklaart de materiële controle als volgt. De zorgverzekeraar gaat na of:

- de door de zorgverlener in rekening gebrachte prestaties geleverd (‘tigheid’);
- en die geleverde prestatie het meest wat aangewezen gezien de gezondheid 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 (buiten de fraudemeldingen van zorgverzekeraars) geen data hebben. Het Kenniscentrum Fraudebeheersing verzamelt fraudemeldingen van de zorgverzekeraars ten behoeve van de coördinerende van zn-richting zorgverzekeraars.’²⁵

Wenig fraude vastgesteld

Het bedrag aan fraude bedraagt minder dan 1 procent van het totale bedrag aan onjuiste gecodeerde declaraties. De nza besamt dat dit een disoutabele verhouding is:

‘De preventieve van deze cijfers komt wel ongelukkig. Fraudes van heel lage beschuldiging, die niet snel wordt geuit. Dat is een gevolg van de eerste zorgvuldigheid in het hele langdurige proces, alond 16 jaar per bestuurrechtelijk onderzoek en al drie tot soms vier jaar langer 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 flagrantgevallen worden naar het om doorgeschoven.

‘We zien dat er veel fouten worden gemaakt en als er voor een miljoen euro in orde is gededareerd, kunnen we veelal niet achterhalen of er sprake is van die boel bovustflosson. We leggen dan wel een bestuurrechtelijk oobstoot, maar strafrechtelijke vervolging is dan heel moeilijk.’²⁶

Genoemd Verzamelpunt Zorgfraude rapporteerde in juni 2016 over het jaar 2014:

‘Er waren in dat jaar 608 unieke signalen’ bij het verzamelpunt aangemeld door verschillende partners, van wie twee de patiënten. De grote meerderheid betrof tips over ‘upcoding’ en ‘spookfacturen’. Dit aantal resulteerde in een kleine tweehonderd afgeronde vooronderzoek en mid mogelijk een maatregel. Daarover werd inhoudelijk niet gerapporteerd. Ook betrof dit geen data analyse, wel *geteelde noten van onderzoeken*.²⁷

²⁵ Wordvoering zn, schriftelijke antwoorden 25 januari 2016.

²⁶ Interview met Daan Molenaar van de nza.

²⁷ Rapportage Verzamelpunt Zorgfraude 2014, nza, 30 juni 2016 <http://www.tweedekamer.nl/kamerstukken/detail?id=2015020238&did=2015020203>

Dit lijkt vrij geringe cijfers, in vergelijking met de eerder genoemde jaarlijks tot 6,5 miljard oplopende declaratiecorrecties. Dit vinden wij zelf ook wel enig, maar we verwachten dat het aantal tips de komende jaren zal toenemen als bij consumenten de bekendheid toeneemt van de mogelijkheid om verdenkingen van incorrecte declaranten te melden.²⁸

Ook de cijfers over resultaten van de inspecties zwijven omgekeerd geen indicatie van een edantant-succes in bestrijding van zorgfraude. In heel 2016 zijn elf opsporingsonderzoeken en twee ondernemingsonderzoeken met pgb's afgerond en ingeleverd voor strafrechtelijke vervolging.

Het ging bij elkaar om een kleine 6 miljoen euro. Daartoe zijn bijna 2.000 opsporingsuren besteed. Er waren, in samenwerking met de zorgkantoren, in z'n ligz, Belastingdienst, en GGD's wel honderd zaken bij de bekendheid gemeld, waar van dus 10 procent met succes is afgerond. Zaken zijn tijdrovend, zo werd gemeld.²⁹ Op een totaal van 2,75 miljard aan pgb-tokkenningen is dit een gering resultaat. Volgens de Rekenkamer was het spuren naar pgb-fraude zodoende inefficiënt.³⁰ De teams voor pgb-fraude en declaratiefraude van de inspecties zwijven samenwerkend met de GGD's vanwege de daar aanwezige kennis en expertise. Ook de mogelijke samenhang tussen zorgfraude en andere vormen van fraude, zoals fraude met inkoop van medicijnen of fraude met de verkoop van landbouwproducten, is niet onderzocht.

Tot verbetering leidde dit echter nauwelijks. In de eerste tien maanden van 2014 rondde de Inspectie zwijf strafrechtelijke onderzoeken en vijf ondernemingsonderzoeken van pgb-fraude af. Er werd verbetering voorzien: "Doordat de vnb 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." Dit zaertent dat deze fraudebestrijding met twee sporen, via de GGD's en de Inspectie zwijf, niet efficiënt genoeg was: "Werk aan uitbreiding naar samen. De samenwerking is niet altijd goed gegaan afgelopen jaren. Dat is nog een uitdaging."³¹

²⁸ Interview met eerdergenoemde.

²⁹ Signaleringsbrief van de Inspectie zwijf gericht aan ministerie van vws, 7 april 2014 <http://www.rijksoverheid.nl/documenten-en-publicaties/brieven/2014/04/07/signaleringsbrief-van-de-inspectie-zwijf.html> (laatst geraadpleegd 19 april 2016).

³⁰ Rekenkamer Aanpak pgb-fraude: veel maatregelen, nog onvoldoende zicht op effecten <http://www.toezichtonderzoekrekenkamer.nl/2014/veel-maatregelen-nog-onvoldoende-zicht-op-effecten> (laatst geraadpleegd 19 april 2016).

³¹ Mededeling regering <http://www.rijksoverheid.nl/onderwerpen/fouten-en-fraude-in-de-zorg/inhoud/gericht-tegen-pak-over-tredingen-bij-declaratie-en-betalingen-in-de-zorg>

³² Interview met eerdergenoemde.

Mislukking expertisecentrum

Ook moest de zaak kennen dat het Expertisecentrum Zorgfraudbestrijding (ezb) als samenwerkingsverband een mislukking werd. Het ezb kreeg een strategische en een operationele functie.

De operationele functie behelsde de centrale aanpak van meer eenvoudige zorgfraude, ook op terreinen waar de grootste risico's liggen, zoals deggz en de medisch-specialistische zorg. In de strategische functie speelde intelligentie een belangrijke rol bij het verzamelen, verwerken en interpreteren van (digitale) gegevens waarmee (patronen van) fraude in de zorg opgespoord kunnen worden. Deze taak neelde naar grootschalig datascrubbing.

Van enig resultaat is echter weinig tot niets vernomen. In de vorm van het expertisecentrum werd het niet. Vooral de algemene analyse waar niet goed gereageerd werd (het 'loose spel') ezb bleef eind 2016 opheffen. Middenlaad wordt onder de hoede van vier overleggepleegd om een nieuw instituut op te richten om de krachten te bundelen in fraudebestrijding. Ook Andersson Effter Felix (aef), een adviesbureau voor maatschappelijke vraagstukken, adviseerde om één opsporingsdienst voor de zorg op te richten.

De conclusie luidt dat de bestrijding van onrechtmatiggededacties effect sorteert dank zij inspanningen van de individuele verzekeraars, maar dat het in samenwerken vervolgen van fraude in de zorg problematisch zijn.

Poging samenwerking verzekeraars

In maart 2016 stuurden de minister en staatssecretaris van vws de Kamer het programma met plannen 'Redtmatige Zorg' toe. Daar in 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 [...] data-mining'.

Het inzetten van data-analyses, bestaande in systeemvergelijkingen op biologische boden waar verbetering vatbaar. Maar fouten en mogelijk barst overtreedingen zouden daarmee aan het licht komen. De politiek bepleitte dat zorgverzekeraars nauw samenwerken en – waar zinvol en juridisch mogelijk – gebruik maken van elkaars analyses en resultaten.

Zorgverzekeraars investeerden immers elk apart in controles en aanpak van fraudebeheersing met behulp van eigen data en het om (risico's op) onrechtmatigheid en toedoeletoeren.

In 2015 verkenden zorgverzekeraars mogelijkheden voor gezamenlijk fraudeonderzoek – inclusief data-uitwisseling en analyse – uiteindelijk in een gezamenlijke onderzoeksseenheid. Ze maken ergaan haast mee in het 'Plan van aanpak fraudebeheersing 2015–2017' van zijn 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 zorgdoelen die extra aandacht behoeven in de fraudebestrijding, en samen suggesties te doen voor het verbeteren van wet- en regelgeving op grond van fraude signalen.³³

In januari 2016 liet in op schriftelijk vragen van mij over de uitvoering het volgende weten: 'Onlangs heeft in dit plan van aanpak geëvalueerd. Ten aanzien van punt 1 (Thema is om samenwerken in ketens op specifiek fenomeen) is geconstateerd dat dit lastig te stroomlijnen is. Dit punt vervalt daarom. Dat is geen ramp, omdat het ons niet zo ver gaat om data-analyse, maar om risicoanalyse (hoe vaak 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 waar in zorgverzekers in fraudeonderzoek met elkaar samenwerken. Bijvoorbeeld data-analyse in definitieve vorm worden uitgewerkt.³⁴

Wel is binnen zijn een proef gestart van het portal Raadpleging Integriteit Zorgaanbieders (ri-z). Zorgverzekeraars kunnen via het ri-z diverse relevante databronnen (tijdens de pilot agb, big, en Insolventieregister) gelijktijdig raadplegen, waardoor het screenen van zorgaanbieders efficiënter wordt. Voorts nog blijft data-analyse een zaak van zorgverzekeraars apart.

De belangrijkste profwensen niet bedrikkbaar. Volgens Cappelmini heeft gemeenlijk e fraudebestrijding van verzekeraars als Achmea, vgz, oz en Menzis geen prioriteit, omdat de kostenverlaging door vorminering van fraude concurrentievoordeel oplevert. Kijken in elk anders kijken niet voor de hand. De kleine verzekeraars, zelf al op streek met pragmatische opzet te data-analyse voor fraudebestrijding, doet volgens Cappelmini pogingen om tot collectieve fraudebestrijding te komen.³⁵

Den zaander nam, onder meer via het ez-b, de nodige pogingen om gemeenlijk op te trekken in fraudebestrijding. En ontloopte ook zelfstandig initiatieven; zie onder. Niet holder is waar de grens ligt tussen aanpak van vorderingen door de zwaeren door verzekeraars. Volgens de zwaeren dat afhankelijk van de plaats waar het signaal wordt opgepakt. Soms vindt samenwerking plaats tussen zwaeren verzekeraars.

Kritiek op de sector

Adviesbureaus efw als in een recente evaluatie van de wmg (markt wet zorg) en nzo kritisch. De nadrukkelijke aandacht voor zorgfraude is volgens de f met con

33 'Plan van aanpak fraudebestrijding 2016-2017', ongedateerd, zie <https://saas.zn.nl/pl/32768/None/files/Plan%20van%20aanpak%20fraudebestrijding%202016-2017.pdf> (geraadpleegd 16 januari 2016).

34 Rik van Druen, woordvoerder al van zn, 27 januari 2016.

35 Inter view Norbert Janen, adviseur Business Development Fraude and Error, Cappelmini Nederland.

bureaucratisering gepaard gaan. Den za 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 den za heeft met de nadruk op fraudewiel bewust wording bewaakt elgd over onrechtmatig gebruik van zorggelden en controle door verzekeraars.

Blijverdictes had dat niet tot gevolg. De manier waarop den za invulling geeft aan het toezicht kan in het veld op weinig draagvlak rekenen. Er is met name kritiek op de protocolering en de manier waarop den za die handhaaft.³⁶ Kortom, verzekeraars vinden dat n z at 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 die zorgverzekeraars voorop met de patroonherkenning vanuit data verzamelingen voor fraudebestrijding.

Het risicoprofiel kan per claim worden vastgesteld op grond van data-analyse, zoals vanuit claimgedrag (her)familie, demografische- en geografische kenmerken, tekstanalyse en sociale banden zoals die zich online openbaren. De effectiviteit zou kunnen toemomen door meer samenwerking in uitwisseling van methoden en fraudesignalen, maar het eigen belang prevalet.³⁷

In de zorg maken die grote verzekeraars ook gebruik van de expertise van Deloitte voor data-analyse en fraude detectie. Deloitte adviseerde om niet langer een ondergrens te hanteren voor bedragen waar bij fraude wordt onderzocht. Niet de hoogte van de claim, maar combinaties van indicatoren in relatie tot een opgebouwd profiel moeten bopalen of er controle op con d id m plaatsvindt. Fraudelen ook in kleine bedragen frequent optreden.

Deze fraudeprofielen kunnen naast de geschiedenis van een klant worden gelegd. In de data-analyse van zorgdatabases worden patronen vastgesteld: gaan tandartsen bijvoorbeeld of geen pgb-aanvraag zo speciaal offer is in het heel grote bestand wel vergelijkingsmateriaal voorhanden. Statistisch gezien is niemand of geen enkele situatie uniek, aldus Deloitte.

Het dedaren van r i g t r o k k e n k l i z a n b i j d a n p a t i e n t v a l t z o w o o p , m a a r k l i z n e e f w i j k i n g e n o o k . A l s e e n n o t a o p v e r s c h e i d e n e r i s c o - i n d i c a t o r e n a f w i j k t ,

36 Ordeningen toezicht in de Zorg – Evaluatie Wet Marktordening Gezondheidszorg en de Nederlandse Zorgautoriteit. Anderson Elffers-Pelx, in opdracht van het ministerie van welzijn, september 2014 https://www.nzan.nl/1048076/1048511/Rapport_AEF_Evaluatie_Wet_Marktordening_Gezondheidszorg_en_de_Nederlandse_Zorgautoriteit.pdf

37 Interview met Norbert Jansen van Capgemini Nederland.

moet de kans op controletaken. Deloitte noemt succesratio's tot boven de 90 procent bij het traceren van onregelmatig gedrag afgeleid 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 nidi in orde is. Los van de oorzaken. De resultaten, zowel de juiste indicaties als onjuist gebleken verdenkingen, moeten 'terug' in het systeem ter verijning van bestaande indicatoren, zodat de volgende rondes daarop worden afgestemd.³⁰

Paging tot fraudemonitor

De twentse hoogleraar. I heb 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 de belangrijkste sleutels naar data-schakelamer. 'De toename in data vraagt om inzet van nieuwe geavanceerde methoden voor handelingen 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 400 miljoen dollar een zo gnfraudeur ontdek dank zij analyse van de data. 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 (difi) van de Universiteit Twente. De doelen waren:

1. Het ontwikkelen en opzetten van een nationale fraudemonitor, van belang gescht voor een groot aantal beleidsinstaties.
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.

difi 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 difi met pging voor een promotieonderzoek naar faillissementstrajecten aan de Universiteit Twente vindt onderzoek plaats naar fraudegevoeligheid van verschillende bo-categorieën met zorginstaties. Beoogde samenwerking

met de National Fraud Authority (nfa) in Engeland liep spaak, omdat de Britse regering daarin 2014 opdoekte om maar ministeriale 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 Universiteit Twente. Wel wist hij meesamen 'scans' van de Stichting Toekomstbeeld der Techniek (stt) om de omvang van fraude en ICT-belasting te schatten.

De Vries constateert te weinig gebundelde inspanning van partijen die bezig hebben bij de bestrijding van zorgfraude. Hij verwijlt dit vooral aan de Vanoucs zijn de diverse belangen in de Nederlandse zorg volgens hem echter getragmenteerd. De Vries: "Het is eenvoudig om je 80 tot 90 procent ontdekken, want verzekeraars hebben uitstekende data verzamelingen. 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 vaak voor het bedrijfsleven. Je moet die mensen goed betrekken en goede perspectieven bieden in de zorg. Hun werk is goud waard."

Anderszijds toonde De Vries zich bezwaard dat de groei in kopopdringen 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 data-toepassingen versus de risico's voor de privacy van individuen. "Maar de privacy is sterk juridisch geïntendeerd, 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/stijp/2019/200-022%20presentatie%20fraudeseminar%20tho%20de%20vries%2022.pdf> (geraadpleegd 20 januari 2016).

Nieuw bericht t.d.m.: <http://www.digitaleoverheid.nl/onderwerpen/stalalinfomatiepunt/staal-van-basisregistraties-1858-presentatie-tho-de-vries> Dutch Fraud Initiative (dfi), Universiteit Twente <https://www.utwente.nl/ig/dfi/dfi/> (geraadpleegd 22 januari 2016).

Fraudemonitor rapportage 2006, Universiteit Utrecht, Departement Methoden en Technieken <http://docplayer.nl/6257816-Fraudemonitor-rapportage.html> (geraadpleegd 22 januari 2016).

FraudeLoont... nog steeds!, Redactie Alas van Geldrop en Theo de Vries, 2016, Stichting Toekomstbeeld der Techniek (stt) <http://stt.nl/publicatie/quick-scan-fraude-loont-nog-steeds/>

Data-analyse van declaratiegegevens

Den zal 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. Dit specialisatiedat in datamining en datastream mining, respectievelijk vissen in databestanden en in datastromen.

Den zal 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 farmacieën, 4 miljoen van ggz gebruikt vanuit de Vektis-databanken. Totaal 1,7 miljard gegevens, die dan zijn toegelaten computerkracht en nieuwe analysemodellen nu 'lekken' waren. Met behulp van datamining zijn onregelmatigheden opgespoord in declaratiebestanden.⁴⁰ 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 of meer keren per jaar de patiëntvergoeding declareren. Dat wil nog niet zeggen dat het fraude is, het kan een menselijke of een systeemfout zijn.

Het declareren van anomalieën met een breed scala van modellen en technieken was ook volgens het FDEC goed mogelijk met de Big Data-exercitie. Deze leverde direct identificatie van de declaratie op en indicaties op om het mogelijk te verbeteren de bedrag was eenvoudig te berekenen en relatief zeker. Erg omwaarschijnlijk cases werden snel zichtbaar.

Om het totale bedrag dat gemoeid was met overtredingen van declaratie regels 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 declaratie regels bloot te leggen. Voor 2010 is geconcludeerd dat het overtreden van declaratie regels leidde tot een te veel vergoede 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 detecteerbare declaraties varieerden van 0,8 bij huisartsen tot 0,1 procent voor de ggz.⁴¹

Data-analyse wtz

Den zal vroeg voor aan het FDEC om declaratie inzake de Algemene Wet of 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 medische specialistische zorg", Prof. dr. H.M.P. Kersten, Dr. W.J. Kooijman, Dr. F. Kleye, FDEC, 8 augustus 2014
[http://www.zaan.nl/regelgeving/bijlagen/Eindrapport_Onregelmatigheden_in_declaratiebestanden_in_zas_zorgsegmenten_FDEC\(gesdopgego23\)anuari2016](http://www.zaan.nl/regelgeving/bijlagen/Eindrapport_Onregelmatigheden_in_declaratiebestanden_in_zas_zorgsegmenten_FDEC(gesdopgego23)anuari2016).

pgb. Voor het pgb worden veel minder gegevens vastgelegd in systemen, dus is detectie van fraude niet eenvoudig, terwijl juist het pgb fraudegevoelig is volgens de onderzoekers. In sommige gevallen wordt er geen zorg ingekocht of er wordt te weinig zorg ingekocht.

Dit volgens de deo-onderzoek⁴¹ richtte zich specifiek op de declaratiebestanden waardoor over de zorginkoop bij pgb geen uitspraken gedaan konden worden, louter over Zorg in Natura. Van het oak en zijn zijn 29 miljoen declaratie-reeds over 2012 en deels over 2013 gemaakte.

Voor het pgb ontbrak alle gegevens over 2013. Louter goed gekleurde declaratie-telden mee, niet de door zorgkantoren reeds afgewezen declaraties. Dat waren te beperkt en moesten completer zijn om een goed beeld van onregelmatigheden op te stellen, aldus de onderzoekers. Ze splitsten hun bevindingen in:

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

Het teveel gedeclareerde bedrag bij de wettelijke 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 zijn is in 2013 voor circa 300 miljoen euro teveel gedeclareerd op een totaal van ruim 20 miljard euro facturen. In 2013 voor circa 50 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 pgb kwam voor 2012 op circa 42 miljoen. De meest voorkomende overtredingen waren het overschrijden van maximum beleidsregelwaarden, niet-volgende combinaties van zorg en meer zorgfacturatie en dan goedgekeurd. Deze uitkomsten vragen om nadere bespreking door domeinexperten, vinden de onderzoekers. Data-analyse levert direct identificerbare zorgaanbieders op. Het teveel gedeclareerde bedragen worden berekend en is relatief hard.

Het rapport laat – mede vanwege privacyoverwegingen – niet zien hoeveel en welke zorgaanbieders bij dit onderzoek zijn betraapt. Deze informatie is wel aan de nabestaanden gesteld. Momenteel is niet altijd de oorzaak, maar moeilijk te onderscheiden: 'We hebben waargenomen dat vaak fouten worden gemaakt met de tijdsenheden van declaraties, dat waar in een gedeclareerd moet worden, vult

41 'Onderzoek naar onregelmatigheden in de bestanden van de Zorg in Natura (zin) en het persoonsgebonden budget (door fd eo)' dr. H.M.P. Kersten, Dr. W.J. Korvalskyk, 14 september 2014 https://www.zin.nl/1048073/1048159/Onderzoek_naar_onregelmatigheden_in_de_bestanden_van_de_Zorg_in_Natura_ZIN_en_het_persoonsgebondenbudget

men minuten is. Dit leidt natuurlijk – zonder juiste controle en arts medewerkers – tot een veel te hoog gedecarieerd bedrag.⁴²

Data-analyse op ggz-declaraties

Vervolgens heeft den za zelf aanvullend onderzoek gedaan om meer details te kunnen analyseren over ggz-declaraties.⁴³ Het dco-informatiesysteem (dis) biedt declaratiegegevens van aanbieders van geestelijke gezondheidszorg, inclusief de daadwerkelijk besteedte tijd (althans, die door aanbieder is ingevuld, de werkelijk tijd is niet controleerbaar vanuit een systeem).

Den za heeft op deze dis-data een aantal toetsen uitgevoerd. Als eerste is de waarde van gegevens gecontroleerd. Zo kwam naar voren van welke geregistreerde behandelingen of activiteiten het aantal geregistreerde minuten groter was dan de wachttijd 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 in de praktijk niet voorkomt? Immers, zodra een zorgaanbieder 800 minuten heeft besteed, levert een extra behandelingfinanciering niets op, maar leidt dit wel tot kosten. De nza berekent hoeveel procent van de dco's van een zorgaanbieder 800 of 900 minuten geregistreerde besteedde tijd bevatten om in kaart te brengen of er zorgaanbieder zijn die zich hierdoor laten leiden.
2. In hoeverre geven aanbieder patiënten die in 2011 onder behandeling waren met de diagnose 'aanpassingsstoornis' vanaf 2012 een andere behandelcode? Immers, de 'aanpassingsstoornis' behoort de niet langer tot het verzekerde pakket. De nza constateerde dat het aantal patiënt en met deze diagnose in 2012 sterk terugliep.
3. Verder een anomaliedetectie op de totale tijd die zorgaanbieder hebben besteed aan patiënt en per dag: hoedat kan er bijvoorbeeld worden als de meest extreme gevallen op een lager niveau uitkomen. Op basis van deze analyse hebben we vastgesteld dat voor 2011 54,8 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 levert de onterechte dubbele vergoedingen op voor een totaal van 166 miljoen euro.

Dit rapport heeft inzicht in de mogelijk heiden van fraude detectie met behulp van grote databases. Het gaat hier over gegevens nog om vrij basale en voor de hand

42

43

Idem.

Tijdschriften verblijfsdagen en diagnoses in ggz, nza, 12 december 2014 https://www.nza.nl/publicaties/1043188/Tijdschriften_verblijfsdagen_en_diagnoses_in_ggz

liggende indicatoren. Naar verwachtings spelen zorgaanbieders daar ook op in. In bepaalde opzichten is het ook bijna hierisch: een dag helt 1440 minuten. Maar bij één aanbieder kwam n.z.a tot registraties van gemiddeld 254 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 behandelster in kwestie leerstellig deweg is kwijt geraakt.

De vraag is wat er concreet gedaan is met de resultaten van deze onderzoeken. Volgens de zwaaiers zal er eerst bedoeld om die verzekeraars te prikkelen om meer onderzoek te doen, gestimuleerd door de minister van v.w.s. Die minister wil de ook de omvang van de zorgfraude weten. Dat kwam er niet van.

Immers, in vergelijking tot veel andere landen, die per centage van 3 tot 12 procent rapporteerden aan fraude met zorgbudgetten, waren de percentages van de d.n.z.a.-onderzoek en 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 radar met deze uitvoering van de data-analyse.'

Dit heeft invloed op de prestaties van fraudeonderzoek aan de hand van data-analyse. Ofschoon vooral de indicatoren en de wisselwerking met daadwerkelijk e.w.m. (bepalingen) tot de huidige 'pakken' modellen leiden. In de p.w.-wereld wordt de omvang van fraude groot geacht, maar exact is dat niet vast te stellen, want niemand wil uitgebreide inhoudelijke 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 declaratievoorhanden

Denk aan voor deze analyse een beroep doen op de declaraties van al elke verzekeraars die v.w.s. is van zorgverleners komen. Vekt is publiek: in samenwerking met d.n.z.a. van 2014 de Vektis Datasat Zorgverzekeringswet, open data ten behoeve van studie met in eerste instantie het databestand Zorgverzekeringswet 2012, gevolgd door 2013. Dit geeft inzicht in de bestaande 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-

heid en de kwaliteit van zorg te verbeteren. Zo zijn er data op postcode (driedigheids) 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 gepasseerde zorgdeclaraties niet enkel doorluist, maar ook bundelt en analyseert. Vektis komt daartoe via leverandiers als Intech ICT, Axians- en IBM-systemen waarmee volgens Vektis de data-analyses worden versneld met een factor 10 tot honderd. Dat genereert ook fraude signalen als onderdeel van trendanalyses. De analyse is beperkt door bescherming van privacy en vanwege concurrentiegevoeligheid. Vektis bundelt geen data op personeelniveau en de specifieke gegevens van individuele zorgverzekeraars worden afgeschermd.⁴⁶

Er treedt een spanningsoverloop. Vektis biedt kwalitatieve overzichten, maar verzekeraars vinden analyse op dit niveau niet wenselijk. Volgens Achmea schieten de mogelijkheden voor Vektis tekort om patronen te duiden, zoals het hiërmas 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 Ido 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 bestaat toenemende aandacht aan fraudebestrijding door tientallen miljoenen declaraties op afwijkendjes op te analyseren. In 2011 heeft Achmea een Kenniscentrum voor onderzoek en toepassing van haar databank opgeleht. Intern werken er nu 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', nieuw bericht Vektis, opgedateerd <http://www.vektis.nl/index.php/nieuws/onderzoeken/375-data-analyse-speelt-belangrijke-rol-bij-aanpak-zorg-fraude> (geraadpleegd 21 januari 2016).

⁴⁶ 'Sensitap publiceert Open Data', nieuw bericht Vektis, 4 november 2014 <http://www.vektis.nl/index.php/nieuws/algemeen-nieuws/518-sensitap-publiceert-open-data> (geraadpleegd 21 januari 2016).
Vektis/Open Data/Databases and Zorgverzekeringwet

⁴⁷ <http://www.vektis.nl/index.php/vektis-open-data> (geraadpleegd 21 januari 2016).

⁴⁸ 'Referentie Vektis', Intech ICT Performance Solutions, opgedateerd http://cdn2.hubspot.net/hub/227033/files/59232780-pdf/docs/Referentie_Big_Data-Vektis-Intech_ICT.pdf (geraadpleegd 16 juni 2016).

⁴⁷ Interview met Daan Molenaar van den za.

⁴⁸ Interview met Barry Egbertsen Rob Konijn van Achmea.

zoek om de concurrentiepositie te vast te leggen. De scheiding tussen beide is niet altijd absoluut. Vanuit de data wordt gezocht naar opvallende relevante correlaties, zowel bewust als met serendipiteit.

Afleen al 13 miljard euro aan zorgdeclaraties verwerkt Achmea Zilveren Kruis per jaar, de belangrijkste basis voor de data mining vanuit de pas-software voor databewerkingen - analyse. De onderliggende Achmea Health Database wordt steeds vaker door derden gevraagd voor wetenschappelijk onderzoek, voornamelijk om wetenschappelijk erendemen.

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 heeft twee categorieën:

1. formele controle: toetsing aan wettelijke politissen;
2. materiele controle: afwijkingen van normaal declaratiegedrag in beeld brengen, mer behulp van onder meer data analyse.

De materiele controle (adherief) leverde op jaar basis tussen de 40 en 45 miljoen euro op (2014). Ook Achmea neemt het woord fraude bij voorkeur niet in de mond, omdat zowel de vermoende opzet als strafrechtelijke implicaties een goede reden, verregaande bewijsvoering vereisen.

Zo blijft de categorie: bewezen fraude bij Achmea door deze benadering beperkt in omvang: een kleine 8 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 defacturen inzien en afwijkingen vaststellen in vergelijking met ondergaande behandelingen. Patroonanalyse uit data check online noemt toe, ook in combinatie met deze tips. Voorbodden van onjuist declareren dat is getoetst met, of ondersteund door, data-analyse volgens genoemde woordvoerder:

- Eerder is gepubliceerd over een casus zorgfrauderij binnen een plastic chirurgie 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 tekorten van fraude.
- Op het raakvlak van tandverzorging en kaakchirurgie vallen vanuit de analyse steeds meer onregelmatigheden op. Tandchirurgie valt vaak onder de aanvullende verzekering zonder eigen risico, kaakchirurgie behandelde als vallen onder het eigen risico. Artsen gaan daarmee soms in default.
- 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 strekking van medicijnen onderhevig aan antedatering bij declareren; overnemen naar een vorig jaar waarin het eigen risico al verbruikt was, of juist naar een volgend jaar waarin meer kans is op het opcoûperen van het eigen risico; ook het juist in of uit de basisverzekering halen van – zoals van de anticonceptiepil – lavant opvallende grafiek en op over de behoefte aan anticonceptie in Nederland.
 - Id-fraude: zorgontvangen op het paai van een ander is een grote categorie. Ook buitenlandse familie en kennissen kunnen hier van gebruik maken. Data analyse van buitengewone combinaties van kwalen lavant verdinkingen op. De vervolgate wel moeilijk, hard bewaken zijt.
 - Het voorschrijven van remidipaten vaker gevilde methode. Patroonherkenning kan aan het licht brengen of bepaalde zorgverleners hiervoor vatbaar zijn.
 - De eerder met veel *probeding* omgevoerde 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 dat niet opvallend gemakkelijk.
 - Het voorschrijven van opiaten is vanouds fraudegevoelig. Shuivende zaken of diñten zijn via data analyses soms op te sporen.
 - Verkeerde bankrekeningnummers komen aan het licht, vaak per abusie vult. Gebruik van bankrekeningen van familieleden voor betalingen door zorgverleners kan duiden op een verkeerde bededding.
 - Te veel nullen in declaratiebedragen of andere typfouten blijken meer komen dan gedacht en er ook vaak door heen teglippen. 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 me

Rapportage succes

Eind oktober 2015 zijn over Programmaplan Redmatige Zorgen Aanpak van Fouten en Fraude 2015-2016 resultaten bekendgemaakt. Deze is echter door het ministerie van vws zelf geproduceerd en het plan sprak in vrijheid louter positieve termen over successen van de 'integrale aanpak' op drie terreinen en thema's. Hoe 'integraal' de aanpak van fraudebestrijding is in de praktijk, en op welke momenten het containerbegrip 'integrale aanpak' bijdraagt aan eventuele successen, komt in de verantwoording niet tot uitdrukking. Wel maakt het rapport uitgebreid melding van de activiteiten van den za 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 integrale ‘integrated approach’ nog niet is gerealiseerd.⁴⁹

Toezicht 2.0

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

- 10: toezien **Toezicht**nteljk eadministratieve organisatie, procedures, integriteit, ethiek, deskundigheid, data.
- 2.0: In het **Officiële**tdad rastie vaker wordt steeds diepgaander data-analyse toegepast. Opleiding- en expertise is op het terrein van de zorg wordt gecombineerd met vindingsrijke van onderzoekers en de denkkracht van wimpulatie om te komen tot innovatieën.

De Vektis-bestanden vinden zeechter onvoldoende toespitst op analyse om fraude op te sporen.

Zo maken de reeds door zorgverzekeraars geleverde declaraties er geen deel van uit. Er is in de onderzoeken voor de nazalouter een schatting gegeven van de omvang (frequentie en bedragen) van de onregelmatigheden. Er moet volgens de onderzoekers van fideo een volgnakering worden gehouden met *vooral falsen rege-tives* (het is mis, maar het alarm gaat niet af), maar ook met de falsen positives (vals alarm).

Om vast te stellen of merkwerdige zaken daadwerkelijk frauduleus zijn, vindt het fideo nader dossieronderzoek noodzakelijk. Dat geldt ook voor de vergelijking met informatie over daadwerkelijk valende zorg (zie onder). Ook wijzen ze op het ontstaan van kat-en-muis spel tussen fraudeurs en spouder in data-analyse. Fraudeurs kunnen zich terugtrekken in het niet te controleren gebied achter het ‘scherm van de privacy’, aldus de fideo-onderzoekers.

‘Het is overduidelijk dat de behandeloor/indikator maar op zijn hoofd is. Dit door de anomalieën kunnen verschuiven naar andere behandelingen/verrichtingen/medicijnen is een fact of life. Hier mee is de wedloop tussen overtreders en zij die de detectie doen, geschikt.’

Voor vervolgstappen adviseert fideo dringend om in het database and 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 encryptie) is een slag die de onderzoekers willen maken om een compleet beeld van de behandelingen en kosten per verzekerde. Om nate gaan of zorg conform factuur is gele-

verd, moeten, aldus onderzoekers, verder onderzoek van databestanden, materiele controles en audits uitkomst bieden.

Zepieten echter niet voor grootschalige materiele controle en audits, maar selectief bij sterke fraudesignalen en merkwuurde gevallen. De administratieve problemen zijn zowat hinderlijk als behulpzaam. 'Het percentage correcte declaraties is hoog. Dat wijst niet alleen op een administratief proces dat beter kan, maar het bemoeit ook het opsporen van onregelmatigheden. Het goede nieuws is dat die zorgaanbieders die veel correctieboekingen indienen als vanzelf de aandacht op zich vestigen.'⁵⁰

nza: topje van de ijsberg

Den zal positief over dat mining als methode om mogelijke overtredingen en aanbieder afwijkingen van het gemiddelde op te sporen. Met daar kansen van de data-analyses kunnen verzekeraars hun controles verbeteren. Ook zal de naze data-analyse gebruiken voor prioritering in eigen toezicht.

Den zalst 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 declaratie op voorhand niet duidelijk of een aanbieder bewust onrechtmatig declareert.

Dit zijn nadere oorzaken dat de naze niet heeft gowogd aan het produceren van een 'zorgfraudecijfer' (percentage), zoals haar was verzocht van verschillende kanten. We zien s edis 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 betrouwbare wijze door te rekenen naar een totaal cijfer voor zorgfraude.⁵¹

Dit brengt de naze 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 fraudeurs: 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 geringe deel 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. Karsten, Dr. W.J. Koozelezyk en F. Kleyne, fd 55, 8 augustus 2014.
http://www.nzanl.nl/regelgeving/bijlagen/Biedrapport_Onregelmatigheden_in_declaratiebestanden_in_zorg_zorgaanbieders_FOEC/geraadpleegd%20januari%2015.
 Interview met Daan Molenaar van den za.

Privacy en medisch beroepsgeheim

Tenslotte veel beter zicht krijgen op de ruimtetussen behandelingen en declaraties zouden verzekeraars als Afdmeabaet hebben bij inzage in medischedossiers. 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 matierele en formele controles geldt ook dat in de regel eerst algemene controles moeten worden uitgevoerd voordat er datacontroles gedaan mogen worden. Verzekeraars zouden volgens denze echter effectiever kunnen zijn, als ze bij een standaardcontrole een steekproef nemen uit patiëntendossiers. Zo sporen zij eerder (vermoedene en onvermoede) fraude en frauderisico's op en kunnen zij hun controlelaak beter uitvoeren.

Behalve op privacy (van patiënten) sluit het uit te sluiten met in zage in medische dossiers ook op het medisch beroepsgeheim. Dit moet volgens denze niet ter discussie staan.

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

Ruimere regelgeving

Denze vroeg het ministerie van vws om een verkenning of het mogelijk en wettelijk 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 denze, zijn zorgverzekeraars is vastgesteld dat het wettelijk mogelijk maken van steekproeven weinig oavolgt aan bestaande methoden van opsporing van fraude. Zorgverzekeraars zouden dat steekproeven zonder vormoeden 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 tenslotte vermoedens van fraude te checken. Declaraties verschaffen al informatie over medische handelingen.

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

52 Interview met Barry Egberts en Rob Konijn van Afdmeaba.

53 Samen vat tend rapport: 'Onderzoek naar kwetsbaarheden en financiële onregelmatigheden in de zorg', nza, november 2014. https://www.nza.nl/104107/188040/2_Samen_vat_tend_rapport/Onderzoek_naar_kwetsbaarheden_en_financiële_onregelmatigheden_in_de_zorg.pdf (geraadpleegd 22 januari 2016).

gelegd met betrekking tot de controle door zorgverzekers [...] Er zijn nog voldoende mogelijkheden, waar zorgverzekers 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 fraudebestrijding een no-go area.

Den zacht anders geadviseerd en reageert: "Steekproeven zijn nodig om verder te kunnen gaan dan met de protocollen voor gebruik van medische gegevens mogelijk is. Hoek om je er immers achter vast te zetten is? De Belattingpiens: doet dat ook."⁵⁵

Hulp van patiënten

Den zacht 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 aanbieder, terwijl mijns inziens de discussie een norm zouden moeten gaan over de privacy van de patiënt."⁵⁶

Zo ontvangt den zacht nodigtijde van patiënten over verduidelijking van levensverklaringen, bijvoorbeeld van niet-ondergaane behandelingen of door namen van artsen die niet gezien zijn.

In onderzoek krijgen we al medische informatie, industriele inzage in de medische informatie. Vervolgens beroept de zorgaanbieder zich op het medisch beroepsgeheim om controle tegen te houden. Dat vinden wij een nader verduidelijking van het recht op medisch beroepsgeheim. Het gaat toch om de bescherming van de patiënt."

Overigens kan hier de data-analyse in de declaratiebanden wel soelaas bieden. Dat trad naar voren met de zorgfraude die snel "oorsmeer-gateling" heten. In het ZorgBoom zieleenhuis in Tonnouzen bracht een kno arts 1066 euro in rekening voor een paar minuten oorsmeer verwijderen. Daaropging den zacht de voorbehandelingen over de afgelopen jaren analyseer.

"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 den zacht belangrijk om aan te geven dat zij dat aardyssoort nodat deze dubbel gepseudonimiseerd zijn; dus dieniet tot individuele personen te her-

54 Voortgang programma Rechtmatige Zorg 2016, minister van vws, 25 oktober 2016 <http://www.tweedekamer.nl/kamerstukken/detail?id=2016D410676&id=2016D41067>

55 Interview met Daan Molenaar van nza.

56 Interview met Daan Molenaar van den za.

57 Idem.

leiden is voor degenen die de analyse doen (wel terug te leiden in een eventuele later fase, zie hoofdstuk over I s i en B y t i).

Mochten verzekeraars dossiers inzien, dan nog is het de vraag of dit die 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 n z s: "W e nemen bij de interpretatie van de uitkomsten van onze toetsen aan dat het geen is geregistreerd gelijk is aan de werkelijkheid [...] van onze toetsen en de conclusies die erdaaruit 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 uitloof van de rekening. Die kan bij inzage in de facturen (schillen) te beperken of genoemde behandelingen inderdaad zijn verricht.⁵⁹

Weggeving voor vernieuwing dat opvoeding

Ten einde onder meer de intensivering samenwerking in fraudebestrijding mogelijk te maken, heeft de minister van v w s het wetsvoorstel Verbetering Toezicht en Opvoeding (v t o) als onderdeel van de Wet mark toeding 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 gediende toezeggingen wordt ingebast. Het wetsvoorstel voorziet onder meer:

- in het bieden van overzichten over notiss, eigen r i s i c o en eigen betaal
- bestuurrechtelijk optreden tegen notiss voor niet geleverde zorg (ij notiss);
- handhavingsbesluiten (aanwijzingen en bestuurlijke sancties) open te maken, ook als deze zijn opgevolgd;
- een last onder dwangsom op te leggen bij aan wijking met de wijk toezichtonderzoek van de zorgautoriteit.

Een van de belangrijkste onderdelen betreft de wettelijke verantwoording 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 toegestaan bij de doorvoering. In het kader van de verstrekte onderzoeksopdracht voerde het te ver om hier in

⁵⁸ Idem.

⁵⁹ Samen vattend rapport Onderzoek naar i w e t s b a a n h e d e n en f i n a n c i e n r e g e l m a t i g h e d e n i n d e z o r g, n z a, november 2014, https://www.nzan.nl/104107/138040/2_Samen_vattend_rapport_Onderzoek_naar_koretsbaanheden_en_financieregelmahgheden_in_de_zorg.pdf (peradpleegd 22 januari 2018).

extensie op in te gaan industriele politieke behandeling. Dat laat onverlet dat dit onderwerp industriele wetgeving bij groeiende medische (factuur)data uitwisseling openbare aandacht behoeft.⁸⁰

De afwegingen aangaande privacy in verandering van wetgeving op dit terrein zijn niet of nauwelijks in de openbaarheid gekomen. Dat is gerelateerd tot, in figuratieve 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 overheidsinstellingen [...] De verzekeraars en informatiewordt uitgevisseld, kan via wet- en regelgeving en de polisvoorwaarden van de verzekering kennismaken van het feit dat zijn persoonsgegevens, onder strikte randvoorwaarden, worden uitgevisseld [...] In specifieke situaties [...] zoals in de geestelijke gezondheidszorg, is aanvullend gespecificeerd dat verzekeraars 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 uitgevisseld."

In de Tweede Kamer zijn amendementen ingediend door de K-leden Leijten en Van Gerven om te voorkomen dat ziektekostenverzekeraars nieuwe bevoegdheden krijgen tot in zage in de medische persoonsgegevens van verzekerden, evenals voor het beheer van het medisch beroepsregister. Ook de Autoriteit Persoonsgegevens en de Raad van State hebben kritieken ingediend bij het voorstel. Daarop heeft de minister van VWS een notitie van wijzigingen ingediend.⁸¹

Zorgaanbieders anticipeeren

Zoals fidac opmerkte, wordt het traceren van onregelmatig declaratiegedrag moeilijk waar zorgverleners anticipeeren op ontdekking. Zo gingen fysiotherapeuten

80 Wijziging van de Wet marktordening gezondheidszorg en enkele andere wetten in verband met het verbeteren van toezicht, opsporing, naleving en handhaving. Nr. 5 Memorie Van Toelichting, Kamerstuk 33960 Nr. 3 Vergaderjaar 2013-2014

<http://zoek.officielebekendmakingen.nl/dossier/33960/kat-33960-3>

81 Wijziging van de Wet marktordening gezondheidszorg en enkele andere wetten in verband met het verbeteren van toezicht, opsporing, naleving en handhaving. Nr. 5 Memorie Van Toelichting, Kamerstuk 33960 Nr. 3 Vergaderjaar 2013-2014

<http://zoek.officielebekendmakingen.nl/dossier/33960/kat-33960-3>

(geraadpleegd 24 januari 2015).

Aanbieding nota bij wetsvoorstel wijziging marktordening gezondheidszorg

<http://www.rijksoverheid.nl/documenten/kamerstukken/2015/09/16/aanbieding-nota-bij-wetsvoorstel-wijziging-marktordening-gezondheidszorg>

(geraadpleegd 24 januari 2015).

Nota van Wijziging, 33960-9, 18 september 2015, E.J. Schippers, minister van Volksgezond-

heid, Welzijn en Sport

<http://www.tweedekamer.nl/kamerstukken/detail?id=2015034401> (geraadpleegd

24 januari 2015).

die werden aangesproken vanwege declaraties op twee of meer opeenvolgende dagen, maar dagen tussen de declaraties agenderen.

Ook zien verzekeraars dat zorgverleners declaraties indienen zonder namen van behandelde patiënten. In dat geval zijn patronen per behandelaar niet te analyseren en afwijkingen moeilijker te traceren. Zo kunnen gestolde zorgverleners ervoor om de specificatie van behandelingen niet te vermelden, met een beroep op de privacy. Verzekeraars wensen juist inzicht om de redelijkheid van de zelfdoelmatigheid van declaraties te kunnen vaststellen.

Ondanks het feit dat zorgverzekeraars – net als de Belastingdienst – vooroplopen met fraudebestrijding door data-analyses hebben ook zij soms discussie over het onderscheid privacy. ‘Zoveel juristen, zoveel meningen.’⁶²

Tokentatiegevoelensdoelgebruik

‘We bevinden ons in een wankel evenwicht: enerzijds horen we vaak dat het schandig is dat het medisch beroepsgeheim op de proef wordt gesteld, maar op hetzelfde moment wordt er geuit dat het schandig is dat verzekeraars niet beter controleren tegen fraude, aldus denzaker des paaat tussen regelgeving enerzijds en maatschappelijke druk anderzijds, waarvoor de politiek afwisselend argumenten haartert.

Juist deze behelbelangen 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 gechieden houden van die discussie 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 ruimte zijn dan nu.

En daar vervolgens ver antwoordend 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: divergentie van 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 verzekeraar nodig. En dan controleert de protocollen.

Dit is geen ideale situatie, vinden dan zien de verzekeraars, zelf heeft geadviseerd om een opsporingsdienst in de zorg op te richten. Die zou ver moeten kunnen gaan met bijvoorbeeld inzet van steekproeven bij verduidelijkingen die voortvloeiën uit tips van patiënten of signalen uit data-analyse.

Ik denk dat dan zal altyd want om onregelmatigheden op te sporen, zijn dubbel geanonimiseerd, zodat ze niet herleidbaar zijn tot de patiënt, maar wel tot de zorgverlener. Ze kan de naam van de patiënt wel terughalen in specifieke verden-

⁶² Interview Barry Egberts en Rob Konijn, Adma.

elingen van aanbieders. Bij den za vindt discussieplaats over mogelijk systemen met gebruik van patiëntdossiers voor controle zonder privacyrisico's.

Koppeling van hele bestanden van dossiers is onhaalbaar. Ziekenhuizen hebben volgens Achmea wel mogelijk heden om op grootschaal behandelingen te vergelijken met declaraties, in dit geval de uitgaande declaraties. Ook worden mogelijk heden 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 declaraties zijn gedeeltelijk weliswaar 'lief', maar onder meer de fideo-onderzoeken toonden aan dat dit op zich onvoldoende is om de groot gezondheidszorg fraude 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 den za is het vooralsnog voldoende als verzekeraars en toezichthouders analyses draaien op eigen data. Wel kunnen ze dan signalen samenbrengen, in een vervolgpunt het te overwegen is.

Het bundelen van bestanden binnen de zorg en met derde partijen is nu niet nodig. Eerst is het zaak dat den za, ligz en verzekeraars hun signalen (vondstingen) delen. Een mogelijkheid is het opkopen voor een opt-in-systeem: bij uitdrukkelijke toestemming door patiënten zou inzage mogelijk moeten zijn. Dat sluit echter op bezwaren van zorgverleners.

'Welkomen louter uit dit dilemma door burgers de eigenaar te maken van hun eigen zorgdossiers. Zij bepalen dan wanneer en voor welke doeleinden inzage in de data krijgt, en voor hoelang'⁴⁹

4

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 klf (on)juiste aangiften, wanbetaling] van het koren te schieden. Dat begon met een experimentele eenheid: "brockamer".

Deze aanpak slaagde en werd dienom voor de gehele dienst: van apart functionerende e-mail-systemen naar een data-gedreven netwerk van applicaties.

Risicoanalyse leidt tot selectie van verdacht(e) 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 socialedomein als in de strafrechtelijke opsporingen bestrijding van zorgfraude spelen gegevens over inkomens en vermogen een steeds belangrijere rol.

In dit hoofdstuk passeert een groot aantal voorbeelden van dataprojecten met inzet van data-analyse door de Belastingdienst der ere. 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 beoekstaafd door de Belastingdienst (Bd) en partners in fraudebestrijding?

4.1

innovatie in data-analy

Megadatabase

De Belastingdienst bezit de grootste hoeveelheid data over personen in Nederland:

- 11 miljoen burgers die aangifte inkomstenbelasting doen.
- 1,5 miljoen ondernemers, vaak dezelfde personen (zelfstandigen).
- 8 procent van alle bank- en girotransacties in Nederland, oftewel 1 miljoen transacties per dag.

Dit grote datahuis, aangevuld met uitkomsten van verschillende staekproeven, vormt de basis voor het vaststellen van "inlevingsgeleken" 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 daar in patronen herkenbaar die nadere aandacht vragen voor controle en eventueel correctie?

Bijna drie jaar werkt de Belastingdienst met een aparte eenheid Business Intelligence Analytics (bi& a). De afdeling is opgericht om inzicht in uit data te genereren. In een interne 'inubador' ('broedkamer') worden deze inzichten omgezet in nieuwe werkwijzen voor de operatie.

De innovatieve analytische producten die op kort- en middellange termijn worden ontwikkeld en ingevoerd, moeten het werk van de medewerkers van de Belastingdienst efficiënter, efficiënter en makkelijker maken. Inmiddels draaieert s, veelal jonge creatieve economen, meest wijs- en natuurkundigen en econometristen, storten zich op de analyse van de enorme data berg van de Belastingdienst.

De nieuwe eenheid moet gaan bijhouden een kostenverlagings opbrengst stijging, met krachtige slagen gericht op een maximaal resultaat. Centraal staat het observeren met een frisse blik van de vaak al decennialoed 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.^{16,17}

Werkwijze Broedkamer

bi& a werkt met 'lekkerende' modellen die steeds verfijnder aangerekenen waar zich risico's bevinden op grond van eerder geregistreerde aangiften en terugkoppeling van resultaten. Risico modellen worden steeds verfijnd en geactualiseerd met praktijk uitkomsten 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 indicatie die duiden op mogelijke zwakte, systematische fraude, met bijvoorbeeld netwerken van bv's en stichtingen.

De Belastingdienst werkt met een nauwgezte methodiek om ruwe data op te werken naar informatie en vervolgens inzichten, die vertaald worden in analyse producten. Deze methodiek kent verschillende stadia, waaronder:

verzameling van ruwe data van alle transacties en aangiften via vator ge

voor benadering van data;

- risicom- en waardeanalyse;
- segmentatie
- identificatie;

- outminnerend in een dashboard waarop de aantal verschillende soorten kan filteren en combineren.

Zoals in alle fraudebestrijding ontstaat ook bij risicoslectie respons in de vorm van geïncultuurd gedrag van fraudeurs in een kant-en-misplid. De fraudeur tracht onder de radar te blijven met pogingen der risico-indicatoren van de dienst te onderkennen.

Modellen zullen daarom "bijgetraind" moeten worden door steekproeven waarmee "nieuw gedrag" wordt ondankend 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 kwaliteitsontwikkeling al snel jaren in beslag nemen, met de inmiddels van lotprojecten bij de overheid bekende pieken en (vooral) dalen.

Zwakke leedzaamheid voor sluiting door il. De leiding van de werkveld is als startpunt van dataprojecten de grootste kans op falen biedt. Bij deze interne Broedkamer van Data&Analyse lopen verschillende projecten tegelijkertijd, tegen lage kosten.

In het eerste van onze vraggesprekken met de Belastingdienst⁵⁵ werd een periode van een maand genoemd waar in de investering in datapactiteit en onderstaandend lot zou worden terugverdiend met bestrijding van fraude en (andere) onjuiste aangiften en -gedrag. Zok onder projecten van de Broedkamer ook snel worden beëindigd bij gebrek aan resultaat. In tegenstellingen tot traditionele it-projecten, die zoals bekend uit departementaire enquête vaak in drama's eindigen.

De focus ligt op informatieprojecten zonder de wens tot verbouwing van grote transactieprocessen. Gevolg is dat de slagkans van projecten ten opzichte van de oude situatie flink was toegenomen, mede dankzij eenvoudiger lot. Benodigde software voor data-analyse is standaard in de markt voorhanden. De resultaten zijn in een webbrowser te delen.⁵⁶

Resultaatmeting

De taak van de eenheid bi & a is breder geformuleerd dan louter in termen van handhaving en fraudebestrijding. De vijf t.w.v. 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 fraude mogelijkheden (loon, auto's, vastgoed, etc.) ontstaan bij openbare 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 Incasso centrum, die de vorderingen van particulieren afhandelen.
- De succesratio van loonbeslag steeg met een factor twee, terwijl tegelijk de tijd benodigd voor het afhandelen van een loonbeslag halveerde. Van minder belastingplichtigen werden onnodig heiliggewallen, waardoor deze Big Data toepassing ook de nationale stressfactor verlaagt.
Inkomstenbelasting (ib) is dankzij de inzet van data analyse een vooroplopende modellering de hit rate, het aantal gecontroleerde aangiften die correctie behoeven, significant verhoogd. Met de resultaten worden nieuwe analyses gevoerd, die tot steeds hogere succesratio's leiden, of schoon maar een afnemende stijging.
- Op grond van data-analyse is de selectie van te controleren bedrijven die terugvragen, veel scherper geworden. Met hetzelfde aantal ambtenaren is de slagings van btw correcties meer dan verdubbeld.
- De bestrijding van carroussel fraude en multi taal fraude is dank zij netwerk ses veel effectiever geworden. Door het voortdurend monitoren van alle handelsrelaties tussen bedrijven en stichtingen worden mogelijk carroussel fraudes eerder en veel omvangrijker dan voorheen gespot en beëindigd. Inmiddels zijn, mede op grond van terugkoppeling van ervaringen, 60 patronen ontwikkeld die uit de grote bestanden relaties van maldiezen netwerk organisaties in beeld brengen. Ook deze modellen worden voortdurend 'getrind' op grond van uitkomsten en verder geperfectioneerd.
- Door het de interne data nu op methodische wijze zijn georganiseerd, is later antwoord gegeven worden op actuele vragen, bijvoorbeeld bij beantwoording van Kamer vragen. Bij de gecorende Bulgari fraude met loonlagen was dank zij deze afdeling binnen 24 uur het mogelijke schade bedrag bekend: 95,2 miljoen euro. En konden transacties onmiddellijk worden gestaakt.

- Ook bij ~~de aanpak~~ ~~met~~ een enkele uren nadat minister Plasterk besloot om vermissingen als overlijden te behandelen, deschudenposties van slachtoffers bekend en kon het verzenden van 'blauwe enveloppen' op hun naam worden gestakt.
- 2014 is ~~de~~ ~~Belastingdienst~~ ~~onregelmatigheden met 50.000 aangiften, met 100 miljoen euro aan valseteruggaveclaims. Daarvan is 80 miljoen niet uitgekeerd, de overige 20 miljoen later teruggevoerd.~~
- 2014 is ~~de~~ ~~Belastingdienst~~ ~~adviseur uit Overijssel veroordeeld, omdat hij bijna 2000 vals 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 160.000 euro mee verdiend. Data-analyseonderzoekers leverden een relevante bijdrage aan de opsporing.~~
- 2014 zijn 100 wilksa onderzoekers afgevoerd, waar van het Courantvaluit Bestag 310 miljoen euro bedroeg⁶⁷.
- 2014 ~~de~~ ~~Belastingdienst~~ ~~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 besteedt het Combiteam ~~aanpak~~ ~~Facilitators~~ (gestructureerd gebruik van belastingprocedures dan wel toelagen). Het team heeft in het 100 bestag van ongeveer 15 jaar direct eenhonderd zaken opgepakt. Vervolginschort daarbij.

Begin mei 2018 maakte de Belastingdienst bekend dat het oaf vanuit data-analyse honderd belastingadviseurs met hun 75.000 klanten in het veld kwamen die voor meer dan 400 miljoen euro aan onterechte aftrekposten hadden gedaald. Met 70 adviseurs is een schikking getroffen en 21 worden er voor de rechter gebracht.

- De Belastingdienst schonk extra aandacht aan de algemeen nut beoogde instelling (anbi). Er bleek een groot aantal anbi's te zijn, zo'n 60.000, met geringe fiscale aandacht. De Belastingdienst stelde twee honderd extra boekenonderzoek in. De resultaten leveren data op voor permanente analyse voor handhaving als mede aanbevelingen voor wet- en regelgeving.
- De douane pak ook meer en meer data-analyse toe voor de selectie van te controleren zendingen. De intelligentie functies van groot belang bij de analyse van risico's en voor de keuze voor instrumenten voor handhaving. Dit is bij-

voorbeeld toegepast bij de aanpak van kleding en schoenen die eren een te laag waarde worden aangegeven, voor ontduiking van douanerechten.⁶⁸

Uiteraard meent de dienst bij voorkeur de successen. Maar projecten leveren soms niet het gewenste resultaat op, waarvoor juilt met de korte doorlooptijd dan ook alle ruimte is. Bijturen 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 genoemde criteria (opbrengst, procesbeheer, etc.). Als een idee/innovatie onvoldoende scoort, wordt de ontwikkeling stopgezet.

De gedragsrichtlijnen:

- Commitment vanuit het topmanagement is cruciaal. Dit evert het benoemde draagvlak en versnelt besluitvorming en ontwikkeling.
- Niet teveel ideeën en innovaties tegelijkertijd ter hand nemen. Alleen ideeën, met het grootste effect, gaan door.⁶⁹

4.2 samenwerkingverbanden

Alletwintigconvenanten

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

⁶⁸ Halja rapportage Belastingdienst, 26 maart 2016: http://www.twedekamer.nl/kamerstukken/brieven_gesprek/detal?id=2016201518&di=2016201162

⁶⁹ Halja rapportage van de Belastingdienst, 16 september 2016: <http://www.rijksoverheid.nl/documenten/kamerstukken/2016/09/16/halja-rapportage-van-de-belastingdienst>

⁷⁰ Interview met Cyprian Smits van de Belastingdienst.

[http://www.belastingdienst.nl/wps/wcm/connect/bl/docenten/twintigbelastingdienst/midiana/loosch/20/convenanten/convenanten_mit_afnemers_van_informatie_\(laatst_geraadpleegd_8_februari_2016\).](http://www.belastingdienst.nl/wps/wcm/connect/bl/docenten/twintigbelastingdienst/midiana/loosch/20/convenanten/convenanten_mit_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. Centrale Administratieve Afdeling (caak), 2011
Uitwisseling: 'Authentieke Inkomensgegevens'
Doel: controle op de hoogte van eigen bijdragen in de zorg voor handhaving Wmo, aw-bz en Wet Tegemoetkoming Chronisch Ziekten en Gehandicapten.⁷²
3. Centrale Justitieel Incassobureau (cijb), 2016
Uitwisseling: de Belastingdienst levert fiscale informatie, het cijb verstrekt informatie benodigd voor de belastingheffing.
Doel: de uitvoering wettelijke cijb-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 aw-bz; eveneens inzake invroedelingen, arbeidsloze, relatieve overleving en zelfstandigen, niet ingesloten zelfstandigen, gemoedsbezwaarden.⁷⁴
5. d.g. Fiscale Zaken, 2015
Uitwisseling: toegang van de Afdeling afp/Analyse tot data over tien verschillende, apart benoemde vormen van belastingen, in de niet-omgeving van de Belastingdienst. Productie analysebestanden in de niet-omgeving van de Belastingdienst. Overzetten geaggregeerde resultaten van analyses naar Ministerie van Financiën.
Doel: analyse van behoefte van ontwikkeling van fiscaal beleid.⁷⁵

⁷¹ http://www.belastingdienst.nl/wps/wcm/connect/bldcontent/nl/themas/verslagend/brochure_en_publicaties/convenant_mai_arbeidsomstandigheden_doeel/convenant_arbeidsmarkt

⁷² http://www.belastingdienst.nl/wps/wcm/connect/bldcontent/nl/themas/verslagend/brochure_en_publicaties/convenant_belastingdienst_cak

⁷³ http://www.belastingdienst.nl/wps/wcm/connect/bldcontent/nl/themas/verslagend/brochure_en_publicaties/convenant_belastingdienst_centraal_justitieel_incassobureau

⁷⁴ http://www.belastingdienst.nl/wps/wcm/connect/bldcontent/nl/themas/verslagend/brochure_en_publicaties/convenant_belastingdienst_college_voor_zorgverzekeringen_cvz

⁷⁵ http://www.belastingdienst.nl/wps/wcm/connect/bldcontent/nl/themas/verslagend/brochure_en_publicaties/convenant_belastingdienst_dircoraat_generaal_fiscale_zaken

6. Financie Expertise Centrum, 2014
Uitwisseling structurele data over straffelijke samenwerking van Autoriteit Financiële Markten (afm), de Belastingdienst, De Nederlandse Bank, Financiële 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.⁷⁵
7. ICov (Crimineel en Oververtelbaar Vermogen), 2013
Uitwisseling: bestanden Bld (inclusief bld), Douane, Looslagen), om, Politie en B.
Doel: 'oververtelbaar' vermogen en witwassen fraudeurs om uit te 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, u.w.v. (polisadministratie), desvb, het om, gemeenten (vng), Divosa (sociale diensten) departementen Financien en z.w.⁷⁸
Doel: teruggangen belasting-, premie- en uitkeringen fraude en misstanden op de arbeidsmarkt en samenhangend overdraafroding. Permanente werkgroep. Informatieanalyse, geleid door de Inspectie z.w., voor ondersteuning tegen regionale platformen bij keuzen bepaling van projecten voor interventie.
9. Kansspelautoriteit, 2013
Uitwisseling: deksa verschaft bedrijfsgegevens, de Belastingdienst signalen van mogelijk illegaal aanbod van kansspelen en gegevens inzake cases die mogelijk van belang zijn voor k.z.o.
Doel: heffing, inning, toezicht en handhaving van de kentak en van beide partijen. Gericht op aanbod van diensten, niet op spelers.⁷⁹

76 http://www.belastingdienst.nl/wps/wcm/connect/bl/conten/nl/thema/verlrijdend/brochures_en_publicaties/convenant_houdende_afspraken_over_de_samenwerking_in_het_kader_van_het_financieel_expertise_centrum

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

78 http://www.belastingdienst.nl/wps/wcm/connect/bl/conten/nl/thema/verlrijdend/brochures_en_publicaties/belastingdienst_interventieteams

79 http://www.belastingdienst.nl/wps/wcm/connect/bl/conten/nl/thema/verlrijdend/brochures_en_publicaties/convenant_mel_de_kansspelautoriteit

10. **Illece / r i e c** (Landelijke Regionale Informatie- en Expertise Centra) 2012
 Uitwisseling: informatie tussen ministerie Van de politie, burgemeesters, hof om de politie, de Delictendienst (ind. Douane, B d), Inspecties w , provincies, de Marechaussee en de ind. Onder meer structurele inbreng politiedata op grond van de Wet politiegereguleerders (Wpg). De samenwerking staat open voor andere belanghebbenden.
 Doel: ompr van ondermijnende criminaliteit (zoals mensenhandel, hennepcultuur, 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 eerder overeenkomsten)
 Uitwisseling: Openbare Doelinstellingen, Landelijke Landbouw en Transport.
 Doel: verhoging van de doeltreffendheid en doelmatigheid van beleidshandhavingen, dat wil zeggen nauwe samenwerking bij controles.⁸¹
12. Ministerie van Justitie (rittenadministratie)
 Uitwisseling: irrelevant in kader dit onderzoek.
 Doel: komt naar opschaffing van verplichte rittenadministratie voor het aanhouden van beperkte rijbewijzen.⁸²
13. Ministerie van Oor, verlenging 2015
 Uitwisseling: informatie over detectie, beoordeling, analyse en nader onderzoek van risicovolle vastgoedtransacties uitwisselen, met name over ereditssperren en hun bestuurders actief in het onderzoek.
 Doel: misbruik, ongelukkig gebruik en het ondoelmatig van vastgoed tegen gaan en mogelijke overtredingen van en subsidie regeling Praktijk leren in kaart brengen, te beperken en te bestraffen.⁸³

80 http://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/themasverijgend/brochure_en_publicatie/convenant_belastingdienst_het_ministerie_van_de_politie_burgemeesters_korpsbeheerders_en_lokale_besturen
 Zie ook www.riec.nl/

81 http://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/themasverijgend/brochure_en_publicatie/convenant_milieu_het_ministerie_van_infrastructuur_en_milieu

82 http://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/themasverijgend/brochure_en_publicatie/convenant_belastingdienst_rittenadministratie_dienst_voor_tuigen_politie

83 http://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/themasverijgend/brochure_en_publicatie/convenant_milieu_het_ministerie_van_oor_wijze_cultuur_en_wetenschap_oor

94. Ministerie van oew/jr/ Dienst Uitvoering Onderwijs (duo), 2018

Uitwisseling: Duo levert structureel geverifieerde bsn-nummers met geboortedata aan bij de Belastingdienst die deze 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 indientolaanvragen van data geeft de Belastingdienst de rechtmatigheid na. duo levert jaarlijks aan de Belastingdienst data over studiefinanciering, zowel subsidie als leningen. Doel: oorspronkelijk gebruik van studiefinanciering toegangen en handhaving belastingplichten.⁸⁴

95. Kamer van Koophandel, 2010

Uitwisseling: in principe geen uitwisseling van belastingen of data voor fraudebestrijding. Doel: samenwerking bij inschrijvingen om lastendruk te verminderen. KvK geeft r/s n-nummers (fiscaalnummers) uit en meldt die terug aan de Belastingdienst.⁸⁵

96. Nederlandse Mededingingsautoriteit, 2007

Uitwisseling: data van ministerie de Belastingdienst, verkregen uit uitoefening van de Mededingingswet; eventuele tips over en weer over mogelijk strafbare feiten. Geen grootschalige data uitwisseling voor risicosegnalen. Doel: handhaving Kansspelwet en Belastingplichten.⁸⁶

97. Openbaar Ministerie, 2008, Convenant Gegevensuitwisseling Aanpak Vastgoed

Uitwisseling: de Belastingdienst en de FIOD verschaffen belastingdata het om (en politie) strafvorderlijk edata en KvK data. Ook uitgedeelde 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 uitbreiden 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/blcontent/tl/themaverstijgend/brochures_en_publicaties/convenant_mel_met_ministerie_van_ondereis_outuur_en_vereniging_oew_dienst_uitvoering_ondereis

85 http://www.belastingdienst.nl/wps/wcm/connect/blcontent/tl/themaverstijgend/brochures_en_publicaties/belastingdienst_kv

86 http://www.belastingdienst.nl/wps/wcm/connect/blcontent/tl/themaverstijgend/brochures_en_publicaties/convenant_belastingdienst_nederlandse_mededingingautoriteit_nma

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

17. Politie 2014

Uitwisseling van de Politie betreft de Belastingdienst realtime alle gefotografeerde kentekens van de tweehonderd mobiele en vaste (anpr-) politiekameras op de Nederlandse hoofdverkeersaders. Dit is het totale bestand met miljoenen kentekens, onafhankelijk of er een verdienking is. De Belastingdienst beroept zich hierop op Art. 11 van de Belastingwet (Awr), dat wil zeggen op 'de autonomie van de Inspecteur om op basis van de hem bekend(e) ten/ waarnemingen een aanslag op te leggen'.

Doel: de Belastingdienst wendt de data aan voor bepaling van privégebruik van zakelijke auto's en handhavingen (controle inzake, motorrijtuigenbelasting, vennootschapsbelasting en zware voertuigen (Eurovignet).

(De controller looft 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 'database auto'.

Belastingplichtigen hebben recht op informatie over opgeslagen data en hoe hun aanslagen zijn gekoppeld en kunnen daar een beroep op doen. Dit worden vervolgens als ze niet relevant meer zijn. Minimaal eenmaal per jaar wordt de database 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 gegevens van ondernemers over hun aanligte en betaaldedag bij de Belastingdienst. Gezocht naar de 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/thermaoverslaggen/brochure_an_publicatie_convenant_gegevensbelasting_aanpak_vastgoed

⁸⁸ Convenant http://download.belastingdienst.nl/belastingdienst/doc/convenant_belastingdienst_politie_anpr_20142015.pdf
Protocol Convenant Belastingdienst met de Politie betreffende anpr-camera's, versie 2.0 van 7 jan van 2016
http://download.belastingdienst.nl/belastingdienst/doc/protocol_convenant_belastingdienst_politie_anpr_20142015.pdf

Deze snedelijke data-uitwisseling is in het kader van dit onderzoek irrelevant.⁸⁹

9. Team Track van het ministerie van VenJ 2013

Uitwisseling met Team Track (onderzoek dienst Justis van VenJ) wisselt de Belastingdienst sinds begin 2010 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 carouselfraude. 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: uitwisseling van de Wk en kriterieën op rechtspersonen.⁹⁰

Kenmerken:

- In alle convenanten zijn bepalingen opgenomen voor doobinding, geheimhouding (beveiliging) en vaak ook betrokkenheid van privacy-officers
- Alle convenanten kennen een stilzwijgende verlenging. Ook wordt er vaker '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's een convenant aangegeven. 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, bod, c n b, B en af m, stond in de Staatscourant. Maar deze ging evenmin als de convenanten langs het parlement.

Het gezamenlijke doel van de factopartners is het voortduren van de integriteit van de financiële sector. Voor verantwoordingen 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/wa_/content/bldoenten/nl/themaverstijgend/brochures_en_publicaties/convenant_richtlijn_normering_arbeids_en_de_belastingdienst_met_betrokking_tot_de_gegevensuitwisseling_van_singel_en_belastingdrager

⁹⁰ http://download.belastingdienst.nl/belastingdienst/doc/convenant_uitvoering_wet_controle_op_rechtspersonen_20111116.pdf

⁹¹ Convenant houdend afspraken over de samenwerking in het kader van het Financieel Expertise Centrum (Convenant Fec 2014). Staatscourant, Jaargang 2014, Nr. 2351 <https://zoek.officielebekendmakingen.nl/stc-2014-2351.html>
fec-jaarverslag 2014 & fec-jaarplan 2015 <http://www.fec-partners.nl/nl/nieuws/nieuwsbericht/> 120

Samenwerkingen zonder convenant van de Belastingdienst

- Anti-Money Laundering (AML) is een multidisciplinair centrum op het gebied van witwasbestrijding. Deelnemers: b.d. en andere. Bijzondere Opsporingsdiensten, Financial Intelligence Unit (f.i.), politie en om.
- Landelijk Informatiecentrum Voertuigcriminaliteit (koppelt informatie van d.w., Nationale Politie, b.d., de stichting Verzekeringsbureau Voertuigcriminaliteit (vbv) en de Belastingdienst. Voor fraudebestrijding vindt ook data analyse en informatiecoördinatie met bescheiden plaats. Onder meer verzekeringsmaatschappijen maken hiervan gebruik.
- Er is ~~een~~ **een** ~~andere~~ **andere** Belastingdienst niet heeft getekend. De belastingdienst wisselt dan ook geen gegevens uit met de andere partijen.⁹²
- Ook kentaken van auto's van politie in gemeenten waarvoor geen p.b. betaald, worden door de Belastingdienst en de d.w. vergoeden met belastingen, 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 d.w., o.a., de Belastingdienst, u.w. en d.w.v. Ze richt zich op samenwerking en beleidsingetbreiding van dienstverlening. Vanuit de Manifestgroep begon in 2012 een poging tot oprichting van een gemeenschappelijk Expertisecentrum Fraude, waarin deze overheidsorganisaties samenwerken. De Belastingdienst was trekker. Andere partijen die aansloten waren:

- szw: Inspectie
- Immigratie- en Naturalisatiedienst (
- Dienst Uitvoering Onderwijs (
- Sociale Verzekeringsbank (
- Kamer van Koophandel;
- bbk/jus (ministerie
- Koninkrijk/Afzacheesee (
- Centraal Adresregister (antoor (
- Basisadministratie Persoonsgegevens en Rijdsdocumenten
- Rijksdienst voor ondernemend Nederland;
- u.w.v.;
- r.d.w.;
- n.v.k. Nationaal Vreemdelingen Informatie Knooppunt.

(Het laatste is een project van de Nationale Politie ter bevordering van het informatiegebruik en van de vreemde ingreep politie Nederland (nu: avim), een dubbel die de afgelopen jaren in veel samenwerking ingreep banden partideerde). Het Expertisecentrum begon met de ontwikkeling van gezamenlijke (stok)merken en -profielen. De beoogde opzet van het centrum bleef aan goed beeld van de ambities met gezamenlijke data analyse voor fraudebestrijding.

Doelen:

- productie van signalen waarmee fraudeurs kunnen worden geïdentificeerd en gepakt. Oftewel een *overheid/bredely warning system* zodat nieuwe fraudeurs sneller en completer in beeld komen;
- kennis over fraude en fraudebestrijding *plaatselijke body*, invordering) verspreiden en afstemmen.

Middelen:

- *pleitberisgoppging* te zetten. Beschrijf fraudeprofielen en daarna fraudeursprofielen met daaraan merken. Pas die toe, via idee en wissel het resultaat daarvan uit.
- Ook werd al geopperd om daar toe algoritmen op de totale populatie (beelden) los te laten, benadrukken hoe fraude benadrukken en deiding aan te brengen tussen groepen burgers en bedrijven met grote en kleine risico's op fraude.
- Het stimuleert de eenzijdige uitwisseling van kennis over fraude, intelligentie, privacywetgeving, van databank systemen (sas), data-analyse, van software, fraude opleidingen, profilering.

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

94

Mani fest-groep Fraude analyse—van overheid/brede bundeling van know how tot fraude-expertise centrum, presentatie Frans Bent van Belastingdienst, 25 april 2014 via Slideshare op 31 december 2015
<http://www.slideshare.net/Buzzlout/mani-festgroep-door-frans-bent-van>

Pilotprojecten:

1. dienst **Belastingdienst**: Ten behoeve van de in d zijn op bedrijfs-adressen eendagscontroles uitgevoerd door u.w.v en de Belastingdienst. De in d leverder is (ge)gevalen. KVK en de Belastingdienst vullen die aan met gegevens. Onder deze (ge)gevalen bevinden zich ook de met sanzen (ijk enale) vinge (el)orten bij meer d e overheden. Sommige controles zijn of worden daarom opgeschald.⁹⁵
2. De in d vroeg de Belastingdienst om onderzoek te doen naar de aanvraag van verblijfsvergunningen voor vijfthond Chinese koks. Is volgens de dienst een 'grote b d -zaak gewor den' met p d in p e de dienst betrek k inen.⁹⁶
3. Invordering van studieschulden. Duo heeft te mak en met een steeds vaker voorkomend fenomeen waar bij burgers d ieren studieschuld hebben zich uitschrijven uit de Gemeente (te b e ad m in i t a l e (y b e) en w a s v a n g a m s t e m e e r b e k e n d i s, d u o w o r d t g e h o l p e n b i j h e t v e r z a m e l e n v a n a d r e s s e n. I s d e b u s i n e s s e v o o r t g e z e t.
4. Buitenlands studenten: de in d (verblijfs)status en k m a r (i d e n t i t e i t e n w o o n p l a e t s) h e l p e n d u o i n t w i j f e l g e v a l e n o f b u i t e n l a n d s e s t u d e n t e n r e c h t h e b b e n o p e e n s t u d i e b e u r s. R e s u l t a a t : g r o o t a n t a l s t u d i e b e u r z e n z i j n i n g e t r o k k e n e n v a n (A n g o l e s e e n N i g e r i a n s e) j o n g e r e n z i j n d e v e r b l i j f s v e r g u n n i n g e n i n g e t r o k k e n.

Vervolgens kwamen er meer 'Antifraudprojecten':

- monitoring en analyse inkomend webverkeer;
- overheidsbrede veelplegers aanpak;
- Belastingdienst en Logius werken samen in misbruik DigiD voor fraude toelagen;
- 'Oriëntatie Rijdschalee' Hield h a v e n d e a c t i e s t a r t e n e n v r o e g d e B e l a s t i n g d i e n s t o m a d r e s s e n o m z e t g e g e v e n s v a n r i j s c h o l e n ;
B u l g a r s e o n d e r n o m d e r e t e d i g i d B e l a s t i n g d i e n s t o m t a c h t i g B u l g a r e n t e o n d e r z o e k e n , d i e a a n g a v e n e e n v o l t j e d o n d e r n e m i n g t e d r i j v e n ;
- In de haven van Rotterdam worden in het zogenoemde Regenboogt bestaande uit verschillende toezichthouders, risicoanalyses gedeeld, controle afgestemd en inspectieresultaten met elkaar uitgewisseld.⁹⁷ Zo ontstaan een gezamenlijk beeld van de goede en minder goede nalevers van de wet- en regelgeving in de Rotterdamse haven.⁹⁸

Maandelijkse monitoren van de originatie van de buitenlandse groepen en wordt kennelijk gedeeld over fraudeproblemen, maar geen data. De proefprojecten en definitieve

project en zijn immers niet uitgevoerd in een FraudeExpertisecentrum 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 pr

Manifestgroep twijfelt aan convenanten

Dit initiatief van de Manifestgroep verschaft 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 verspreiden van gegevens als probleem gezien. Volgens de deelnemers waren er drie drempels tot intensievere data-uitwisseling:

- de gemeentelijke aansluiting van de Belastingdienst,
- de huidige privacywetgeving,
- eu-verdrachten tegenover privacy.

Er bestaan tweehonderd convenanten – Kortom, een lappendeken⁹⁸, aldus de Belastingdienst.⁹⁹ Dus was de vraag opgeworpen of er één algemene regeling voor uitwisseling van data noodzakelijk was.

Dit is niet gekomen, in tegenstelling tot de Syrië-regeling voor opsporing van fraude in het sociale domein, waar voor de Belastingdienst overigens ook obstakels bestonden 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 voor 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 uitbreide aandacht aan borging van privacy, dat wil zeggen aan de vereisten om in theorie aan de regels van de Wbtp te voldoen. Zoals bijvoorbeeld voor de data die de risico en risico-hanteren. De stuurgroep ziet erop toe dat deze gegevens niet wordt vastgelegd in de Checklist Wbtp 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 Wbtp geactualiseerd en wordt de update opnieuw aangemeld bij het Autoriteit Persoonsgegevens.

Zaaijaar oud onderzoek

Er is pas lief noch actief toezicht van de Autoriteit Persoonsgegevens op de samenwerkingen. Op de site van de a.p. 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 'Registratiedienst') om controle op de verstrekking van persoonsgegevens door de fiscus, die verdegat dan nodig is voor de belastingheffing. De ap deed onderzoek naar het 'spanningsveld' tussen de datanogervan de dienst en privacybescherming. Ze stelde vast dat een adequate wettelijke grondslag en voldoende wettelijke waarborgen tegen ongewenst inbruiken op de privacy ontbraken.

Ze pleitte al voor:

- het vastleggen van de noodzaak van dataverstrekking in verband met schappelijke 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 datauitwisseling met de departijen.

Nu afgesproken van een afweging van de toen afgekeurde keurmerkingen voor dataovergave en uitwisseling: doelbinding (data alleen gebruiken voor het doel waarvoor ze zijn verzameld); subsidiariteit (slechts nodig); proportionaliteit (slechts gebruik). De ap vond dat dataovergave 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 Wvbo, 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 gelijk(e) behandeling. De dienst mag zich niet concentreren op bijvoorbeeld Oost-Europese, of nog nauwer, hier verblijvende aanvragers met een Bulgaars paspoort. Er moeten concrete veronderstellingen bestaan zonder discriminatie van een groep (op de vraag naar de verantwoordelijkheid wijst de Belastingdienst naar de adr). De openbaarheid van de rapporten van Auditdienst staat ter discussie. Er zijn Kamervragen over gesteld.¹⁰⁰

¹⁰⁰ Nummer 2016Z2586: Vragen van de leden Ronne en Omtzigt (beiden o.d.a.) aan de minister van Financiën, van VenJ, de staatssecretaris van Financiën en de minister van Defensie over de rapporten van de auditdienst rijk (ingezonden 30 december 2016). Beantwoording werd uitgegeeld <http://www.veedika.merit.nl/Kamerstukken/Kamervragen/detail?id=2016Z2586&did=2016D2188>

Koppeling met externe bestanden levert juridische vragen op. De dienst zegt terughoudend te zijn, en daarbij behalve de wettelijke grenzen, ook die grenzen van maatschappelijk 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 bezet 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 tegen en het programma is inmiddels stopgezet. Dat was een zelfstandig besluit zonder politiek inbreng of controle.

In een vraaggesprek antwoordde de directeur op vragen over ongebreidelde datagebruik: 'Redes om die reden heb ik een veiligheidsventiel ingebouwd. Wij gebruiken voor het opstellen van risico-profielen alleen gegevens die wij 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 spoorwerk. Zelfsonderzoek of afdelingen met eigen spoorbevoegdheid zoals het Internet Service Centrum.

- Op de vraag naar bewaartijd van gecombineerde bestanden en in de Belastingdienst dat ze zich houdt aan de regels van de Archiefwet. De archiefwet kent geen privacy principes. De gegevens mogen zo lang bewaard worden als fiscaal relevant wordt geacht, wat een periode van zeker vijf jaar kan belopen, maar ook zeventien jaar.

- De *Gesamenlijke* adviseur van de professor Theo de Roos. Guido de Bont en Gerrit-Jan Zwanezicht inkritische termen over de mogelijkheden voor de Belastingdienst om bestanden en op de (gerechte) persoon gerichte inlichtingen van andere partijen te betrekken en om eigen data te verspreken aan derden.

'We hebben een monster gaarbord', 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://de correspondent.nl/2015/04/21/Belastingdienst-over-Big-Data-Mijn-missie-is-gedragsverandering/> 8355320-10678aaf

In die vraaggesprekken voor dit onderzoek gezien als een draadschrift voor data voor fraudebestrijding.

Het Des uit suw i maakt verdergaande uitwisseling mogelijk. Zo mag de Belastingdienst meer externe koppelingen maken die nodig zijn voor risicoprofiling.

Zwenne stelt dat wetgeving onvoldoende is toegesneden op de grenzeloze mogelijk heden om op bestanden data-analyse toe te passen voor risicobepaling, patroonherkenning en uiteindelijk profilering van personen en bedrijven die lang meegaat.

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 wetgeving ook paalen en perk worden gesteld aan 'data-voorzieningen' van de Belastingdienst en de samenwerkingsverbanden waar ze despijt vormt.¹⁰³

- De Algemene Rekenkamer en Auditdienst Rijk waren kritisch over de afbeveiliging van data en systemen van de Belastingdienst op onderdelen. De dienst vormt een single point of failure, een groeiend risico voor privacy-schending bij systeemlekken.¹⁰⁴

Ook de bevoegdheden van vaste medewerkers en losse krachten van buiten vormen een aanhoudend privacyrisico van de groeiende databorg. 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 voor gaat in informatieoverdracht aan politie, om inlichtingendiensten, Minister Opelsten van Venj en staatssecretaris Willems van Financiën antwoorden met een weergave van artikelen 67 van de Algemene wet inzake rijksbelastingen (awr), dat voorziet in verstrekking van data bij strafvorderingen.

¹⁰³ Vergad. de politiestaat. Welkom in de belastingstaat, 30 september 2014, *De Correspondent* <https://decorrespondent.nl/1768/Vergad-de-politiestaat-Welkom-in-de-belastingstaat/> 543-60-65-70-88-94

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/> 505-29-328-381-385-1

¹⁰⁵ Interviews met Cyprian Smits en Nicole Back, Belastingdienst.

¹⁰⁶ *De Correspondent*: Zie <https://decorrespondent.nl/1847/De-Belastingdienst-als-databank-voor-OM-Politie-en-Inlichtingen-diensten/> 50021790-30366936 <https://decorrespondent.nl/1768/Vergad-de-politiestaat-Welkom-in-de-belastingstaat/> 34250-4594-40-73670-987

Het tweede deel betreft 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 en welke gegevens over hen worden verzameld en opgeslagen, daar melding van wordt gemaakt bij de Autoriteit Persoonsgegevens en de functionaris gegevensbescherming.¹⁰⁸

Bovendien staan er volgens de Belastingdienst ook in de privacywet, en zijn de convenanten over gegevensverstrekking door de Belastingdienst gepubliceerd op de website. Dit voldoet volgens het kabinet. De minister bewaart 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.'¹⁰⁹

De burger wordt, aldus het kabinet, op voor de ethische wijze geïnformeerd over de Big Data uitwisseling, zoals de miljarden gefotografeerde tekens van de aanpak om de lange 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 wilt, kan over de wettelijke grondslag informatie krijgen.'

Het omkijken behelst via verzoeken, ook data verkrijgen via eerder genoemde samenwerkingen. Volgens de minister is dat wettelijk gedekt, wat door het Hof Arnhem-Leeuwarden is bevestigd. Het ging om vervolging van een drugshandelaar wegens witwassen op grond van onder meer met het omkijken op grond van een convenant gedeelde belastingdata.¹¹⁰

Enkele weken daarna stelde ook de k-lid Geethuisen (sp) vragen aan de minister van VenJ en de staatssecretaris van Financiën over uitwisseling van persoonsgegevens door de Belastingdienst met a.i.v.d., politie en justitie. De antwoorden kwamen gro-

¹⁰⁷ Uitvoeringsregeling Algemeen wet inzake rijksbelastingen, Hoofdstuk 10: <http://wetten.overheid.nl/BWBR0006736/2015-0-10-16/Hoofdstuk10>

¹⁰⁸ Brief van minister van VenJ, D. Pesten en staatssecretaris van Financiën, Wierboon aan de Eerste Kamer, 3 oktober 2014 <https://www.rijksoverheid.nl/documenten/kamerstukken/2014/10/04/brief-afgave-over-verzamelen-gegevens-door-belastingdienst-en-uitwisselen-met-andere-overheidsinstanties>

¹⁰⁹ Voorzitter Hof Arnhem-Leeuwarden 8 november 2015 <http://deplink.rechtspraak.nl/uitspraakRd-EBLI:NL:GHARL:2015:0478>

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 geventureerde aanpak van georganiseerde criminaliteit'. De beschikbaarheid van 'alle informatie die nodig is' wordt van zwaarwegend belang geacht door de vragende instantie. Welk cijfer op oorspraken zijn ook in dit geval, zoals met de meeste data-uitwisseling besproken in deze bijdrage over data-analyse en fraudebestrijding, onbekend. Wel het aantal strafrechtelijk overdringen van het om bij de Belastingdienst voor specifiek evaardenkingen: 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 in volstaat de opdracht om aan haar taken uitvoering te geven. Er is geen actie handhaving, maar optreden bij melding van ernstige, structurele overtredingen van de privacywet die grote groepen mensen treffen en waarbij inzet van a-p-bevoegdheden een verschil kan maken.

Volgens Gesthuizen kunnen de al v.d. het omen de politie dank zij verregaande bevoegdheden van de Belastingdienst (door artikel 43 van de Uitvoeringsregeling Algemene wet inzake rijksbelastingen, 1994) dan nog aan persoonsgegevens komen die zichzelf niet mogen verzamelen dat wel bevestigen.

Minister Opstelten ontdekt dit niet: "Van belang hierbij is dat de Belastingdienst alleen dat soort relevante gegevens bevoort. De uitwisseling met de Belastingdienst is legitiem en geen achterdoet. De Belastingdienst versprekt 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 doelzinnen van samenwerkingverbanden."¹⁰

Ook de (voormalige) tk-leden Schouw (D66) en Ossenbrugg (PvdA) oefenden kritiek uit op de minister van Verkeer en staatssecretaris van Financien gezien de gebrokkelt transparantie oangaande de uitwisseling van persoonsgegevens door de Belastingdienst.

Het antwoord van de minister luidde: "De convenanten die zijn afgesloten met de a-ivd, politiek en om zijn uitsluitend aan uitwisseling binnen de grenzen van de wettelijke basis voor de uitvoeringspraktijk. Er bestaat 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 sobor' ten algemene wordt toegepast bij het verzamelen van gegevens in het kader van de uitvoering van zijn taken, zo ook bij het vastleggen van aan pr-gegevens. "De wettelijke persoonsgegevens worden alleen opgeslagen en

110

Antwoord van Minister Opstelten (VvdL) en staatssecretaris Wierbes (Financien) op vragen van Kamerlid Gesthuizen (sp) van 30 oktober 2014, over uitwisseling van persoonsgegevens tussen Belastingdienst, a-ivd, politiek en justitie 24 november 2014) <https://zoek.officielebekendmakingen.nl/ah-bk-2014-045.html>

bewaard, als blijkt dat ze fiscaal relevant zijn. Als dat niet het geval is, worden de gegevens direct verwijderd.¹¹¹

De politie voert in het systeem referentielijsten in waarop de kentekens staan van personen die bijvoorbeeld een boete oeten betalen of die worden gezocht in verband met een misdrijf. Uitsluitend deze 'hits' worden bewaard en gebruikt. Volgens de Autoriteit Persoonsgegevens schendt automatisering en de registratie 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.¹¹²

De Belastingdienst heeft op haar website een brochure gepubliceerd waar in duidelijk wordt gemaakt welke rechten een burger in dit opzicht heeft, zoals het recht op insage van zijn gegevens en het wettelijke recht. Van deze laatste rechten kunnen in principe ruim 12 miljoen zakelijk en privé belastingplichtigen gebruikmaken.¹¹³

4.4 beleid en toekomst

Informatiegestuurd werken

Privacy-afragingen maakten de Belastingdienst al meer jaren zegen veelvuldig, maar ze ontbreken nog steeds in de halfjaerapportages van de Belastingdienst. Daar tegen is het enthousiasme groot over de conclusies van data analyse de belangrijke onderdelen 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 gutfes van deze varen 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 mikt met 'ocht mazels data analyse, op basis van proefproeven en ervaringen getallen'. Het effectiefste instrument in de handhaving is vol-

111 Antwoorden van de minister van Ven Jans de staatssecretaris van Financiën op vragen van de (voormalige) tk-leden Shouwe (D66) en Ossenbrug (PvdA) van 3 november 2014 over de uitwisseling van persoonsgegevens door de Belastingdienst, al vd, politieke Justitie, 8 november 2014 <https://www.rijksoverheid.nl/binarise/rijksoverheid/doornentent/kamervragen/2014/11/29/bijlage-2014z9045-antwoorden-op-kamer-vragen-over-uitwisseling-persoonsgegevens/bijlage-2014z9045-antwoorden-op-kamer-vragen-over-uitwisseling-persoonsgegevens.pdf>

112 De Belastingdienst en de Wet bescherming persoonsgegevens (Wbp) http://www.belastingdienst.nl/wpa/wpa/nl/concept/belastingen/themas/afwijzend/brochure_en_publicatie/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 'voorant', bij de aanvraag of de aangifte in plaats van achteraf.¹¹⁴ Hierbij wordt steeds meer gebruik gemaakt van data-analyse. Door aanvullende selecties en analyses worden risicovolle posten beoordeeld en geselecteerd. Deze detectiewordt vroeger in het proces uitgeroerd, zodat wordt voorkomen dat ten onrechte betalingen op (voorlopige) aangiften plaatsvinden.¹¹⁵

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 data gerelateerde 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 totaaleenvorming van de dienst. Daarin is sprake van de spuren A (vereenvoudiging stelsel), C (operationeel en transparantie) en B (toetend data). Over de laatste schrijft hij uit: 'Er is een ontwikkelfilecofio voor de lot opgesteld, con gegevensinfrastructuur (de 'dataag') ontwikkeld en gebouwd. Een team van specialisten (de 'broedkamer') heeft proefgedraaid met een informatiegestuurde aanpak, die 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 informaticuitverschillendecsystemen, zodat voor een boekonderzoek bij een onderneming tot wel 28 in totaal.¹¹⁶ Er zijn afdelingen waar medewerkers gegevens uitlezen uit het systeem en intikken in het andere.¹¹⁷

Deze informatiehuishouding is gebaseerd op processen en voor elk proces is destijds een systeem gebouwd. De nieuwestructuur brengt de data bijeen per belastingplichtige. Technisch is het formen van een 'dataag' gebaseerd op standaard-

113 'Verslag van een algemeen overleg, gehouden op 8 oktober 2014, over Belastingdienst' Nummer 2014D39685, 4 november 2014.
<http://www.breedakamer.nl/kamerstukken/verslagen/delal?id=2014Z1760&did=2014D39685>

114 'Halfjaarrapportage Belastingdienst, 26 maart 2015.
http://www.breedakamer.nl/kamerstukken/brieven_regeling/delal?id=2015Z2586&did=2015D1182

den waarmee data vanuit verschillende systemen samengebracht worden. Zo ontstaat per 'subject' een dossier o.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. Informatiegebruik toezicht en inling...', 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 detecties zijn aanzienlijk hoger, het systeem peeft ook de aard van het risico aan, en de behandel-tijd door de medewerker gaat aanzienlijk omhoog.'

In de inning hetzelfde beeld van grote successen dank zij risicoanalyse op bijeenge-brachte data. 'Het systeem heeft de (dermate) kansrijke debiteuren, ontmaskert oninbaar gecombineerde inkomsten en adviseert te nemen maatregelen. De opbrengsten per medewerker springen 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.¹⁵

In de rapportage van de Belastingdienst over het eerste halfjaar van 2015 is de voortgang weer gegeven.¹⁶ Zo heeft voor het segment Particulier en de broedkamer een nieuw risicomodel ontwikkeld. Dit leidt tot beter oordeel bij de controle van onderdelen van aangiften (aandachtgebieden). Dit zou tot meer opbrengsten leiden. Het behandelen van twee aandachtigebieden is in Eindhoven en D en 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, almede de capaciteit voor data-analyse. Handhaving wordt verbeterd en kosten gereduceerd, aldus de bewindsman.

Een groot aantal transactiesystemen is nu onderzocht op ontlopen:

- inkomenbelasting;
- omzetbelasting;
- bezwaar;

¹⁵ Brief over de uitwerking Bijzondere Investeringsregeling Belastingdienst van Staatssecretaris Wiebes van Financien aan de Tweede Kamer, 20 mei 2015.
<https://www.rijksoverheid.nl/documenten/brieven/2015/05/20/brief-over-de-uitwerking-bijzondere-investeringsregeling-belastingdienst>

¹⁶ Halfjaar rapportage van de Belastingdienst, 10 september 2015.
<https://www.rijksoverheid.nl/documenten/kamerstukken/2015/09/16/half-jaar-rapportage-van-de-belastingdienst>

- klantregistratie;
- vennootschapsbelasting;
- auto;
- loon;
- betalingsverkeer;
- inkomens.

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

Verantwoording moeilijk

De nieuwe Digital Deal levert de wetgever de mogelijkheid dat de politieke verantwoording ('accountability') van de Belastingdienst ook verandert en voortaan de volgende onderwerpen behelst:

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

Echter, het is moeilijk voor de Belastingdienst om risico's 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 voorspeld voorstellen die vanaf 2020 gaan optreden en die door het internationale adviesbureau zijn bekrachtigd. Hoe worden die hardgemaakt? Immers, het data- en IoT-spoor kost meer geld dan bespaagt, maar zal ook maar oplopen volgens de staatssecretaris. Hij geeft de term 'business case' mee, gezien de endabele (extral) investering. De plannen zijn doorgeleid door mondiaal adviesbureau Oliver Wyman.

Deze bevestigt dat de totale stappen voor investering van 1 miljard euro de komende vijf jaar vanaf 2020 zo'n 750 miljoen euro aan extra belastinginkomen oplevert. Nog afgezien van de kostenbesparingen aan personeel van zo'n 300 miljoen euro per jaar. Dit zijn algeronde bedragen met een vooruitziende blik van vijf jaar. Wat het 'nulpunt' is op basis waarvan het resultaat over vijf jaar gemiddeld kan worden, is niet openbaar.¹⁷

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.¹⁸ Het heeft in 2013 en 2014 minder opgeleverd dan was beoogd. Zwaarte kritiek betreft het gebrek aan goede verantwoording. Er werd uiteindelijk 6 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 nocht het ministerie van Financiën is juist geïnformeerd. De minister van Financiën antwoordde later wachten 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. Daar waar vindt daar ontwikkeling plaats van de waarde van de 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 medewerkerstevredenheid.¹⁹

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 opleidingsstraject op het vlak van data science en worden specifiek externe experts betrokken met ervaring bij andere belastingdiensten.²⁰ De ontwikkeling van inzichten en producten vindt plaats in samenwerking met verschillende marktpartijen, die expertise en ervaring inbrengen van uit buitenlandse belastingdiensten.

¹⁸ Intensivering toezicht en invordering bij de Belastingdienst - Voorbeeld van een 'business case' bij de Rijsoverheid, 11 februari 2016

<http://www.rekenkamer.nl/Publicaties/Onderzoeksrapporten/Introduities/2016/02>

¹⁹ Intensivering toezicht en invordering bij de Belastingdienst

²⁰ Idem.

Samenwerking buitenland

België vormt een voorbeeld. Volgens de betrokkenen heeft data-analyse de btw-fraude van naar schatting 11 miljard euro per jaar teruggebracht naar 40 miljoen dankzij het 'Hybride Detectie Model'. Dat is gestoeld op signalen in het systeem en analyse van (sociaal) netwerken.

Opening van een vestiging in Panama door een Belg geeft bijvoorbeeld een signaal, maar ook subtiel 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 en data om potentiële btw-fraudent netwerken 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 directeur Menno Griffioen zo'n 2 miljard euro per jaar aan btw mis door onjuiste aangiften, waaronder btw-fraude. Dat is drie procent van de totale opbrengsten.²¹

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.

Mondialesamenwerking is het doel, opgezet via de Organisatie voor Economische Samenwerking en Ontwikkeling (oecd), die de internationale anaysediensten 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 oecd in Amsterdam gehouden, met veel aandacht voor voorspellende modellen en data-analyse. Het programma Analytics: Exploiting big data of fight tax crimes and other financial crimes had sprekers uit Singapore, Australië en Ierland.²²

Verzocht: ondsugende kinderen en gedragsoefening

De 'kleuterjuffrouw' wilt precies welke kinderen 'lief' of 'ondsugend' in welke omstandigheden en in welke interactie waren met welke andere kinderen, en paste daar haar toezicht op aan. Facebook kan uit onze e-mails en gedrag op het scherm exakte portretten van zijn klanten samenstellen. Dit peespediefonk ook voor de Belastingdienst.

De staatssecretaris liet de Tweede Kamer weten: 'Een inspecteur, hoe ervaren ook, stuit met veel informatie op beperkingen. Met massale data-analyse, op basis van

²¹ Btw-fraudeurs opgepoord met big data, Cyriel van Rossum, 29 april 2016

²² <http://bestuur.nl/magazine/btw-fraudeurs-opgepoord-met-big-data>

Tax Crime Forum 2016 Outcomes Statement

<http://www.oecd.org/tax/crime/forumontaxandcrime.htm>

zeer grote hoeveelheden beschikbare gegevens, wordt dit reflectanszien ijk 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. Elk '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 pensioen.¹²⁴

In feite vindt ook een profilering plaats en deze bepaalt de mate van controle. De kunst is om er niet te veel en niet te weinig mee af te handelen, dus met het weer. Daar in worden globaal drie hoofd categorieën 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 huld 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 van personen of rechtsoorzoeken: te weten die of te goeder trouw? De categorisering moet actueel blijven met aanhoudende steekproeven. Bepaalde patronen geven duidelijk een vergissing aan. Anderen

¹²³ <https://www.rijksoverheid.nl/documenten/brieven/2016>

king-brede-agen-de-belastingdienst
(5 jan. 2016).

¹²⁴ 'Directeur Belastingdienst over Big Data: 'Mijn missie is gedragsverandering', 21 april 2016, De Correspondent <http://decorrespondent.nl/2720/Bas-Belastingdienst-over-Big-Data-Mijn-missie-is-gedragsverandering-8325520-16w78aaf>.

¹²⁵ Interview met Cyprian Smits, Nicole Bak, Belastingdienst.

tonen onomwonden bewust bedotten aan. Uiteraard is er een grijs gebied daartussen, waar dat minder duidelijk is. Aldus de dienst in een toelichting.²⁵

De Belastingdienst die per aangever een dossier of 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 en 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 sneeuw egen.

Zonder dit beeld te oppakken of de data in volkomen te versimpliciseren werd in een interview met algemeen directeur Hans Blokpoel de term Big Brother opgevoerd. 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.'²⁷

Het beeld per klant werd tot kort opgebouwd uit ingediende aangiften, betalingen en cetera. Met het online invullen van aangiften kan de dienst ook gedrag real time gaan volgen. De betrokken manager van de Belastingdienst schreef in zijn motivatie van het Fraude Bijportaalcentrum voor de Manifestatiegroep aan bodend dat dit: 'Werkelijk een stap-voor-stap hoe fraude kan worden gepleegd, bijvoorbeeld al bij het invullen van een formulier.'²⁸

Met de aangifte inkomstenbelasting over 2014 hebben miljoenen Nederlanders voor het eerst via Mijn Belastingdienst in 'the cloud' hun data verstrekkt. Niet alleen ontvangt de Belastingdienst daarmee digitaal het resultaat van

25 Brief over de uitbreiking Brede in verband met de Belastingdienst van Staatssecretaris Wiebes van Financiën aan de Tweede Kamer, 20 mei 2016 <https://www.rijksoverheid.nl/documenten/brieven/2016/05/20/brief-over-de-uitbreiking-brede-in-verband-met-de-belastingdienst>

27 Preek Blankens, 'Belastingdienst zoekt heel in de datalog', *IR&B* nr. 14 oktober 2016 <http://irb.vws.nl/nieuws/belastingdienst-zoekt-heel-in-de-datalog> (5 januari 2016).

28 <http://www.digitaleoverheid.nl/acties/buzz-tour/1/audierapport/buzz-blog-financi%C3%A9n-geraadpleegd-februari-2016,-slat-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; waaraan op welk tijdstip, hoe lang en met welke mate van twijfel invulling plaatsgrijpt.

Zo kunnen patronen worden ontwikkeld en toegepast voor een bepaald wijze van invullen, die in samenhangen met dewil tot frauderen. Ook opgeslagen versies die niet officieel worden ingediend, staan de Belastingdienst ten dienste bij het speuren naar fraude.

Diegenen 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

inleiding

Het Inlichtingenbureau (ib) functioneert sinds 2006 als knooppunt of wel schakelpunt voor informatieoverdracht aan gemeenten en andere overheden. Dit met als doel verhoging van de efficiëntie in het bepalen en controleren van handelingen van instanties die besluiten nemen over uitkeringen en belastingen. Te danken valt daar bij 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 de aanmelding van Box 5-gegevens uit de aangiften inkomstenbelasting.

Big Data wordt gekoppeld en gemiddeld tot nu tien "informatieproducten", zoals databundels voor een Rechtmatigheidscontrole Participatie wet. Het ib levert gemeenten en des v.b. 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 "onruke samenmet" of uitvraag.

Het ib staat voor behoor, analyse en beveiliging van een enorme hoeveelheid per soonaangegeven. 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 telefonische gesprekken, aangevuld met door de voorvoerders geleverde informatie van inlichtingenbureau.nl

5.1

doel

Het ib is opgericht in 2006 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 die gemeente ontvangen, daar ook recht op hebben (rechtmatigheidscontrole) en anderzijds om te bepalen of zij geld laten liggen, zoals huur- en zorgtoeslag. Als knooppunt of wel 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 voor tijdig schoolverlaten (r-mc), Regionale Coördinatiepunt en Fraudeteam tijdig (r-cf), de vng (stichting gerechtshoeveaars), het cijb en des v.b. Het doel van deze operatie is om de efficiëntie 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 controleren en te antwoorden worden administratieve lasten verlicht en de efficiency en effectiviteit van werkprocessen groter. Het meer realiseert het bijvoorbeeld volgens betrokken 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:

- **Rechtspraak** (Belastingen en Inkomens):
 1. Rechtspraak voor de Partij (patroon)
 2. Digitale Inkomens (dikd)
 3. Rechtspraak (Syril)
 4. Participatie & Re-integratie
 5. Armoedebestrijding
 6. Landelijke Informatievoorziening Participatiewet
- **Diensten** (Zorg en Jeugdzorg)
- **Orde en Veiligheid** (Orde en Veiligheid voor de Landelijke Inkomens)
- **Belastingen** (Belastingen: Geautomatiseerde toets op kwijtschelding)

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

1. Rechtmatigheidscontrole voor gemeenten (bijstand, loaw en loaz) en desvb (aio) met gegevens van uuv, de Belastingdienst, de Justitie (informatiedienst (Justid)), de Justitie (dw) en andere gemeenten. Deze gegevens worden vergeleken met de gegevens van de uitkeringgerechtigde zoals die bij gemeenten of desvb bekend zijn, bijvoorbeeld of het een buitenlandse gastarbeider of voortvluchtig voor de politie betreft.

Heffingskortingen als onderdeel van inkomens 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 uuv 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 hoe veredit 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 Iib geeft alleen aan dat een situatie onderzoek waardig is, als suggestie.

Dij de nieuwste generatie signalen levert het Iib een prioritering mee, een tag, die de signalen indeelt naar mate van onderzoekwaardigheid. De samenloopsignalen kunnen automatisch worden ingelezen in de meest uitkeringsadministratiepakketten van de gemeenten om het werk proces te vergemakkelijken.

De signalen vormen samen de productgroep rechtmatigheidscontrole. Hier toe behoren bijvoorbeeld ook signalen over direct uitgesloten de heffingskortingen en voortuigbezit. Het Iib geeft signalen voor beoordeling van het recht op studietoelating, de overschrijding van mogensgrens, uitkering in andere gemeenten, detentie en voortvluchtig veroordeeld, inschrijving bij een hogeschool of universiteit, en een overzicht van bankrekeningen en saldi.

2. Landelijk verwijzings- en routeerservice: een knooppunt voor de gegevensuitwisseling tussen gemeenten en andere partijen binnen het domein suw i en de Partidopatielevet. Partijen kunnen via het Iib gebruik maken van de gemeentelijke verwijzingsindex, automatische antwoordservices en putten uit een centrale database. De gegevens die beschikbaar zijn, komen voort uit bestanden opellingen en andere elektronische informatielevering.

Centraal staat het Digitaal Klantdossier (dkd), een gemeenschappelijk v i l u a l dossier waarin informatie gedeeld wordt op het gebied van werk en inkomen door uw v. z v b n gemeenten. Het dkd is ontwikkeld in het kader van de Wet eenmalige gegevensvraag (w eu), waarmee burgers voor de k e n Werk en Inkomen maar eenmalig hun gegevens hoeven te verstrekken.

3. Syri komt in hoofdstuk 6 uitgebreid aan de orde. Het Iib is daarvoor 'onderaannemer'. In het kader van Syri biedt het Iib ondersteuning. In opdracht van de Inspectieszw verzamelt het Iib data over risico profielen worden samengevoegd. Dit doet het in een geanonimiseerde omgeving. Het Iib stelt resultaten beschikbaar waarmee de data-analisten van de Inspectieszw aan het werk gaan, nog zonder dat het gepersonaliseerd is, zekrijgen van het Iib anonieme data.

De Inspectieszw heeft een eigen systeem voor data-analyse om signalen van fraude op te sporen, de Black box genoemd. Het Iib deed al Syri i-achtige activiteiten v o r d e w a t w i j z i g i n g t o t s t a n d k w a m, in nauwe samenwerking met de Autoriteit Persoonsgegevens. Dit behelst de twee typen onderzoek: or is voor enkele wijken een risico profiel samenstellen, te weten op basis van postcodes. In voor ondernemingen die een groter aanspreken op wat overtrekkingen, zoals bepaalde uitzendbureaus. Het Iib is de onderaannemer voor de uitvoering van projecten met bestanden opelling van de Landelijke Interventie teams op grond

van Syr I. Het Ibi koppelt daartoe afhankelijk van het doel van het onderzoek maximaal zo'n 66 bronbestanden.

4. Kwijtschelding gemeentelijke en waterschapsbelastingen: verschafting 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 verplicht zijn op het bevorderen van participatie en reïntegratie van kwetsbare groepen in de samenleving.
6. Armoedebestrijding: voorzien in signalen die duiden op recht op voorzieningen en regelingen uit de sociale zekerheid waar geen gebruik wordt gemaakt. In sommige gevallen bleek tot bijna 70 procent van personen die recht op een bepaald bijdrage hadden, daarvan geen gebruik maakten. Het als bijdraudesignalen betreft het suggesties waarbij een sociale dienst al dan niet actief betrokken benadert. Het Ibi bezit ook over deze categorie geen informatie over de onderzochte uitkomsten. Het Ibi verschaft, bijvoorbeeld signalen over betalingsachterstand zorgpremie, het ontbreken van een zorgverzekerings, onbenutte bijzondere bijstand 66 plussers, onbenutte huur- en/of zorgtoeslagen en onbenutte kinderopvangtoeslag. Om gemeenten hier op zicht te bieden, wisselt het Ibi gegevens uit met desvb, de zorgverzekeraars en de Belastingdienst.
7. Informatievoorziening Knooppunt diensten maakt voor gemeenten, zorgaanbieders en andere partners 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 Ibi zelf gebouwd, tot drie jaar geleden met een adviesbureau, eerst Capgemini, daarna met het systeem voor rechtmatigheidscontroles in eerste instantie door Cap gebouwd, daarna door hph gebouwd en daarna weer beheerd door Cap. Dat was het "Sectoralek systeem". Het eigen systeem heet Ibis, Inlichtingenbureau Informatiesysteem. Dit wordt onderin 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, u.w.v. Belastingdienst hebben hun eigen formaten, zoals xml. Het Ibi levert data aan gemeenten op open-nummers. De

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

5.3

uitvoering

Het lib verzorgt rechttoerechtaan 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 lib verschaft gemeenten en dus bv de relevant over eenkomsten, hits, samenloop situaties die mogelijk inbreed 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. Daarmee deden de gemeenten een periodieke toets, een arbeidsinbreefproef. Dat is nu veranderd door een gesloten mailbox, dat aanleunt op de achtergrond gemeenten informatie verschaft indien daar toe 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 Wv et werken en bijstand (Wvb) opgenomen dat mensen die zich onttrekken aan een opgelegde gevangenisstraf geen recht hebben op bijstand. Een dergelijk aanpassing geeft voor het ministerie van sociaal leiding het lib te vragen een signaal te creëren (een gegevensuitwisseling op te tellen) waar mee het gemeenten op olik en wijzen dat een persoon die bijstand krijgt toegewezen. In het register van voortvluchtig ver oordeelden staat geregistreerd. Indicatoren en risicoprofielen komen tot stand vanuit onderzoek. Een dergelijk onderzoek wordt uitgevoerd door de Inspectie szw.²⁹

Het lib kijkt dus met bestanden koppelingen 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 dit is verandert met de uitkering. Het lib werkt to aan het slimmer maken van deze signalen.

Voorbeelden van 'slimmere signalen' die in 2014-2015 beschikbaar kwamen:

- Bij signalen over arbeidsongefitgenen die mensen wonen.
- Bij signalen over inbreed in de wettelijke net toeloo, zodat gemeenten sneller inschatting kunnen maken of het inkomen boven of onder de wvb norm valt.
- Gemeenten krijgen elke maand een lijst van bankrekeningnummers standgerechtigden. In de nieuwste situatie wordt gemiddeld twee spraken van een nieuw of een gewijzigd bankrekeningnummer.

²⁹ Interview met Paul Schaafsma en Jan-Peter Bergfeld, Inlichtingenbureau.

Er liepen ook twee proeven:

- In de pilot opspor en buitenlandse gedetineerden zijn gegevens van Nederlandse gedetineerden in het buitenland vergeleken met die van uitkeringsgerechtigden.
- In de pilot bestandskoppeling landelijk register kinderopvang en peutersalen (Irkpi) 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 dat het geval, dan wordt via het ib de betreffende gemeente geïnformeerd.

De pilot bestandskoppeling Irkpi werd door onvoldoende nullig 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 ontstaan van inkomsten, maar alleen op het geregistreerd staan.

Het ib voegt steeds nieuwe tags toe aan signalen. Een 'tag' is in feite een label-ijmer met contextinformatie over de gegevens. Bijvoorbeeld, vanuit een bestandskoppeling met de dwi ontvangt het ib informatie dat een bijstandsklant een voertuig op zijn naam heeft staan. Dit geeft aanleiding de gemeenten hirop te attenderen. Het ib kan op basis van de meegelerde 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 ek afzonderlijk voertuig wellicht weinig aanleiding nader onderzoek te starten, maar het feit dat de betreffende persoon gedurende een bepaalde periode ook verschillende voertuigen op zijn naam heeft gehad wordt wel.

Niets blijft overigens anoniem. Het gaat wel anoniem door de den 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 geminimaliseerde gegevens geoppeld aan personen.

Ze zijn dan nog geen verdachten, maar worden in een hokje geplaatst. Het is een behouden deel van de onderzoeksprofiel. Het ib levert het gegevens af dat er

130 Monitoren van de Fraudewet en rapportage fraudeaanpak en handhaving, 90/50-474, 26 mei 2014.

LF. Aascher, minister van szw, aan de Voorloverscommissie szw van de Tweede Kamer. Misbruiken ongewoonlijk 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.¹⁹¹ De heft van de uitkeringingerichtigden 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.¹⁹²

Voor bijvoorbeeld voertuigen ligt dat niet vast. Er komt een lange beslissboom voor bepaling van relevantewaarden bij kijken en waar van de criteria samen met de dienst en Handhaving van de gemeenten zijn opgezet. Op grond daarvan heeft het Ib in dit geval labels mee van mogelijk vermogen. Een Porsche is per definitie een auto die een signaalkrijgt, Rolls Royce, Mercedes of BMW ook wel; auto's die je niet verwaadt bij bijvoorbeeld ouderlijken.¹⁹³

Zo'n dure auto lijst wordt periodiek nagelopen om die te herijken en vervolgens in het systeem bij te werken. Daar toekomen gemeentelijke afnemers met het Ib bijeen voor export bijeenkomsten: een keer per jaar en ten minste één keer per jaar.

Met het bk w i, beheerder van Suwinet, vindt afstemming plaats. Dit bureau coördineert de verstreking van informatie aan vragende partijen. Bij het bk w i moet je voor inzage een team instellen. Dat houdt handig om diezelfde afnemers gegevens in te zien. Gemeenten kunnen echter niet dagelijks voor elk w b-klant kijken of er nog bijzondere omstandigheden zijn.

Het Ib en het bk w i hebben niet dezelfde bestanden, maar wel dezelfde databronnen. Ze delen soms bestanden, bijvoorbeeld gegevens over bank saldi van uitkeringingerichtigden ('vermogensignalen') die het Ib aan gemeenten verstrekt.

5.4

resultaten

Het Ib verstrekt gemeenten maandelijks voor nu 350.000 w b w i uitkeringingen de signalen van mogelijke fraude van uitkeringingerichtigden gekoppeld de databestanden. In het (niet openbare) jaarverslag 2018¹⁹⁴ worden de volgende aantallen nieuw verschafte signalen aan gemeenten voor de rechtmatigheidscontrole w b genoemd (afgerond):

¹⁹¹ Interview met Paul Schaafsma en Jan-Peter Bergfeld, Inlichtingenbureau.
¹⁹² Idem.
¹⁹³ Idem.

- heffingskortingen: 230.000
- ~~10.000~~ verbanden:
- svb-uitkeringen: 06.000
- 59.000 vermogen:
- 108.000 auto bezit:
- sofinummer controle: 00
- 8.700 detentie:
- voor tv ~~000~~ig veroordeeld:
- ~~1000~~ Basissanloop:
- studie in ~~in~~ ~~de~~ ~~sch~~ ~~op~~ ~~pl~~ 200

Volgens het ib betreft zeker 80 procent van de verstrekte signalen informatie die reeds bij gemeenten bekend is. Immers, vanwege de meeste bijstandsklanten houden zich aan de informatieplicht om gewijzigde omstandigheden die van belang zijn voor de wvb-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 duikt 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 wel strikt in nemen en direct een maatregel (boete), andere zijn wel ouderlinter in. Daarop heeft het ib geen enkele invloed. Het ib heeft noodt of een sanonloop bovast handelen de 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-imag

Het ib staat voor beheer, analyse en beveiliging van een enorme hoeveelheid persoonsgegevens. Er ontstaat daardoor eenvoudig een imago probleem, te meer daar de term 'Inlichtingenbureau' direct af omstijgt uit 1984 of gelijksoortig doomsdario met grootscheepse privacy aching. '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 conproce hebben gautomatiseerd om de onrechtmatigheid 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 heeft de opvatting bij publiek dat wij fraudebestrijding doen.'¹³⁵

¹³⁴ Ibid.
¹³⁵ Ibid.

Het ib werd in 2016 genomineerd voor een 'Computable Award' voor het Gemeentelijk Gegevensnooppunt als beste IoT - project van het jaar bij dooverheid. Maar dat is voor technisch kunnen van de koppelingen en draagt eerder bij aan de doem dan dat het erafbreuk 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 begreepd. 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 privacybeoordeling zou je veel meer kunnen doen. Maar dank om te politiestaat wel erg dichtbij.' Dit ervaart het ib eerder als probleem dan als voorrecht. 'We betwijfelen of het werkelijk helpt. Om aan die informatiebehoefte die veel terug is te denken 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 informatiebron bekijken om te weten wat er speelt. Waar ben je mee bezig? Waar loop je tegenaan? Ze zijn tevreden over de transparantie die wij betraden'.¹³⁸

In feite moeten de afnemers (gemeenten) als gebruikers van de data signalen zich afvragen of ze binnen privacygrenzen blijven, maar het ib moet hen regelmatig helpen 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 'integrated data sharing' (geïntegreerd gegevensdeling): 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 zorgtak en vanuit de Rijks-overheid. Gemeenten zijn verantwoordelijk voor jeugdzorg, werk en inkomen en zorg aan langdurig ziek en en ouderen op grond van de Jeugdwet, Participatiewet en Wmo. Het ligt voor de hand dat gemeenten dan ook allerlei informatiewijzen verzamelen omtrent een aantal leefgebieden (inkomen, schulden, huisvesting, gezondheid, overlast, etc.) van een persoon en/ of gezin. Wat en regelgeving vast 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
137
138

Idem.
Idem.
Idem.

Het is maatwerk. Volgens het lib gaat de discussie altijd over wat vanuit maatschappelijk belang zou moeten mogen, tegenover wat nu feitelijk mag. De gedachte is vaak, aldus het lib, dat oplossingen zich vanzelf zullen gaan aandienen, zodra maar eerst kan worden beschikt over een ruime gegevensverzameling. Wetgeving dwingt gegevensverwerkers echter anderszins andersom te denken, zo moet het lib haar afnemers regelmatig voorhouden.

De privacywet begrenst de gegevensverzameling aanzienlijk. Doelbinding, proportionaliteit, subsidiariteit zijn dan de breinbrekers waar veel gemeenten op vast lopen.¹² 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 maar gegevens moeten invullen, maar opvolgen met een dossier met reeds bekende data. Heel begrijpelijk volgens het lib, maar daar voorziet de wet niet in.

Willt de sociaal regisseur voor initiatie, 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 de zelfde dwars.

Dat mag een gemeenteraad niet als een bevestiging, maar zij dient dit te beschouwen als een recht van hulpbehoevenden. Zelfs als deze 'cliënten' er niet op zitten te wachten om aan de knuutentafel wederom – en soms moedzaam – alldit faten op te lepelen of uit schoenendozen te halen die bij de gemeenteraad lang bek en zijn. Soms stuit ook proactief beleid voor armoedebestrijding op deze privacy grens:

gemeenten willen dat verzamelen en combineren over mensen maar 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 lib wel leveren, maar mag dat niet.

Wel is er een proef gedaan om hiertoe bestanden van de Belastingdienst te koppelen, met vrijgave van het ministerie van Financiën. Het resultaat van deze test was echter negatief: de hoogte van het belastbaar inkomen bleek een slechte indicator van actuele armoede van huishoudens.

5.6

toekomst

Momenteel speelt de vraag hoe het lib eerder data kan verkrijgen, niet per se de uitkering is toegewezen, maar reeds tijdens het aanvraagproces van de uitkering. Het lib wil ook het budgetverbruik meer dan direct ontvangen, zodat het de aanvraag kan ondersteunen. Het lib 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 totdie 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 bank rekeningnummers van personen met bijstand aan gemeenten verstrekt. Als gemeenten dat zelf bijhouden, kan vaststaan worden met signalen van louter nieuwe bankrekeningen.

Op de vraag naar Big Data-toepassing zegt het ib dat dit afhangt af van de gihan-taar de 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 bergende data, dus nog zonder vooruitbedacht 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 bergende 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 Syr i, laten we over aan de voor Syr i verantwoordelijke minister van zw. Wij verlenen hand en spandiensten bij de uitvoering. Overigens is het ook bij Syr i noodzakelijk dat vooraf een specifiek doel is geformuleerd waartoe het belang van de verantwoordelijk ordelijk onw ijs strekt.

Dit is een generiek beperking van de mogelijkheden van datamining met persoonsgegevens. Als de data daarop analyses worden uitgevoerd, niet terug te voeren zijn op specifieke personen geldt deze beperking uit aard niet. Maar dat doen we niet uit eigen beweging.'⁸⁹

⁸⁹ Ibidem.

6

Inleiding

Begin 2004 is voor sociale fraudebestrijding de Landelijke Stuurgroep Interventie-teams (Lsi) opgericht onder (destijds nog) staatssecretaris Rutte van Sociale Zaken, met als deelnemers: u.w.v. Belastingdienst, de v.b. si.d. en Arbeidsinspectie (nu beiden deel van de Inspectie SZW), het om.d.v.ing en Divosa. Data-analyse is een van de middelen.

De voorloper van het systeem Hiscod-indicatie (Syr i) voor bestandsoepeling werd onder de naam "Black Box" jarenlang toegepast voor het sporen naar fraude met uitkeringen, belastingen en loontijden, fulltimeverantwoordelijke medewerkers zonder afzonderlijk wettelijke grondslag maar wel binnen de regels van de Wet bescherming persoonsgegevens.

Dat ontrok zich grotendeels aan de openbaarheid. Par. de verantwoording in de wet door minister Asscher en de Tweede Kamer (zonder stemming, dus unaniem) leidde tot beschuldiging van Syr i als Big Brother-achtige opsporingsmethode.

In hoeverre is dit gerechtvaardigd? Hoe uitgebreiden intensief wordt gebruik gemaakt van Syr i en hoe merkbaar is in de praktijk, wat wordt waar data-in gebruik en wat levert dit op? Dat komt in dit hoofdstuk gedetailleerd aan bod.

6.1

wettelijke basis

Per 1 januari 2016 is de Wet aanscherping handhaving en sanctiebeleid SZW van kracht, bekend als de Fraudewet, gericht op fraudebestrijding in het sociale domein door gemeenten, de v.b. en het u.w.v. Deze verplicht onder meer om bij geconstateerde gebreken in informatieplicht een boete op te leggen aan uitkeringsgeregelden.¹⁴⁰ Een logisch vervolg op de Wet voorstel Fraudewet door Bestandsoepelingen van minister Asscher van SZW. Dat werd zonder stemming aangenomen.¹⁴¹ Per 1 januari 2014 is de Wet Structuur Uitvoeringsorganisatie Werk en Inkomens (Wet suw i) 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 u.w.v., de v.b., 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 arbeidsregels. Zo kan op basis van informatie uit de verschillende wetten

140

141

<http://wetten.Overheid.nl/BWBR0032037> geleidheidstat

Wet voorstel tot wijziging van de Wet suw i en enige andere wetten in verband met fraudeaanpak door gegevensuitwisselingen en het effectief gebruik van binnen de overheid bekend zijnde gegevens (Kamerstuk 33575).

personen of bedrijven het grootst risico op regiovertreding aanwezig is. Daarnaast werden nieuwe bestandsoppelingen mogelijk, zoals data van gedetacheerden in het buitenland bij uitvoerders in de sociale zekerheid, alsmede informatie over gestoude aanbijslandsdata. Indien dit samenwerkingsverband van u.w.v., Inspectieszw, dataw i laten verwerken voor risicoanalyse moest het de minister van szw verzoeken om de betreffende gegevens te verwerken in Syr i. 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 Syr i ontworpen. De voorwaarden waar onder dit systeem kan worden toegepast, zijn uitpakket in een Algemeen besluit van bestuur, het Besluit Syr i. Dit is op 12 september 2014 in werking getreden.¹⁴²

De techniek die in het instrument Syr i 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 drafax (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 door de toenmalige lsd (later Inspectieszw) ontwikkelden toegepast. De Black Box was de basis voor het instrument Syr i. In de Wet suw i kreeg dit in een nieuw artikel 85 de wettelijke verankering ten behoeve van integriteitsoverheidsop treden ter voorkoming en bestrijding van uitkeringen, belasting- en premietraude en het niet-naleven van de arbeidswetten.¹⁴⁴ Genoemde partijen zetten bestandsoppelingen in om samenhangende misstanden te kunnen onderkennen en om de pak kansen te verhogen. Syr i 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 suw i in verband met regels voor fraudeaanpak door gegevensuitwisselingen in het effectief gebruik van binnen de overheid bekend zijn gegevens met inzet van Syr i <https://zoek.officielebekendmakingen.nl/ab-2014-220.html>

¹⁴³ In de Memorie van Toelichting <http://www.tweedekamer.nl/kamersuiken/data/?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/kamersuiken/wetvoorstellen/detail?id=2013Z005428.dos&er=33379>

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

Voor verwerking in Syll komen de volgende categorieën data in aanmerking:

- a. arbeidgegevens over verschillende werkzaamheden;
- b. gegevens inzake bestuurrechtelijke maatregelen en sancties, zoals boetes;
- c. fiscale gegevens van natuurlijke personen en rechtspersonen;
- d. bezit van roerende en onroerende goederen;
- e. gegevens voor uitsluitingsgronden van bijstand of uitkeringen;
- f. handgegevens van rechtspersonen en bestuurders;
- g. huisevestigingsdata;
- h. identificerende data: naam, adres, woonplaats, postadres, geboortedatum, geslacht en administratieve kenmerken en bij een rechtspersoon: naam, adres, postadres, rechtsovereenkomst, vestigingsplaats en administratieve kenmerken;
- i. inburgeringsdata;
- j. nalevingsdata, overloveningen;
- k. (financiële) ondernemingsdata;
- l. pensioenrechten;
- m. andere-integratie verplichtingen;
- n. datashulden;
- o. uitkerings-, toeslagen- en subsidiegegevens;
- p. data over verkeer en vervoer, 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 aanmerkelijk maakt;

risicoindicatie: de melding, bedoeld in artikel 10, tweede lid, van de Wet suin;

risico model: een model dat bestaat uit vooraf bepaalde indicatoren en aangest of en sprake is van een verhoogd risico op:

- onrechtmatig gebruik van overheidsgelden en overheidssubsidies op het terrein van sociale en de inkomensafhankelijke regelingen;
- belasting- en premiefraude, of
- het niet-naleven van arbeidswetten;

Voorbeelden van relevante bronnen:

- Gegevensuitwisseling gedefinieerd in het buitenland;
- Vermogen in het buitenland (Belastingdienst, Internationaal Bureau Fiscale Informatie (IBF));
- Gegevenslevering nutbedrijven en woningverhuurders, in de projecten Waterproof is aangest gegevens van nutbedrijven een effectieve en doelgerichte indicator voor adres- en leefvormfraude kunnen zijn voor gemeenten en hetsub. Deze fraudegevallen zouden zonder nutgegevens niet zijn ontdekt. De aanname is dat bij een zeer laag water verbruik op een adres (minder dan 10 m³ per jaar) sprake is van een feitelijke niet-bewoond adres en daardoor mogelijk van verzorgden samenwoning elders met uitkeringfraude en huurtoeslagfraude als gevolg.

Aangezien een volwassene gemiddeld 45 m² 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 gegevens van woningbouwcorporaties over de tenaamstelling van huurcontracten en betaalposse-venissen effectieve indicatoren zijn voor samenwoning.

- Gegevens uit de Registratie Kinderopvang en peuterspeelzalenwerk: Als een burger een uitkering krijgt en daarnaast actief als gastouder, houder is van een Kinderartium dan wel als zelfstandige zonder personeel inkomsten uit kinderopvang ontvangt, dan zijn de inkomsten van in loed op het recht op de hoogte van de uitkering.
- Opschorten uitkering werkloosheidsverzekeringen en volkverzekeringen in relatie tot inschrijving bij de basisadministratie persoonsgegevens.
- Uitbreiding gegevenslevering vanuit de polisadministratie aan pensioenvervoers, Sociale Verzekering bank en gemeenten

Met het besluit Syr i wordt fraudebestrijding met behulp van bestaand oepelling binnen de geldende privacywetgeving toegepast. Hier toe worden data gebruikt die de betrokken partijen in de uitoefening van hun wettelijke taak verzamelen. Dit is ook in het belang van efficiëntie, 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 informatie moet er minder

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 128 miljoen sociale zekerheidsfraude als gevolg van misbruik en misstanden beperken, zodat het maatschappelijk draagvlak voor de sociale zekerheid behouden bleef.

Het instrument Syr i heeft volgens betrokkenen een substantieel aandeel in de fraudebestrijding. In 2010 was de gezamenlijke opbrengst van de afgeronde interventieprojecten ruim 23 miljoen euro. Er gaat bovendien een preventiewerk inguit van handhaving. De unieke combinatie en diversiteit van openbare en gesloten bronnen waaruit geput kan worden met behulp van Syr i, de analyse die wordt opgebouwd met betrekking tot risicoprofielen en -analyses en de gepresenteerde samenhang van gegevens in de risicomelding, maken dat Syr i toegevoegde waarde heeft.¹⁴⁵

¹⁴⁵ Wijziging van de Wet structuur uitvoeringsorganisatie werken inkomsten en enige andere wetten in verband met fraudeaanpak door gegevensuitwisselingen en het effectief gebruik van binnen de overheid bekend zijnde gegevens.
<http://www.heidkamer.nl/kamerslukkert/wetvoorstellen/detail?id=20122059428.dos&sr=33379>

Syr i is volgens hen niet op de eerste plaats ontwikkeld om geld – genoemd de 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 Syr i mag alleen worden gedaan door een samenwerkingsverband van de partijen genoemd in artikel 84 suw i: Colleges van bkw, het uiv, v, desvb, de Belastingdienst en de Inspectieszw. Een bestuursonderzoek dat of persoon die op dit moment geen partij is bij de lsi kan eventueel tijdelijk voor de duur van het Syr i-project toetreden.

In de lsi z, in ook diensten en organen verantwoordelijk (met name het omen de politie) die met reden niet in artikel 84 suw i zijn aangewezen. Het omen levert geen data, maar is betrokken in verband met eventuele strafrechtelijke onderzoek en die uit de contributie van het interverfalsen 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 frauderen misbruik. Bij het ontwerp van het risicomodel beschrijft de Inspectieszw voor welk expediteerfraudevorm het instrument Syr i 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 Syr i vindt in twee fasen plaats.

Fase I: bestandskoppeling

Fase I behelst de bevestiging van data door het ib, dat de bestandskoppeling uitvoert. Het ib koppelt daartoe, afhankelijk van het doel van het onderzoek, momenteel maximaal zo'n 50 bronbestanden, maar dit kan uitbreiden naar gelang de toekomstige behoeften. Het ib vult en beheert vervolgens twee bestanden:

- 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 naast het risicomodel van de Inspectieszw.
- 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

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 ISI brengt data samen van Inspectie SZW, gemeenten, de Belastingdienst, het u.w.v. en de vvb. 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 ISI. De ISI richt zich op de aanpak en voorkoming van arbeidsgerslechte fraude binnen het fiscale en het sociaal zekerheidsdomein en van overtredingen van de arbeidswetten (Wet Arbeidvoorzieningen en de Wet Minimumloon en minimumvakantiebijslag). De interventieteams richten zich op bepaalde branches/sectoren of (stedelijk) gebieden en pakken in de breedte misstanden aan: onderbetaling, schending van regels, misbruik van werknemers-en-regelingen, belasting- en piepmisfraude, uitkeringsfraude, illegale tewerkstellingen en daarmee samenhangende misstanden.¹⁴⁷

De interventieteams onderzoeken branches en gebieden waar de kans op fraude groot is. Daar heeft de vindi plaats op grond van tips en situational analyse, gefaciliteerd door de SIJ, met de hoogste trekant.

Vanaf 2014 hanteert de ISI landelijke thema's waarbinnen projecten worden uitgevoerd: adresfraude, bewoning (recreatieterreinen, huisvesting arbeidsmigranten en wijkgerichte aanpak) en schijnconstructies. Tot en met het tweede kwartaal van 2016 zijn 161 projecten door de ISI goedgekeurd.

ISI-projecten richten zich in de afgelopen jaren onder meer op getoeldebureaus, uitzendbureaus, schijnconstructies, arbeidsmigratie, recreatieterreinen en op probleemwijken, waarbij is gecontroleerd op fraude door illegale tewerkstelling. Recent onderzochte wijken waren bijvoorbeeld Weesp-Noord, De Veluwe in Grijp, Daawendse in Middelburg, de kern van Vals en Meerzicht in Zottemeer. Ook recreatieparken op de Noord-Valuwe, in West-Brabant, Hardenberg/Ommen, Maasdiep en Zundert waren in de afgelopen jaren onderwerp van onderzoek.

De aanpak van adresfraude is in recente interventieprojecten, zoals in de wijk Hoograven (Utrecht), ook een belangrijk themageweest. Voorstellen voor projecten van deelnemers worden te goederkeuring aan de ISI (Stuurgroep) voorgelegd.

147

Brochure: Controle door een Interventieteam, 2012
<https://www.rijksoverheid.nl/documenten/brochures/2016/08/25/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 wijkgordteprojecten is het standaardpraktijk dat, wanneer het interventieteam bij de uitvoering van de controles vastmoed dat er sprake kan zijn van georganiseerde criminaliteit of hennepstief, het riec in die regio wordt geïnformeerd. Indien nodig wordt ook het Bureau bijbobb geïnformeerd.

Voorbeelden: interventieteamprojecten G.A.L.O.P. I en II in Eindhoven ('Gerichte Aandacht Leefbaarheid Ondernemerschap Participatie'), de Value in Cuijk, Redactiepark en 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 riec en het project Landelijke Aanpak Adreskwaliteit (Laak), dat in opdracht van het ministerie van BZK, door de Otu (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 gebruik gemaakt van de landelijke voorbeelddatabank koppelingen risicoanalyse van wat later Synti werd. Van 21 daarvan vond in 2015 rapportage aan de Kamer plaats, het 23e 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 gastoudersonderzoek in Midden-Nederland bijna 6,5 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 gemiddeld 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 Jansen, secretaris van de Landelijke Stuurgroep Interventieteams (Lsi).

¹⁴⁹ Eindrapport Interventieteamproject Gastoudersbureaus, Belastingdienst en Regionaal Platform Fraudebestrijding Midden-Nederland, maart 2012: <http://www.rifn.nl/sites/default/files/content/documents/2016/04/14/eindrapportgastouders.pdf>

Iedere burger kan informeren of hij/zij in het register is opgenomen, zodra meldingen zijn aangekomen. (zie bijlage 2).

Het totaal aan opgelegde belastingen en boetes bedroeg ruim 12 miljoen euro.

- Correcties op toeslagen (stopzettingen en terugbetalingen) ruim 1 miljoen euro.
- Teruggeworpen en beëindigde uitkeringen (bijstandsuitkeringen en op grond van werknemersverzekeringen en volksverzekeringen) en opgelegde boetes: ruim 4 miljoen euro.
- Opgelagde boetes wegens overtreding van de Wet arbeid vreemdelingen: minimumloon- en minimumvakantietoelage: ruim 1,5 miljoen euro.⁶⁰

Het meest valt op dat de Black Box voor de landelijke verzekering van het instrument Syr I in 22 projecten toegepast is, maar er in het eerste jaar er nog een ministeriële goedkeuring gevraagd is voor toepassing van Syr I voor onderzoeksprojecten.

In 2014 zijn geen nieuwe Syr I-projecten begonnen, vanwege andere prioriteiten dat jaar bij de ISI. Deze had voor dat jaar een aantal landelijke thema's vastgesteld, die zich niet (direct) leenden voor deze analyse methode. Daarnaast is er per jaar beperkte capaciteit om op lokaal niveau een zogenoemde wijk- of gebiedsgericht aanpak uit te voeren. Syr I komt zich momenteel niet voor toepassing in projecten waar in een van de landelijk thema's het onderwerp is. Het belangrijkste risicomodel dat in Syr I is ingebouwd, heeft betrekking op risico-indicatoren die in de wijkgericht aanpak kunnen worden toegepast. Wijkgerichte projecten kennen een lange voorbereidingstijd. Een gemeente moet bereid zijn om hierin te investeren en dat vergt lokale politieke toestemming. Daarnaast kent Syr I een zogenoemd Ondernemingenmodel, dat kan worden ingezet om risico's op een bedrijfje te toetsen. Tot nu toe is dat niet ingezet, vanwege het ontbreken van daarvoor geschikte projecten. Het Besluit Syr I is op 12 september 2014 in werking getreden. In de periode voor en na de toelichting op de nadruk op projecten op een van de landelijk thema's. Op dat moment (12/9/2014) was één wijkgericht project in uitvoering: De Valuwe in Guix. 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 waar in wordt verzoekt om Syr I toe te passen: dat is het project G.A.I. op p. II, uit te voeren in de wijk Hanneke als Coöperatie het bedrijf venten in de Hannekestraat in

⁶⁰

Brief rapportage over Syr I-projecten 29 juni 2016.
<https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2016/06/29/kamer-brief-mel-rapportage-over-syr-i-projecten/kamerbrief-mel-rapportage-over-syr-i-projecten.pdf>

Bindhoven. Dit project is in juni 2015 door de ISI 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 ontstond Black Box en vervolgens Syri. Deze mechanismen in een bereikrijke omgeving dat gegevens anonimiseerd 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 te identificeren. Is Pseudonimiseren kan gedaan worden met een procedure waarmee identificeerbare gegevens met een bepaald algoritme worden veranderen door versluiten de gegevens (het pseudoniem). Pseudonimiseren onderscheidt zich van anonimiseren, waarbij het koppelen op basis van informatie uit verschillende bronnen niet mogelijk is.¹⁵¹

De wet op de in september 2008 een op de Wet bescherming persoonsgegevens (Wbpg) gebaseerd toetsingsader 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 risico's indicatoren op specifieke vormen van overtreding expliciet gemaakt.

Syri voldoet hieraan.

De proportionaliteit wordt gewaarborgd doordat deelnemende partijen voorafgaand aan elk project aan de Wbpg toetsen welke gegevens noodzakelijk zijn voor het specifieke opsporingsdoel. Hierdoor wordt de inperking van het recht op privacy zo klein mogelijk gehouden', aldus minister Aasche.

De a.p. (toen cbp) plaatste in zijn advies bij het conceptbesluit Syri i hierbij vragen.¹⁵² Zo vereist artikel 8 van het e.v. met wetgeving bepalingen bevat die regelen welke soorten data mogen worden verwerkt, die categoriën van personen die het betreffen de omstandigheden waaronder dit gebeurt.

De a.p. (toen cbp) plaatste in zijn advies bij het conceptbesluit Syri i hierbij vragen.¹⁵² Zo vereist artikel 8 van het e.v. met wetgeving bepalingen bevat die regelen welke soorten data mogen worden verwerkt, die categoriën van personen die het betreffen de omstandigheden waaronder dit gebeurt.

¹⁵¹ <https://nl.wikipedia.org/wiki/Pseudonimiseren>

¹⁵² Advies aan de Raad van State

<https://doweb.nl/sites/default/files/atoms/files/z2013-00959.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 p is daarop als volgt verwerkt: binnen Syr i 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 Syr i kan worden ingezet en is in de wet de zinsnede verduidelijkt. Hierdoor kan Syr i 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 Syr i verwerkt worden die voor de doelstellingen binnen die domeinen noodzakelijk zijn. Verder merkt de p 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 Syr i. Hierop is de wetstekst aangepast: data mogen enkel worden gebruikt voor het sociale domein.¹⁵³

De p wenste ook dat de minimalisatie met *select before you collect*: eerst bepalen wat je nodig hebt, dan dat aan de eisen. Anders zou het kopiëren van bestanden kunnen leiden tot een *fishing expedition* en zelfs tot willekeur. De p en de Raad van State wilden dat de te gebruiken bestanden inzake Syr i 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 Syr i in dat project aan de daaraan in het Besluit Syr i gestelde voorwaarden is voldaan. Voorafgaand aan een samenwerkingsproject wordt afgevoegd welke gegevens onafhankelijk noodzakelijk zijn voor de bestaande opsporing. 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).
Notaven Toelichting bij het Besluit Syr i (Staatsblad 2014, nr. 320, blz. 17-20)
<http://zoek.officielebekendmakingen.nl/stb-2014-320.html>

¹⁵⁴ Misbruiken onafhankelijk 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=2014D038394

De adviseerde ook om de bewaartermijnen van Syr i aan te passen. Nu is vastgelegd dat de risicomeldingen en de bijbehorende gegevens uiterlijk na twee jaar uit Syr i worden verwijderd.

Er geldt ook een wettelijke geheimhoudingsplicht voor de instanties die over de risicomeldingen beschikken. Immers, een risicomelding ontstaat in de bevestigde omgeving van Syr i, maar komt buiten Syr i terecht. Gegevens die niet tot de definitieve selectie behoren, zullen direct worden vernietigd.

Aanvragen van uitkeringen worden gewezen op mogelijk gebruik van data in een bestandskoppeling, en dat derden, zoals de Belastingdienst, data kunnen gebruiken. Bij de voorafgenomen evaluatie van de Wet suw i in 2020 zal ook Syr i worden geëvalueerd. En de privacyaspecten in openbaarheid worden genomen. Er is reeds een Privacy Impact Assessment uitgevoerd.¹⁵⁵

Syr i is in de mediasoms beschouwd als een uiterste 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 specifiek sociaal 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 vergeerde datakoppeling van Inkt.

Met Big Data-toepassing diemet Syr i in het vizier komt, zou zorgvuldiger en neutraler met indicatoren worden omgegaan: 'Kon een inspecteur voorheen nog zeggen: "Bekijk die jong komt er niet uitrolen 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 Syr i. Die waa machineleest acht een geminimaliseerd proces.'¹⁵⁶

¹⁵⁵ Besluit suw i, 1 september 2014.

<https://zoek.officielebekendmakingen.nl/stb-2014-220.html>

¹⁵⁶ Interview met Hans Berkhout en Ad van Mierlo van vng.kh.n.

Burger wordt straks doorgericht zoals profiel van crimineel wordt opgesteld

http://www.volkskrant.nl/politiek/burger-wordt-straks-doorgericht-zoals-profiel-van-crimineel-wordt-opgesteld-a3758593_15 15 september 2014.

"Syr i is in watch you", 5 november 2014.

<http://argasso.nl/syr/>

7

inleiding

Buiten Syrië en de interventieteams heeft de Inspectieszw. 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. Daar tegenover staat 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. Profileringen van exclusieve relaties ten van de dienstverlening Risicogestuurd werken, op grond van (Big) Data-analyse heeft volgens de op van de Inspectie de toekomst, zo blijkt uit de onderzoeksgaande. Wat behelzen de huidige praktijken, 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 2019 is de Wet aanscherping handhaving en sanctiebeleid szw -wetgeving in werking getreden, ook wel Fraudewet genoemd. De wet geldt voor het gehele szw -domaan en bestaat uit:

de arbeidswetten (Wet arbeidvreemdelingen (w av), Wet minimumloon (w ml), Wet allootarbeidskrachten door intermediairs (w a di), Arbeidsomstandighedenwet (Arbowet) en Arbeidstijdenwet (Atw)),
kinderopvangtoelag,
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 (sovw, okw en onw) en het uuvv (w op / w lo, w v on zw)).¹⁷

Om de mogelijkheden voor opsporing en handhaving van de Inspectieszw. voor te bereiden de Arbeidsinspectie, de Inspectie Werk en Inkomen en de so d (Sociale

157

Wet aanscherping handhaving en sanctiebeleid szw -wetgeving
http://wetten.overheid.nl/BWBR00329577.geldigheidsdatum_04-01-2019

Inspectie en Opsporingsdienst), zijn vermeld. Onder meer met een zwaar accent op analyse van interne, en in toenemende mate ook externe, databestanden. Het meest vergaande onderdeel hiervan vormt 'Gyr 1', dat al in het voorgaande hoofdstuk is besproken. Voor handhaving kwam meer geld beschikbaar. De capaciteit bij u.w.v. 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 eerlijk er systeem (misbruik wordt bestraft), een financiële netto opbrengst van naar verwachting 188 miljoen euro.

Data analyse vormt een subsector in dit voornemen: 'Intensiveren van de handhaving zal niet alleen plaatsvinden door extra budget, maar ook door de bestaande handhaving capaciteit 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 verdeling van gegevens van private organisaties. Hiermee kunnen risicobedrijven geïdentificeerd worden gedoelbaar. Risicooddelen worden geïdentificeerd om de effectiviteit te verbeteren. In jaarverslagen van de Inspectie szw wordt teruggesproken over de bereikte resultaten. Ook de svb en het u.w.v. werken met risicoprofielen en op basis hiervan worden gerichte handhaving activiteiten uitgevoerd.'¹⁵⁹

Uitvoering analyse

Bij de Inspectie szw fungeert de Directie Analyse, Programmering en Signalering als 'denk tank en adviseur' voor de Inspecteur-Generaal (ig) en management. Het team o.s.a. maakt informatieproducten, zoals risicoanalyses. Het verspreiden van risicoanalyses wordt in het Jaarplan 2015 een van de belangrijkste uitgangspunten genoemd:

'Door risicogestuurd 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 5 februari 2015).

¹⁵⁹ Idem.

selectie van te inspecteren bedrijven. Dit leidt tot een afgewogen mix van interventies en efficiënt en efficiënt toezicht.¹⁰

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: 'krijg ze ook omstergeschieds, wettelijke en ontwikkelingen in de omgeving in beeld. Daartoe maakt de Inspectie gebruik van informatie en kennis uit meerdere externe bronnen zoals van Belastingdienst, het u.w.v., de ArbO en de Ind.

Voorbeelden van onderzoek:

- 2015 deed de Inspectie SZW in het kader van naleving sociale zekerheidswetten onderzoek naar de naleving van de inspanningsplicht.
- In het kader van misbruik kenniszorg inspecties tutebij 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 ventilerend opgericht waar in de inspectie onder meer samenwerkt met de Belastingdienst, u.w.v. en Ind.

Sinds 2012 heeft de Inspectie een gericht aanpak om het aantal malafide intermediairs op de arbeidsmarkt terug te dringen, onder meer door samenwerking met publieke partijen als het u.w.v., de Belastingdienst, gemeenten, de politie en waar nodig het om maar ook met private partijen als snou, organisatie van de uitzendbranche en s.n.a., 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. Werk tarieven bopalen

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 geluid via onder andere doelgroep analyses en netwerk analyses. Het resultaat hier van komt in overlog met focusgroepen van deskundigen.

Nader te zien voor een sector of branche om te onderzoeken, bijvoorbeeld horeca, de waserijen of bepaalde detailhandel volgt de object- en subjectselectie

tie, de meest operationele manier van risicoanalyse: welke bedrijven worden doelwit van onderzoek naar onderbreiding illegale tewerkstelling? Dat vraagt. Voor bijvoorbeeld onderzoek naar een migranten worden bestanden van van mensen die Nederland inkwamen en die de ind. verdacht vindt aangegeven tegen bijvoorbeeld de polisadministratie van het u.v.w. om na te gaan of er mogelijk illegale tewerkstelling plaatsvindt. Bedrijven die betreffende personen in dienst hebben krijgen inspecteurs op bezoek. Dit beschouwt de inspectieszw. 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. Deze kennis van inspecteurs wordt vertaald in indicatoren voor data-analyse in bestanden. Bijvoorbeeld een verandering van illegale tewerkstelling toetsen met een de omzet-loonverhouding vanuit de bestanden van de BSA-stand en het u.v.w.

3.

Profilering

Zoeken naar profielen van bedrijven of bestuurders op basis van historische gegevens. Bijvoorbeeld op basis van kenmerken van bedrijven die de wetgeving hebben overtreden, via statistiek gekeken of er een (voorspellend) profiel kan worden gemaakt waarmee bedrijven kunnen worden aangevuld waar de kans op regelovertreding groter is dan gemiddeld. Binnen drie types onderzoek en wettigheid wat wel en niet werkt: trail and error, heel tijdovand. De inzet van data verschildt echt sterk per onderzoek. Voor het ene halen we met een simpele bestandsvergelijking al veel indicatoren boven water, dan weer moeten we een complex data-profiel opstellen, en soms volstaat de kennis en ervaring van de inspecteurs: o.k. a gaat al tijd, dat no of data-analyse bijdraagt. Bovendien is de afdeling afhankelijk van de kwaliteit van de data.¹⁸¹

Inzet systemen

ict is volgens o.k. a geen doorlagerefactor. Louter in de analyse voor Interventietools (I si) wordt gebruik gemaakt van het Syri (Systeem Risico Analyse). Op andere terreinen niet.

Bij de inspectieszw. is in 2011 een aparte data-ovand ingoricht voor het koppelen van verschillende data bestanden, bewaking van de kwaliteit en geautomatiseerde rapportage. De projecten kunnen nu sneller en gebruiksvriendelijker van data-analyse gebruik maken, zegt iszw.

¹⁸¹ Interview met ingez. van de inspectieszw.

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 een Big Data-mining, zo maar correlaties en causaliteit gaan exploreren, maar stellen altijd concrete vragen aan de data. Waaronder miseren de data niet, omdat we niet of nauwelijks werken met persoonsgegevens. We halen de bronbestanden van de Belastingdienst, het uvv en/of overige binnen en passen die toe per project.'⁶²

7.2

externe samenwerking

Met justitie

Samenwerking met politie en helo mis een specialiteitsrein 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 omvallen we onder dewat politiegegevens (Wpg) en zijn we onderworpen aan een vrijheidsvondet zoek van deaard, opsporingsonderzoeken, onder andere naar arbeidsuitbuiting. We kijken in dossiers naar eerder veroordeelde personen en zien om eventueel tekunnen voorspellen waar zich risico's kunnen voordoen. Dat is nog prematuur, maar wel een moedelijom uit te breiden. Dat zijn niet veel data, maar wel boeiend qualtiteitsanalyse. Ook voor de Inspectie szw wordt het werken met data over aldan niet illegale immigranten belangrijker en dus de samenwerking met het Nationaal Vreemdelingen Informatieknocpunt (n.v.i.k.), die alle politie informatie over criminaliteit met vreemdelingen beheert zoals mensensmokkel, illegale arbeid, uitbuiting. In het algemeen kijken we nog porzoek, dus uit oorzakelijk. We zoeken maar voor vorrijking van data per zaak. Dat vergt zorgvuldighandelen. Wij mogen niet zomaar onze data uithet toezicht op de arbeidsmarkt koppelen aan de data van n.v.i.k.' 'Zij mogen dat wel doen, want opsporing en strafrecht mag gebruik maken van data uithet 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 tekijken of zedie met hun datakunnen verrijken. Ook dat vergt eenzelfde regime. Strafrecht is van een andere orde, maar we willen voor de profilering wel meer van toete passen.' Zo is de Inspectie szw op justitieterrein ook participant in loov, die data analyse doet op zoek naar crimineel vermogen. 'We helpen mee in de analyse en leveren onderzoek capaciteit. Wij

⁶² Idem.

tot inzage in, en koppeling van vele bestanden voor data-analyse (zie verder hoofdstuk 3.2.org),¹⁵⁵

Samenwerking basisregistraties

Een bijzondere samenwerking betreft het opwaarderen van de basisregistraties voor adequate gebruik voor onder meer fraudebestrijding. Het grote project Adreswilt uit het ministerie van BZK is daarin een voorloper. Niet 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 maakt de Inspectie SZW veelvuldig gebruik van basisregistraties zoals Basisregistratie personen (brp), Handelsregister en Kadaster, maar mogelijk niet voor spelende in met data-analyse. Daarvoor zijn de databank en niet beschikbaar. De basisregistraties tezamen vormen een datareservoir, maar analyse daarvan op grond van de principes van Big Data-analyse vormen nu nog een 'stap aan de horizon'.¹⁵⁶

7.3

toekomst

Jaarplan 2016

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

¹⁵⁵ Brief van staatssecretaris Van Rijn (vrs) 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>
 Opzoning zorgfraude komende jaren taak van Inspectie SZW, Nieuwsbericht Rijksoverheid.nl, 14 december 2014 | <http://www.rijksoverheid.nl/nieuws/2014/12/14/opzoning-congruente-komende-jaren-taak-van-inspectie-szw.html>

¹⁵⁶ Stelsel van Basisregistraties.
<http://www.digitaaloverheid.nl/onderwerpen/stelselinformatie/nl/stelsel-van-basisregistraties> (geraadpleegd 8 februari 2015).
 Basisregistraties als fundament voor modernisering toezicht bij Inspectie SZW, Ruud Boot (ict u) en Wimfred Grahoff (Servicepunt Basisregistraties), zonder datum.
http://www.digitaaloverheid.nl/images/stories/stelsel_van_basisregistraties_basi-op-rac-tioe-szw.pdf (Geraadpleegd 8 februari 2015).

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

- 2016 ligt bij het toezicht op het domein *Landelijk werk* meer nadruk op grootschalige onderzoek en van complexe fraudes en constructies. Dat past bij de focus van de inspectie op notorie overtreeders en misstanden, maar betekent ook dat er in dit domein minder reguliere inspecties plaatsvinden.
- **2016 inspectiecoördineren** tijd inplannen voor ongevals onderzoek. Dit is nodig omdat de behandel tijd per onderzoek toeneemt. De ongevals onderzoek en leveren informatie over potentiële misstanden en voor risico-analyse. Zo trad naar voren dat er veel meer ongevallen plaatsvonden met de toename van inhuur van zzp'ers in de bouw.
- De inspectie heeft vastgesteld in hoe **specifieke sector** zijn worden bevestigd door andere bronnen, op grond van data uit de Nationale Enquête Arbeidsomstandigheden (neas) van het CBS en uit Arbeid in Bedrijf (aib) door de inspectie zelf. Op basis van deze gegevens is een maat voor risico op blootstelling opgesteld.

De inspectie heeft 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 van de analyse van de risico's, met een 'indicatieve' van 22 hoofd risico'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 tot' traden naar voren als gesterische 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 (vho), de inspectie jeugdzorg (jz) en de inspectie Veiligheid en Justitie (ivenj), ook in een al bestaand coördinerend orgaan: Samenwerkend Toezicht Jeugd (stj).

Meerjarenplan 2015-2018

Genoemde passage over 'risicogetuurd werken' keert ook letterlijk terug in het Meerjarenplan 2016-2018 van de inspectieszw. In een risico diagram staan de uitkomsten van het combineren van analyse van bestanden en meldingen van personeel en derden. Het betreft risicothemas en verschillende risico's. Risicoanalyse neemt een voorname plaats in het nieuwe programma. In de komende jaren zal de

¹⁶⁷ Jaarplan 2016 Inspectieszw http://www.inspectieszw.nl/Images/jaarplan-2016-inspectieszw_tom_335-369-04.pdf

Inspectie SZW de methode van signaleren en het afgeven van signalen verder ontwikkelden.¹⁰⁸

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 dataproberen 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 profielen van verdacht bestuurders, moeten we een risicoanalyse in onze privacyonderbouwing voor hebben. We proberen zoveel mogelijk te beschrijven hoe we voldoen aan deelen van de Wbp waaronder de proportionaliteit en subsidiariteit. Daar plagen 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 samenwerkingsovereenkomsten zijn nu doorlopend onderdeel van het werk, om het goed juridisch te onderbouwen. Dat is erg belangrijk, want we hebben zelf al wel nodig dat we voor meer risico gestuurd werken altijd data van andere partijen nodig hebben.'

Inzage geven in deze afspraken is niet mogelijk. De Inspectie zegt te transparant in te willen zijn, maar bestaat nog niet goed op papier. 'We moesten steeds per project met de Belastingdienst, het UWV en de inderhoud 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 stellen we er veel inspanning in.'¹⁰⁹

¹⁰⁸ Meerjarenplan Inspectie SZW 2015-2018
http://www.inspectieszw.nl/Images/Meerjarenplan-InspectieSZW-2015-2018_tcm335-359027.pdf

¹⁰⁹ Interview met eerdergenoemde.

8

inleiding

Het u.w.v. heeft een heldere, voortvarende visie op de inzet van data voor fraudebestrijding. Het u.w.v. is actief met het ontwikkelen van risicoprofielen. Het u.w.v. heeft een aantal onderzoek en gedoeën 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 u.w.v. heeft een helder toekomstbeeld aangaande data-analyse op grond van klikgedrag. De dataverzameling richt zich ook op het inschalen van individuele personen in een categorie met behulp van een risicoprofiel, gebaseerd op hun 'kans' op niet naleven van de regels. Ook voor gezondheidsfraude kan risicoprofielen de handhaving helpen, met in beeld gebrachte 'verondergevalen'.

Hoezet u.w.v. data-analyse op, met welke verwachtingen en hoe komen privacy, it en samenwerking aan bod? Daarover handelt dit hoofdstuk dat grotendeels steeit op vraaggesprekken en toelichtingen van betrokkenen deskundigen. Zet onder een scherp beeld van de mogelijkheden en grenzen van u.w.v. op het terrein van data-analyse.

8.1

doel en verwachtingen

Het u.w.v. formuleert dit als volgt: 'Het u.w.v. werkt continue aan het toepassen van de nieuwste technieken op het gebied van it en data-analyse om de beschikbare klikgegevens optimaal te benutten bij het voorkomen en opsporen van misbruik van uitkeringsgeld. Hierbij houdt het u.w.v. altijd de privacy nauwlettend in de gaten en overlegt, indien nodig met onder andere de Autoriteit Persoonsgegevens'.¹⁷⁰

8.2

tot standkoming van syst

Momenteel ligt het accent nog op bestandsanalyse op basis van inhoudelijke ideeën en nog niet op data-mining: de data laten spreken. Wel is bij het u.w.v. consequent het benadrukken om informatie aan te binden, maar het gaat om de toestand van een uitkeringsgerechtigde aan een fraude- of bezwaarsaak is niet mogelijk. Dit heeft een technische oorzaak: het is voor het u.w.v. nog niet mogelijk om de geschikte bestanden met kenmerken die een relatie hebben met de kans op

170

Interview met Ernst Veenhoven, Strategisch beleidsadviseur u.w.v. en Michael van Eek, Risico-Ordezoeker u.w.v. Zij zijn verantwoordelijk voor alle verdere taken in dit stuk van het u.w.v., tenzij anders vermeld.

regelovertreding te koppelen. Alleen wv-onderdelen welk en met eigen registratie-systemen en dat zijn workflow- en verantwoordingsystemen die niet (helemaal) op elkaar aansluiten. Sommige systemen bevatten gesonde documenten en kunnen daarom geen relevante data genereren. Echter, na het slechten van de technische hobbels wordt dat amining op grond van bsn, maar ook geanonimiseerd, wel mogelijk. Dan nog moet een aantal voorwaarden worden voldaan, bijvoorbeeld aangeende privacy en relevantie van onderzoek. Zo is het aantal geconstateerde overtradingen voor bepaalde regels te laag voor wv om op grond hiervan risico-indicatoren te kunnen bepalen. Overigens is niet a priori sprake van 'pakkans' of schuld; Het kan zijn dat een klant die regels niet kent of niet weet hoe hij ze moet naleven. Dit is volgens het wv in het grootst deel van de geconstateerde overtradingen derzaden. Degenen die de regels niet willen naleven, vormen volgens wv de kleinste categorie.

8.3

uitvoering (en resultaten)

Het wv is wel actief met het ontwikkelen van risico-profielen. De dataverzameling richt zich op het indelen van individuele personen in een categorie met behulp van een risico-profiel, gebaseerd op hun 'kans' op niet naleven van de regels. Het wv heeft echter een voorkeur voor het handhaven met wat zij noemen 'vrauwondercijfers': gegevens die moeilijk met elkaar te rijmen zijn of wel anomalieën. Dit droogt momenteel maar bij een succesvol handhaven dan het borden van klanten op overtrading op grond van analyse van databestanden, die zou moeten leiden tot risico-profielen. Het wv heeft de volgende onderzoeken gedaan:

1. Risicomodellen opgesteld voor het selecteren van klanten voor huisbezoeken en telefonische controles, gebaseerd op uitkeringsbestanden (wv, wao, wia, et cetera) en frauderegistraties. Deze modellen bevatten kenmerken als leeftijd, geslacht, soort uitkering, uitkeringsduur, onthoogd, sector, toelag, bodaggingen en redive (eerder regelovertradingen). Als methode is gekozen voor logistische regressie (kansverhoudingen met verschillende variabelen), om twee redenen:
 - Het **hieldtoets** tevens geschikt beter voor het selecteren van een specifiek aantal te controleren klanten dan een beslissboom.
 - Het is **inzichtbaar** kan worden van een neurale netwerk, terwijl de voorspelling nog onbegrijpelijk is.

Het voordeel volgens de wv-woordvoerders is ook kan met een logistum regressie-model voor de wv, periodiek voor alle wv's, via een expliciete formule en dus transparant, de kans op regelovertrading worden berekend en een, door de controlecapaciteit bepaald, specifiek aantal wv's met de hoogste kans op regelovertrading worden geselecteerd voor controle.

Dit heeft de voorkeur boven louter een beslisboom of via een neurale netwerk selecteren. Met een beslisboom kan alleen een aantal categorieën en geen precies aantal worden geselecteerd. Een model op basis van een neurale netwerk levert geen expliciete formule op die bij navraag gepresenteerd kan worden en is dus niet transparant.

Bij het risicomodellw bleek over 2014 ruim een verdubbeling van de reflexies, namelijk van 9,8 procent bij de de controle tot 24,6 procent met behulp van het 'w-w-model'.

Momenteel vindt reeds 90 procent van de controles van het u w v plaats op basis van risicoprofielen en nog 10 procent van de controles asselekt. Door verpelijkking van de resultaten van de controles met risicoprofielen en de controles bij asselekt gekozen k anten kan de effectiviteit van het risicoprofiel worden bepaald en het profiel zo nodig worden aangepast. Tegelijk kan worden voortkomen dat nieuwe risico's niet worden ontdekt.

2. **Vrijwilligerswerk** het overtreden van specifieke regels (volgende solliciteren, melden van inkomsten, vakantie en vrijwilligerswerk, e.d.), maar ook profielen van k anten die geen gebruik (kunnen) maken van het e-kanal of waarbij de overtreding vermindert verwijgbaar was. Ook hierbij maak t het u w v gebruik van uitkeringsplanden en frauderegistratie, maar ook van sonar (het registratiesysteem van Werkbedrijf met kenmerken als opleiding en beroep) en van telefoniedata dat wil zeggen de door k anten gestelde vragen via de u w v-telefoon die in databank en zijn versprekt tot data. Dit levert de u w v een basis op voor het ontwikkelen van nalevingscommunicatie en input voor de ontwikkeling van instrumenten voor het baroceren van nalevingsgedrag. Voorbeelden? Zo ontwikkelde het u w v risicoprofielen voor de nalevingscampagnes 'Werken met een uitkering' en 'Vrijwilligerswerk' op basis van de kenmerken van k anten die werkzaamheden niet melden en via u w v-telefoon vragen stelden over vrijwilligerswerk en het mogen bijdragen. Deze profielen maak ten het mogelijk om de campagnes op de juiste doelgroep te richten. Hierbij werd overigens wel gebruik gemaakt van beslisbomen omdat niet ind vidueel blok k anten, maar risicogroepen werden benaderd.

3. **Vrijwilligerswerk** eams, ontwikkeld in samenwerking met de Belastingdienst, de v v r e f / Gemeent en de Inspanningszw met gebruik making van Syri (Systeem Risico-indicatie). Dit is een systeem om bestanden door een *trusted third party*, i.e. het v h, te koppelen an k anten te selecteren op basis van een vooraf vastgesteld risicoprofiel. Alleen de namen van k anten met een hoog risico worden door het lo geleverd aan de interventieteams. Doordat zo ook bestanden van bijvoorbeeld energie- en waterleidingbedrijven gebruikt konden worden, nam de opbrengst van de interventieteams sterk toe.

Interventieprojecten zijn gericht op diverse vormen van fraude, waaronder zwart werk en in woonfraude. Zowel in het eerder genoemde project *Waterproef* gebruikte men van het kenmerk waterverbruik. Ook kon hiermee bij een zeer hoog waterverbruik zwart werk worden getraceerd, bijvoorbeeld als thuiskapster, of het onderhouden van watplantages.

4. Onderzoek naar anomalieën ofwel verdachte combinaties van kenmerken, in plaats van kansen. In dit kader probeert het u.w.v. gegevens te achterhalen over niet gemiddelde inkomsten en gefingeerde dienstverbanden. De Politie-administratie met papieren over alle dienstverbanden vormt de voornaamste bron. Uit everde concrete signalen op waar meerdere betrouwbare lant en geconfronteerd konden worden en om uitlag gevraagd.

Mit deze onderzoeken verkant het u.w.v. de koppeling van het koppelen van dat bestanden bij het opsporen van misbruik van uitkeringsgelden. Vooral nog 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 Politie-administratie dienstverbanden te selecteren en te controleren die na de faillissementen niet zijn aangemeld of waarbijkun t voor het faillissement het loon aanzienlijk is verhoogd.

Een ander voorbeeld zijn zelfstandigen met w.v., die bij u.w.v. maar weinig gewerkte uren melden, maar bij de Belastingdienst zelfstandigenafrak claimden, omdat ze minstens 1225 uren per jaar aan hun bedrijf besteedden.

Resultaten

Cijfers over de resultaten van handhaving:

Onderzoeken (relatief bedrag)	2013	2014
Onderzoeken	30.539	71.542
Gevoerd onderzoek (bedragen)	46.655	65.505
Bemiddeld bedrag (x € 1.000)	71.899	86.200
Opgelegde boetes	37.698	90.048
Boetebedrag (x € 1.000)	23.257	55.294
Waarschuwingen	5286	9225
Proces-verbaal (OV)	302	278
Onderzoeken (relatief bedrag)		
Opgelegde boetes	90.294	97.396
Waarschuwingen	31.853	51.492

De verbetering van de resultaten in 2014 ten opzichte van 2013 is deels te danken aan bovengenoemde onderzoeken met risico profielen en deels aan meer ingezette handhavingsopties. Immers, het u.w.v. ontving van het ministerie van szw

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

8.4

hinderpalen en vraagtekens

De afgelopen jaren is geblijven dat de inzet-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 veiligheidsproblemen. Dit kan ertoe leiden tot de ontwikkeling van Big Data-analyse. Het uwv voerde overleg met de Autoriteit Persoonsgegevens over inzet van risicomodellen voor huisbezoeken en telefonische controles en over het registreren van begeleiders en specialisten bij Ziekteverzuim- en WIA-klanten. Dat werd akkoord bevonden, aldus het uwv.

Ook voerde de Inspectieszw. namens het uwv en de andere deelnemers aan de Interventiestrategie overleg over het koppelen van data over onder andere water- en energietoelagen met de Syrië-markering als opvoeding van de overheid. 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 voorkomen gebeurt in veel besproken plannen voor handhaving terug, ook door het kabinet geprepareerd. 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".⁹¹

8.5

toekomstige voornemens

Het uwv is voornemens om het zwaartepunt in de preventieve handhaving te verschuiven van klanten met name naar klantgedrag: het volgen van gedrag van uwv-klanten via online linksoorten (internet, apps). Het uwv wil zich richten op het online informatie verzamelen van custom er journeys: hoe gedragen klanten zich online en wat kan als afwijking en voorafspijkend voor regeloverbrenging worden gekenmerkt. Vervolgens kan het (afwijkend) gedrag worden beïnvloed.

⁹¹ 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 uiteindelijke sanctie.

Het traceren van patronen in onlinegedrag is samenhangen met het afwijken van de regels is volgens het u.w.v. belangrijk in het preventief ontdekken van het niet weten, niet kunnen of niet willen naleven van de regels. De profielen gebruikt het u.w.v. om klanten met afwijkende kenmerken te stimuleren tot naleving via een op hun afgestemde interventie: herinnering, waarschuwing, concreets (gewetens-)verzoek of opdracht.

r uel (Real User Experience Insight) is een database opgebouwd uit klik- en navigatiegedrag van klanten op werk.nl. Der uel-data worden opgeslagen in een time-series format. Ieder datapunt bevat onder andere: een tijdstip en tijdsduur, sessie, opgevraagde webpagina's op werk.nl en klantgegevens zoals header, http statuscode en ip-adres.

r uel biedt u.w.v. inzicht in het onlinegedrag van klanten op welke momenten, en vanuit welke plek/ computer de klanten in contact zijn met het u.w.v.

Datawarehouse wordt in de nabij toekomst ook toegepast op sociale en andere registratiesystemen. In sociale steun gegevens zoals o.v. inhoud sollicitaties, het laden van berichten en uitvoeren taken door klanten in diensttijd lopen en tijdsduur. Of tevreden in hoeverre voldoet de klant aan de inspanningsverplichtingen die samenhangen met de uitkering?

u.w.v. voert structureel analyses uit op r uel-data en maakt hierbij gebruik van het IBM QRadar Security Intelligence Platform. Der uel-data heeft onder andere bij het opsporen van DigiD-fraude een bijdrage kunnen leveren.

Vooral Logius en de Belastingdienst hebben gediend als inspiratie voor r uel. Een andere bron voor deze dataverzameling en sturing is het gedrag van klanten met betrekking tot de inlichtingenplicht. Zo kijkt het u.w.v. of w.w'ers vanuit het buitenland inloggen en controleren dan of ze ongemeld met vakantie in het buitenland verblijven. Zo ja, dan kan dit reden zijn voor een controlebezoek, zogenaamde flitscontroles.

Een tweede voorname 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 diagnostici kunnen bevatten, wat stuit op privacybezwaren inzake het medisch geheim.

Dit kan worden opgelost door een met r uel (zie boven) vergelijkbare aanpak met screening toe te passen en alleen de verwondergevallen te de-anonimiseren en door aan medische telaten beoordelen alvorens een fraudeonderzoek te starten. Ook is er naar aanleiding van eerder fraudegevallen een registratie van begeleidende specialisten opgezet, maar die wordt nog onvoldoende gevuld.

Wat behelst 'geteenvorming'?

Met behulp van gegevens in de bestanden van Sociaal Medische Zaken (smz) van het u.w.v. kunnen met profielen bijvoorbeeld de volgende verwonderingen worden gesignaleerd voor nader medisch (cassier)onderzoek:

Profiel 1: De cliënt heeft een diagnose met een gunstige prognose, is jong, heeft de langere tijd een wia 80-100 uitkering en had een hoogdagloon. Voor deze cliënt is het gunstig dat hij nog een volledige arbeidsongeschiktheidsuitkering ontvangt en daarom is er een reëlekans 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 andere fraudes waar bij psychiater's valse medische diagnoses opvulden en samen met anderen uitkeringen in stilte opvullen!

Een derde voorname 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 u.w.v. heeft hierop middels web crawling en web scraping gegevens kunnen downloaden van klanten van het u.w.v.

Facebook en dergelijke worden tot nu toe alleen gebruikt voor het 'verrijken' van een fraudemolding 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 u.w.v. een protocol opgesteld teneinde te voldoen aan privacyregels.

Een vierde voorname is dat u.w.v. meer gebruik wil gaan maken van bestanden van derden. Zou het u.w.v. bestanden van de Kamer van Koophandel aan de eigen bestanden koppelen om werken als zelfstandige te kunnen traceren, evonds (relaties tussen) personen achter te liaan met fraude en gefingeerde dienstverbanden.

Hetzelfde geldt voor data van der dw., bijvoorbeeld om klanten met 'klusbusjes' te traceren die worden ingezet voor zwarte werken. Ook de duo-bestanden zijn van belang vanwege studiefinancieringen het volgen van een opleiding zonder toestemming van het u.w.v.. Al deze voorname bevonden zich nog in een verkennend stadium begin 2016.

Samenwerking met derden

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

u.w.v. GegevensDiensten (ugd) wisselt bestanden uit, zoals met de Belastingdienst. Deze ontvangt adviesdienstverbandgegevens uit de Politieadministratie en

verschafft aan u.w.v. onder meer data van personen die zelfstandigenaftrek ontvangen en personen die werk en voor mensen met een pg.b. Logius levert aan het u.w.v. ip-adressen van klanten die via DigID inloggen op de site werken, waarvan het bsn dus bekend is. Bureau Keteninformatisering Werk en Inkomens (bkwil) levert het u.w.v. de bgba-gegevens. De ind levert aan het u.w.v. de aanvragen voor gezinshereniging.

Organisaties als het u.w.v., de dwi en des vb delen hun gegevens via het bkwil. Een aantal jaren geleden zijn ook diensten uit het opsporingsdomain, zoals de Inspectieszw., aangesloten. 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 leveren. Daardoor kunnen ze het gebruik worden in te korten.

Het u.w.v. 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. Dit mag louter worden geraadpleegd.

inleiding

Desvb 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). Desvb zet data-analyse in om fraude te beperken en ontvangt daartoe aanvullend budget.

Nauw samenwerking met andere diensten moet helpen om onder meer 'business case intensivering Toezicht van de svb' tot een succes te maken: dus winst maken op de intensivering. Daarnaast is er veel aandacht voor de svb met de inzet van data- en risicoanalyse en eventueel profilering bij het achter een stuk bescheldener dan van veel andere in deze studie behandelde instanties. Dit is ongetwijfeld mede een gevolg van de omvangrijke (en politieke) problemen bij de uitvoering van taken.

Deze aanvds komen onderstaand aan bod bij de beschrijving van de fraudebestrijding door desvb, de zorgen om privacy en de problemen in de samenwerking.

9.1

doel

Desvb 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 uuv en desvb te besparen op uitkeringen. Dit doen het uuv en desvb door meer in te zetten op preventie, toezicht (controle), opsporing en afdoening.

Bij een brief van 4 oktober 2019 over dit onderwerp bood het kabinet de Kamer aan pakket 'intensiveringsmaatregelen'.¹⁷² Er werd een nauwe samenwerking aangekondigd tussen de Belastingdienst, de in d, het uuv en de Inspectieszw 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 vroege dood in dobijs, maar minister en staatssecretaris lichten data 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 garantstat-

172

Kamerbrief over intensivering toezicht in het sociale zekerheidsdomein, 4 oktober 2019, minister Asscher en staatssecretaris Klijnsma van szw <https://www.rijksoverheid.nl/documenten/kamerstukken/2019/10/04/kamerbrief-over-intensivering-toezicht-in-het-sociale-zekerheidsdomein>

ling bij een gezinshereniging en tal van andere doeleinden. Werkgevers en (pseudo)werknemers kunnen samenspannen in een lucratieve vorm van fraude, die leidt tot onacceptabele maatschappelijke uitkomsten op het vlak van de arbeidsmarkt, desoortezekerheid, belastingen en immigratie.¹⁷³ Het uitwerken van de Inspectieszwaarten extrapersonaal, onder meer specialiseren in data-analyse. De maatregelen zouden naar verwachting 7,5 miljoen euro kosten en 9 miljoen extra opleveren.

De extra investeringen door de svb op fraudebestrijding zouden in de praktijk echter veel geringer zijn, en vooral gericht op samenwerking en pensioen van wvb en/of wvb-uitkeringen vermogen in het buitenland. In een aparte brief informeert de minister Asscher de Tweede Kamer over de 'businesscase' intensivering Toezicht van de svb, een bevoegdheidsverdeling in de leefwereld.

1. extra opactiteit 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 gegevens uit de administratie van de svb te gebruiken en te verspreiden, te onderzoeken en te verspreiden, te onderzoeken en te verspreiden. De svb zou de onderzoeksopdrachten uitbreiden om vijf keer zo veel steekproefonderzoeken te verrichten: van 1000 naar 5000. Daarnaast zouden 500 extra onderzoeken worden ingezet om nieuw risico's te identificeren. Kosten: jaarlijks 2,5 miljoen euro met verwachte besparingen in 2015 van 2,7 miljoen euro, door cumulatieve van de in voorgaande jaren behaalde besparingen oplopend tot 4,9 miljoen in 2018 euro;
3. uitbreiding risicogericht onderzoek in het buitenland met het Control-to-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 in 2018.¹⁷⁴

Dit vergaet investering in de professionalisering van de risicoanalyse, mede gericht op nieuwe, met name digitale, frauded vormen. In totaal zou een kleine 30 miljoen euro aan extra investering in de periode 2015-2018 tot een extra besparing van ruim 40 miljoen moeten leiden.

173 Kamerbrief aan de Tweede Kamer over de 'businesscase' intensivering Toezicht van de svb, een bevoegdheidsverdeling in de leefwereld, 30 april 2015.
<https://www.rijksoverheid.nl/documenten/kamerstukken/2015/04/30/kamerbrief-aan-de-tweede-kamer-over-de-businesscase-intensivering-toezicht-van-de-svb-een-bevoegdheidsverdeling-in-de-leefwereld>

9.2

uitvoering

De Bedrijfscoördinatoren II handhaving van desvb zijn binnen de desvb verantwoordelijk voor data-analyse in het kader van de bestrijding van fraude. Zij zijn zelf geen professionele data-analisten, maar binnen de Businesscasenlijstverlening Toezicht wordt de desvb-formatie van handhavers ondersteund door professionele analisten.

Ondanks de politieke aansporing vervalt in de businesscase wijzen de coördinatoren ⁷⁴ erop dat de aard en omvang van fraude bij de volksverzekeringen veel beperkter zijn dan bij meer fraudegevoelige regelgeving als de wv en de wv b (Hertspatiwet). Waarom zal de meerwaarde van de professionalisering van data-analyse dan ook van een andere orde zijn dan bijvoorbeeld bij het uuv. Per onderdeel van de volksverzekering betreft, zijn dit de bevindingen.

- Fraude bij de kmoerbijdrage komt voor, maar het gaat om weinig geld.
- De wv of fraude bij de kmoerbijdrage komt ook wel eens voor, maar gaat om grotere bedragen.
- In relatieve zin komt fraude meer voor bij de Anw dan de

Desvb analyseert de eigen bestanden en werkt ook samen met partners in binnen- en buitenland. Zo is de Maritieme Oep Fraude-analisten volgens de desvb actief met uitwisseling van tactische informatie over de ontwikkeling van fraude. Dit is een initiatief vanuit het Programma Compositie Overheid. Voord 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.

Desvb werkt mee aan een project waarbij gerichte casussen worden uitgewisseld met de Belastingdienst en inspectie diensten om mogelijke postbus ondernemingen, doorheen constructies of anderszins constructies die relevant zijn op premieontwikkeling, tijdigheid en omvang en gezamenlijk aan te pakken. Daarnaast heeft de desvb een risicoanalyse uitgevoerd die leidde tot het verbeteren van de processen voor de afgifte en ontvangst van de Afsluitingen (bij detacheringen). Dit vloesdoort uit een Actieplan Schijnconstructies van de minister van szw.

Ook op andere fronten wordt met ketenpartners als de Belastingdienst en inspectie diensten gezamenlijk data-analyse verricht: bilateraal wisselen de in de desvb informatie uit om gezamenlijk risico's vast te stellen. Dit betreft onder meer mogelijke risico-indicatoren voor fraude met pensioenen of uitkeringen ingeval de gerechtigde revalidatie onrechtvaardig verlijst status in Nederland heeft. Als er inderdaad aanwijzingen voor fraude worden gevonden, kan een bestandsvergelijking worden opgezet.

⁷⁴ Interview desvb met Paul Burroughs en Frits Warner 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 rechtgevendepartner hebben plaatsgevonden, te onderzoeken. Onderzoek heeft uitgewezen dat in deze gevallen een verhoogd risico bestaat van een niet-gemelde gezamenlijke huishouding met een nieuw partner waardoor de nabestaandenuitkering moet worden beëindigd.

De twaalingenfraude bij de kinderbijslag (kinderbijslag werd aangevraagd voor niet-bestaande twaalingen) in de jaren negentig van de vorige eeuw bleek te worden door data analyse van degenen bestanden. Als in een bepaald land of streek of stad opvallend veel kinderbijslag voor twaalingen 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 Adreswiltet (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 verkrijgt wel 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-persoon 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 die brp omdat de persoon feitelijk in het buitenland woont.

9.3

resultaten

Data analyse op zodanig moet bij de svb verder ontwikkeld en geprofessionaliseerd worden. Degenen interview de svb-medewerkers willen zich hoeden voor presenties 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 gemeenschappelijk lastgroepen. Het betrof tot nu toe kleinsteekproefsgewijs onderzoek om vast te stellen of een mogelijk handhavingprobleem zich daadwerkelijk voordoet.

Een historisch apart voorbeeld is de persoon die omguttergaten, betrekend als pgb's. De uitbetaling ging over naar de svb. Staatssecretaris Van Rijn van vws noemde ook de fraudebestrijding als voorbeeld, juist gezien de mogelijke analyse en koppeling van bestanden. 'Doordat de svb nu op een centraal punt diepgangbestanden beheert, nemen de mogelijkheden voor analyse en controle van deze bestanden op fraudeover diepgangbestanden toe. Fraude kan eerder en beter wor-

den opgespoord en de resultaten kunnen gedeeld worden tussen zorgkantoren, gemeenten en zorgverzekeraars.¹⁰⁵

In de praktijk sneuwerde dit echter het afgelopen jaar onder in de grote problemen met de uitvoering van pgb-voorziening door desvb, 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 desvb en de inspectie szw wel vruchten te kunnen plukken van bestandsanalyse ter bepaling van risicofactoren.

Naar verwachting zal de Directie pgb van desvb in 2016 starten met systematische risicoanalyses waar nodig maatregelen nemen om het fraude risico in te perken.

Desvb kende behalve politieke tegenstand ook iot-problemen, die de overheid en bestuurskantoren in de breedte treffen. Zo uitte 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.¹⁰⁶ Ook desvb, het u.w.v. en gemeenten streven naar een risico-gerichte controle en handhaving. Desvb heeft daarvoor het nieuwe Multiregelingsstelsysteem (mrss) in ontwikkeling. Hierbij wordt via risicoscan en risicoprofielen steeds gericht en volgens vaste uitvoeringsprotocollen gecontroleerd.¹⁰⁷ Volgens de bevindingspersonen zou potentiële frauderelleners opgespoord worden met profielen van 'uitlekingsituaties' en ook fenomenen zoals faillissement-, jobcoach- en medische fraude. Al door risicoprofielen worden de komende jaren vergeleken en geëvalueerd tussen de verschillende partijen in de handhaving keten. Zo wordt een steeds preciezer beeld gekregen van (potentiële) fraudeurs.¹⁰⁸

Dit belangrijke Multiregelingsstelsysteem werd echter een iot-debacle. Eten nederkondigen – Johan Hakenberg, iot-dekundigen Lienke Sneller, hoogleraar tegevoegde waarde bij Nyenrode Business University – adviseerden om te stoppen met het project, nadat oordelend negatief oordeelde Desvb zagde naar aanleiding van het debacle het contract met bouw- en Capgemini op. Navraag bij desvb leert dat de zaak voor arbitrage is voorgelegd. Desvb kijkt tot en zo ja

¹⁰⁵ 'Terugblikken vervolg pgb-fraude-aanpak', brief staatssecretaris Van Rijn van u.w.v. aan de Tweede Kamer, 29 januari 2016 (<https://www.rijksoverheid.nl/documenten/kamerstukken/2015/01/29/kamer-brief-over-terugblikken-vervolg-vgb-fraude-aanpak>). Bijlage A: Alchifit brief 'Signaleringspgb-fraudeonderzoek inspectie szw', 31 oktober 2014 (<http://www.rijksoverheid.nl/documenten-en-publicaties/brieven/2014/10/31/alchifit-brief-signaleringspgb-fraudeonderzoek-inspectie-szw>).

¹⁰⁶ 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-fraude-aanpak-handhaving-en-naleving>).

hoe zij delen van het systeem alsnog in gebruik en. Er was bijna 44 miljoen euro meegemoid tot dan toe.¹⁷⁷

Het mrs-systeem zou aanvragen en mutatie die aan bepaalde risico profielen voldoen, eruit filteren voor nadere handmatige controle en behandeling. Nu dit niet kan, restert 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 mededochtelijke ophef over (mogelijke) fraude al sturend kan werken. Zo is het goedkoop en een moudig urn jensen te leveran de en 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 (n vik) 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 voordoe, alvorens de alarmbel te luiden. Dat is dan ook de lijn van de svb.¹⁷⁹

Het karakter van fraude is internationaal geworden. Met de toegenomen immigratie en arbeidsmigratie is het belang groter geworden om ook internationale fraudebestrijding te combineren 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, Roemeniën en Bulgarije. Zij werken samen met debuitlandse autoriteiten en verzamelen informatie ter voorkoming en bestrijding van achterconstructies en uitkering fraude.

¹⁷⁷ http://www.svb.nl/int/af/over_de_svb/actualiteiten

wikkeling_mrs.jsp (Inmiddels verwijderd)

Bijlage 2- Eindrapport Externedeskundigen -svb Tien/ Ontwikkeling van het Multi Regelingen Systeem (mrs)

<https://www.rijksoverheid.nl/documenten/rapporten/2014/02/07/bijlage-2-eindrapport-externedeskundigen-svb-tien-on-ontwikkeling-van-het-multi-regelingen-systeem-mrs>

Mislukt mrs levert svb stop op van 43,7 miljoen', Computable, 2 september 2014

<https://www.computable.nl/artikel/nieuwsoverheid/5168098/520448/mislukt-mrs-levert-svb-stop-op-van-43-7-miljoen.html>

¹⁷⁸ Interview met Paul Burrough, Prits Warner, svb.

¹⁷⁹ Idem.

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

Ook desvb ervaart enerzijds de maatschappelijke en politieke roep om strengere handhaving en anderzijds de zorgen om privacy. Een ontdekt fout met privacy levert direct 'straf' op van de toezichthouder of deredhr. Desvb is dan ook voorzichtig met datamining en gegevensuitwisseling. Voorgenomen activiteiten worden altijd voorafgegaan door een Privacy Impact Analyse¹. Het huidige maatschappelijke klimaat is niet geschikt voor het opzoeken van privacygrenzen of voor experimenten voor handhaving met ongewisse bijeffecten.¹⁰⁰

In 2013 vroeg Desvb bij het Landelijk Bureau van Klanten (melde) over vermogen in het buitenland te onderzoeken en daarmee mogelijke onterechte afdoelkeeringen vast te stellen. Daarop kwam protest van Nederlandse belangenorganisaties, die meenden dat conform de privacywetgeving alleen bij gerichte verdenkingen dataopgevraagd mogen worden en toepassing van een 'sleepnet' in de vorm van analyses van complete bestanden aan buitenlandse uitkeringsgerechtigden onjuist is.

Privacy is een voorwaarde voor Desvb. Zo kreeg Desvb in 2007 kritiek na een uitspraak van de Autoriteit Persoonsgegevens wegens het gebruik van waterverbruikgegevens omdat de hoogste van dat verbruik een indicator is voor mogelijke uitkeringsfraude. Die wetelijke basis hier voor bleek bij Desvb te ontbreken. Inmiddels is de wet aangepast en is Desvb wel bevoegd om deze gegevens te gebruiken.

De discussie rond Syr i speelt ook bijv.b. De uitbreiding van wettelijk mogelijkheden met het Syr i-besluit levert de Landelijke Structuur Interventieteams volgens de vboedhr juist een 'privacyvriendelijke' omgeving op voor bestaand orgeliking. Hierin kunnen gegevens worden verwerkt van nutsbedrijven (water, energie) en woningcorporaties (bevoening). Gebruik van de nieuwe mogelijkheden is nog bescheiden. De Inspectie szw is nog bezig met een project 'dynamisering risicomodellen Syr i' waar in onder andere de svb en het uuvv participeren. Als proef wordt Syr i wel ingezet bij één project van het Landelijk Structuur Interventieteam (Isi).

Desvb doet geen mededelingen over de risicoprofielen die ze hanteert. 'Door middel van queries op onze systeembestanden krijgen we dan bijvoorbeeld wat voor soort gevallen aan de risico en merken voldoen. Door middel van stakproeven

wordt vastgesteld wat omvang en aard van het risico is en welk behandelingsmaatregelen genomen kunnen worden.⁸¹

Des vvb gebruikt doorgaans de eigen uitkeringbestanden en soms die van geselecteerde partijen in samenwerkingen. Gevallen met bepaalde kenmerken uit het bestand van een andere instantie houden des vvb-analisten dan tegen de eigen bestanden, ten einde verdachte gevallen o.g. personen te detecteren. Voorbeeld zijn de eerder genoemde 'windschutters' of 'spookpersonen' van wiens welkijns iets bekend is, maar die wel een uitkering genieten.

Problemen die optreden zijn tweeledig voor des vvb, 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 IT-systemen tot problemen leiden. Bovendien moet iedere inkoop van bestanden op elkaar afstemmen. Alle organisaties hanteren begrippen op eigen wijze."

Noem bijvoorbeeld een veld "naam" die in administraties heel verschillend ingericht kan zijn qua notering van voor- en tussenvoegsels, voorletters en -voornamen, eigen namen van getrouwde personen, buitenlandse samengeselde namen, etcetera.

De vvb beantwoordt de welke concrete resultaten van alle verrijchingsanalyse er zijn gebekt, noemt des vvb "onbegonnen werk". Wel worden voorbeelden genoemd. Een concreet resultaat volgt uit de samenwerking tussen des vvb en de ind, met analyse van in Nederland wonende vvb-klanten met een verblijfstitel en betaling in het buitenland. Daaruit vonden 56 aow- en 503 ak-wi-gechtigden.

De steekproef telde 46 zaken. Bij 16 van de 28 inmiddels onderzochte zaken is de verblijfstitel op basis van vvb-informatie getrokken. Welke les zijn er getrokken? Data-analyse en ketensamenwerking zijn tijdrovend. Samenwerking in de keten wordt grondig overleg in de voorafcom, misverstanden voorkomen. Men moet elkaar taal leren spreken. Wat deelen met bijvoorbeeld het begrip "wonen" bedoelt, heeft bij de ander soms een geheel andere betekenis.⁸²

9.5

toekomst

De mislukking van het Multiregelingensysteem en het niet doorgaan van de daarvoor bedoelde automatische risico detectie zijn voor des vvb geen reden om de voornemens met analyse voor fraudebestrijding op een laag pijntje zetten.

Te lijn en ambitie is om te werken om zo nauwkeurig mogelijk te handhaven. Het doen wil ook al, ook zonder mis. Op basis van risico-analyse en val dat lieven die risico's met voorgegaande onderzoeken met vragen als: bestaan die risico's ook in

⁸¹ 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 handhavingmaatregelen de komende jaren.¹⁸² Er is extra geld beschikbaar gesteld vanuit de Businesscase Intensivering Toezicht. Uit die businesscase blijkt dat verwachte opbrengsten van voorziene investeringen overtreffen. Naast de intensivering van repressieve toezichtactiviteiten wordt ook geïnvesteerd in de professionalisering van onder meer data-miningen en risico-analyse, ter verhoging van de effectiviteit van de algehele handhaving. Desvib richt in 2015 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. Deze eenheid moet zich ook richten op digitale fraude.

De resultaten van de analyses zullen moeten leiden tot verfijnde fraudeprofielen. Via vulgare kunnen we die profielen op onze bestaande systemen. Dat wil zeggen dat we uit die systemen gegevens selecteren die voldoen aan die profielen. Dan gaan we alderend 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 pak kans vindt desvib het ook belangrijk om de preventieve handhaving verder te verbeteren, onder andere door verbeterde informatievoorziening aan klanten en aanpak van de regelgeving waar die fraudegevoelig blijkt te zijn. Het is vrijwel onmogelijk om de opbrengsten van preventieve handhaving tekentificeren, dus hier zijn nadrukkelijk geen baten aan verbonden.

De kosten en opbrengsten van de voorstellen in de Businesscase Intensivering Toezicht a.u.b. die in maart 2015 zijn goedgekeurd¹⁸³:

	2015	2016	2017	2018
Investering	7.500.000	7.300.000	7.300.000	7.300.000
Opbrengst	8.200.000	10.400.000	12.800.000	14.900.000
Resultaat	700.000	3.100.000	5.500.000	7.600.000

De cijfers over de werkelijke kosten en baten in 2015 zijn nog niet beschikbaar. De vaste kosten van desvib voor het aantrekken van externe en interne fraudelops, inclusief die uit analyse, belopen 12 miljoen euro per jaar. De opbrengsten van men hier daarom van de besparingen op uitkeringen voor de toekomst en de geïnvesteerde terugvoerde de teveelbetalingen en boetes. Die zijn uitgesplitst in de plannen.

¹⁸² Idem.
¹⁸³ Idem.

De voorlopige cijfers en schattingen over 2016 bevestigen dat de opbrengsten gehaald kunnen worden. Wel was 2016 een jaar waarin de investeringen en het starten met de activiteiten om de beten 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 feitelijk realisering van de businesscase eventueel doorlopen tot na 2018.

Des vbm erkent 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 beten inderdaad de kosten overstijgen, zou het onverstandig zijn dit niet te doen. De vraag die daarbij vooral moet worden beantwoord, is of de opbrengsten mind. afnemen omdat de "vijnde" van onschuldigheidslen leeggevist raakt".¹⁸⁴

¹⁸⁴ Idem.

10

gemeente

inleiding

Vanaf 2007 zoogen gemeenten en hun organisaties deze analyse een plaats te geven in de methoden voor bestrijding van onrecht verstrekteww-uitkeringen. Regionale adviescomité voor fraudebestrijding, een r r of 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 pak je dit uit in de praktijk? Waar zijn er welen waar zijn er geen successen geboekt?

In onderstaande beschrijving wordt minuscule het (glibberige) pad gevolgd dat gemeenten betraden op weg naar data en risicoanalyse als middel om – al dan niet vermeende – uitkeringsfraude te rug te dringen.

10.1

doel en

Gemeenten maken bij het voorkomen en tegengaan van misbruik van voorzieningen, zoals de uitkeringen w w, gebruik van het vng Kenniscentrum Handhaving en Nalevingen daarbinnen het Expertisecentrum Sociaal Domein (voorheen r r of, Regionaal Coördinatiepunt Fraudebestrijding), vorder afgeloot doving k h n.

In 2007 ontving vng k h n (r of) grootspons op een uitgebreide enquête naar fraudebestrijding bij sociale diensten. Vooral controle op bestaande uitkeringsgevoeligheden varieerde maar en betere instrumenten.

Immers, nadie goedkeuring van een aanvraag met strenge toetsing moet de gerechtigde el wijzigingen melden, maar vindt er geen toetsing meer plaats. De Autoriteit Persoonsgegevens gaf in 2007 het ministerie van szw groen licht om vanuit gekoppeld de databanden gedurende twee jaar (als profielen toont w i kolen voor bestrijding van uitkeringsfraude. De profielen moesten objectiverbaar zijn, niet tot individuen herleidbaar.

De verwachtingen van dit 'informatiegestuurd handhaven' (i g h) of 'analysegestuurd handhaven' waren aanvankelijk bij lokale bestuurders hoog gespannen. Zo liet wethouder Eric Fassen van Capelle voorafgaand aan een test met vng Kenniscentrum h & n in data-analysesoptekenen: 'Weg van vandenborstels tellen naar de digitale toets of kom bij het bestrijden van bijstandsfraude'.¹⁵

Gemeenten werden ook vanuit de Hoge overheid aangespoord. / A schoten te kort bij fraudecontrole van w w-uitkeringen, schreef vvd-staatssecretaris Paul de

Krom in 2011 en 2012 aan de Tweede Kamer ter motivatie van nieuw wetgeving om handhaving- en sanctiebeleid op het zwart-domein 'aan te scherpen'.¹⁶ Die Kamer onderschreef breed de noodzaak om uitkeringsfraude terug te dringen: het percentage fraudeurs met verwijfbare Vorderingen boven de 25.000 euro in debijstand 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 w.w.b.

Bij het u.w.v. stond eind 2011 voor ongeveer 300 miljoen euro aan vorderingen open en bij de s.v.b. 90 miljoen euro, waarvan steeds een deel als gevolg van fraude. In 2011 was er voor 18 miljoen euro aan sociale zekerheidsfraude geconstateerd, waarvan voor 69 miljoen euro aan fraude met w.w.b.-uitkeringen.

Dit is deels het van gemeentelijke zijde en een verslag op de soliditeitslijst van het sociale zekerheidsstelsel. De bewindsman beloofde strengere sancties en meer mogelijkheden voor huisbezoek en voor data-oppeiling.

Zo had de rechter niet goedgekeurd dat gemeenten data over huishoudelijk waterverbruik mogen gebruiken om verdenkingen van fraude op te sporen, bijvoorbeeld van zwartwerk als thuiskapper. Of samenwonen van een w.w.b.-gerechtigde met kinderen met een studietoelage of met een verdienende partner.

Die Kamer liet in oktober 2011 aan de Kamer weten dat een inventarisatie van zwartwerk gemeenten, het u.w.v. en de s.v.b. met succes mogelijkheden hadden verkend van een broedersinzet van gegevensuitwisseling om fraude te voorkomen en te bestrijden. De gemeenten werden gestimuleerd door middel van een 'Verzamelsbrief'.¹⁷

De meeste maatregelen lagen op het terrein van gemeenten en waren mogelijk binnen de huidige wet- en regelgeving. Een aantal maatregelen voor verbetering van bestandsoppeiling, noodzaak te w.d. tot een w.d.w. (zorging). De regering streefde er naar deze in het najaar van 2012 aan de Tweede Kamer voor te leggen. Juist in het combineren van data schuilt een groot potentieel voor fraudebestrijding, 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 bestandsoppeiling goed te benutten.' Gewezen werd op een intensiever gebruik van de 'link' functie van de w.w.b.-met Services' bij beoordelingen van aanvragen voor een w.w.b.-uitkering. Deze worden verschaft door de w.w.b., die gegevens ophaalt bij het u.w.v., des v.b. gemeentelijke sociale diensten, de w.d.w., het Kadaster, de w.d. om de Kamer van Koophandel. Voor beoordeling van bezit en inkomsten van bestaande uitkeringsgerechtigden moet

¹⁶ <http://www.tweedekamer.nl/kamerstukken/detail?id=201215>
<http://www.tweedekamer.nl/kamerstukken/kamervragen/detail?id=201212249&did=20121047636>

¹⁷ Verzamelsbrief sociale fraudebestrijding
<http://www.tweedekamer.nl/kamerstukken/detail?id=201210040&did=201210040>

ten gemeenten intensiever gebruik gaan maken van de data van het Inlichtingenbureau (zie ook hoofdstuk 6).

In 2012 ging het ib over langere periodes inkomen, vermogen en transacties analyseren, bedoeld door de staatssecretaris. Nieuw signaal voor voortuigbezit, bankrekeningnummers en toeslagen werden geïntroduceerd, en later ook nieuw signaal voor woon- en leefsituatie en gezinsinkomen. De Kom gaf als voorbeeld het meermalen achteren een auto invullen dat tot de 'adstringerende' verdenking van handeldel' 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 spoorloosheid vervangen voor een geautomatiseerd 'vulger' van despotu loze debiteuren met behulp van koppelingen door verbetering van adresregistratie en opsporing van fouten in de brp met data uit de wv v Polis-administratie (zie hoofdstuk 1).⁸⁸

Er waren wel privacyvraagstukken. Zo twijfelden gemeenten of ze via Kvic-bestanden persoonlijke data voor wv v controle en opsporing mochten gebruiken. De staatssecretaris gaf zijn fiat. Ook werd het licht op groen gezet om de gegevens te koppelen van het wv v van gemeenten wellicht mogelijk te maken. De Autoriteit Persoonsgegevens had de proef van Amsterdam met adrescontrole met de wv v Polis-administratie immers afgeurd.

Gemeenten werden gemaand om het inzagere en correctierecht beter te hanteren. De bevestiging van bestanden bleek bij honderd gemeenten echter te wens en over te laten. Zorgvuldig gebruik van gegevens uit de wv v Services liet ernstige wensen over. Er startte een campagne, maar nog tot in juni 2015 werd misbruik en 'lekkage' vastgesteld.⁸⁹

10.2

opzet systemen

De uitvoering van de besluiten op gemeenteniveau werd opgepakt door vng k h n (toen nog r o f) in samenwerking met de Inspectie szw. Informatiegestuurd Handhaven [igh] betekende het koppelen van bestanden, ten einde de kop of elen te genereren voor bestrijding van uitkeringsfraude, oftewel: databestanden in de 'warmachine' met kanarische verdenkingen als resultaat. Met verder als bijkomende gevolg goedwillenden minder lastige te volden met onnodige controles.

⁸⁸ <http://www.tweedekamer.nl/kamerstukken/detail?id=2>

⁸⁹ Interviews met Hans Berkhout en Ad van Mierlo van vng k h n.
'Ambtenaren misbruiken digitaal klantdoosje', Argos, Vpro, 20 juni 2015.
<http://www.vpro.nl/argos/media/afleveringen/2015/Lek-Suwine.html>

vingen onderscheidt verschillende onderzoeken:

- Themaonderzoeken gaan over een enkelvoudig kwantitatief, bijvoorbeeld verbruik, autobestel en bijstand, of niet-erkende kinderen die geboren zijn in de bijstandsperiode.
- Fenomeenonderzoeken zijn – net als themaonderzoeken – gericht op eenvoudige zaken, zoals tupperwareparties, ballonvaarten of Uber taxi. 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 deze bestanden vergelekt. Deze methodewerk met massale gegevens, het uitkeringenbestand met honderden namen wordt vergeleken met de bijstand (het vroegere gulde), 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 raken en aan het werk te gaan.

vingen hanteert drie eenvoudige criteria voor licht:

- 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 voor gekomen 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 maanden, terwijl SmartBox een structureel gebruik van data voorstond met een vaste aansluiting op de data systemen van de gemeente.

Voor het Informatiegestuurd Handhaven werkten vng h&n 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 Vlaanderen, make van h&n en intelligenz uitwerken Alert van Capgemini in Utrecht. Zie onderstaande spreke.

10.3

uitvoering

InfoSupport ontwikkelde met vng k h n de SmartBox om de bestanden te koppelen en via k ruisverbanden 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 link omens, samenwoon- of vermogensfraude: combinaties van ten o l ieverbanden, vak antiebestemmingen, beroepen, aanvragen van rijbewijzen en bouwvergunningen. Om zoveel mogelijk fraudegevalleten te detecteren zou InfoSupport per gemeente het systeem optimaliseren. Een licentie kostte 20.000 euro.⁸⁰

Een voorbeeld is het antalkeren dat iemand op vak antie gaat naar het land van herkomst, voor lange perioden van bijvoorbeeld zes weken. Een 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 parkvergunningen, die duidelijk op vermogen, van mak vergunningen, die duidelijk op handel. Of neem meldingen van woonoverlast zoals burenhuzes. Als daar steeds een nieuwe partner aan moedert, is dat wel raar.⁸¹

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 dank zij verr ijking van de data [...], nu verdwijnt dat eigenlijk. Nu prioriteren we hem dan niet en verdwijnt hij weer uit beeld. Goede fraudeurs pek je niet zomaar'.⁸²

Ook de gemeente Delft ging enthousiast aan de slag met SmartBox, nadat de gemeenteraad b b w maande om werk te maken van vermindering van bijstandsfraude. Delft stopte de data van het I b 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 aanvraagd hebben van bijzondere bijstand. De expertise voor het vaststellen van de indicatoren en behandeling van resultaten komt vooral van de fraudeambtenaren intern. Zij kunnen de indicatoren die op fraude kunnen wijzen uit hun praktijk. De burgervernieuwingsnummers die eruitrolen, worden aan nader onderzoek onder-

⁸⁰ Interview met Hans Berkhout en Ad van Merlo, vng k h n.

⁸¹ Verdict door data - Van ten den borstel stellen naar datafuk, (Bestuur, 2 oktober 2014, <http://bestuur.nl/magazine/verdict-door-data/periode/15-februari-2015>).

⁸² Idem.

worpen, administratief, telefonisch, met een afspraak aan de balie of met bezoek van opsporingsbeamten.⁹³

Slimme data doos

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. Veldresearch/Inlichtingenbureau krijgen gemeenten maandelijks signalen uit de bestanden van het uuv, de vrb, de Belastingdienst, duo, Justd, het gbo en de rdw, te weten:

- heffingskortingen uit
 - voor tijdsbest,
 - sortingen redt/magtheid controle,
 - signal voor beoordelen aanvraag bijstand/uitkering,
 - inkomsten uit inkortaken en rouwtoes,
- studietoelane/deeltoe op
 - overschrijding vermogensgrens,
 - uitkering in andere gemeente,
 - indelentename,
 - voortvluchtig veroordeeld,
 - inachtneming hogedood of funeralsiteit,
 - overzicht bankrekeningen.

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

- details;
 - bewijsnamen/nummers op naam;
 - uitkeringen bij andere instanties of gemeenten;
- oorzakelijke analyse
 - niet-aangevraagde bijzondere bijstand;
 - andere fraude situaties;
 - veranderingen in gezins- en w. situaties;
 - aanvraag boven vergoedingen;
 - hondenbelastingen;
 - aan vragen vakanties uitkeringen gerechtigden;
 - fraude informatie uit het verleden;
 - re-integratie trajecten, afgebroken of niet meer verschenen;
 - openstaande schuldenposten;
 - aangevraagde, maar niet afgebillade schuldenreningen.

Data gaande SmartBox met naam en metsofnummer, en worden vervolgens geanonimiseerd. Alvorende analyse plaatsvindt aan de hand van ingebrachte indicatoren. Vooral het optreden van combinaties van factoren, bijvoorbeeld het best in drie honden (hoge belasting), een duurdere auto en verna vakantiebepalingen en/of aanvragen van boven vergoedingen kunnen tekenen tot verdere analyse van inkomen, vermogen, of vermogensfraude. Maar ook aangegeven gebroten zonder vader of groot aangevraagd hebben van bijzondere bijstand kunnen risico-indicaties van dit type vormen.

⁹³ Interview met Rappé 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 data-analyse zou groeien, naarmate profielen nader na elkaar zijn. Deze methoden worden aangepast op grond van nieuwe analyses.⁸⁴

Holje's: gedgeprimeerden en onwaarschijnlijken

ving klm noemde op het nationale congres 2013 van Divos een globale typen fraudeurs naar hoofdprofiel:

1. gemiddeld, financieel gewin;
2. actieve, welers, financieel gewin;
3. onafhankelijke vrouwen, financiële onafhankelijkheid;
4. gedgeprimeerden, ongevoelig voor risico's;
5. onwaarschijnlijken, financieel gewin;
6. klanten die worden gebruikt, financieel gewin (van derder).

Type Mantagrad en karakterisering van fraudeurs typen als volgt:

1. Wel willen werken, wel kunnen werken;
2. actieve, welers, onafhankelijke vrouwen;
3. Niet willen, niet kunnen, actieve welers, gemiddeld, onwaarschijnlijken;
4. Niet willen, niet kunnen, gedgeprimeerden en klanten die worden gebruikt door derden.

Deze krachtige wijze van profilering is momenteel niet van toepassing in het lgh van vng klm, maar geeft een indicatie van het denken in de praktijk over profilering in fraude aanpak.⁸⁵

Het tweede systeem voor data-analyse door gemeente, Alert, is onder leiding van vng klm samen met Capgemini in 2009 gebouwd met populaties van landbouwbedrijven in Utrecht en vervolgens in 2010 en 2011 in Tilburg, Nijmegen, Middelburg, Hilversum, Amsterdam, Leiden en Almere.

De steden Utrecht, Groningen, Zwolle, Tiel en Dordrecht gingen zelfstandig met Alert aan de slag, plus enkele passieve deelnemende steden.

Het betrof testen met 'geautomatiseerde risicosignalering' met inbreng van verschillende bestanden: bpr (g ba), uitkeringregistratie, fraude registratie en

84 Interview met Hans Berkhout en Ad van Mierlo, vng klm.
Info support: productinformatie@www.info support.com
"Verdacht door data - Van landbouwbedrijven naar datafuten, (Bestuur, 2 oktober 2014)
[http://bestuur.nl/magazine/verdacht-door-data-\(gemaakt-plaagd-15-februari-2015\)](http://bestuur.nl/magazine/verdacht-door-data-(gemaakt-plaagd-15-februari-2015)).

85 Voordracht "Verwijzer" Handhaving rechtmatigheid en arbeidsverplichtingen", Peter Haas en Wim Heersink van vng Kenniscentrum H&N
https://www.divos.nl/sites/default/files/bijeenkomst_besanden/112_vakmanchap_1a_ook_handhaving.pdf

externe bestanden van r.d.w. (kentekens). Op basis van een set –geheim gehouden– indicatoren kwamen “diënten” in een stoplichtmodel: rood (hoog risico op fraude), groen (laag risico) en oranje (gemiddeld).

10.4 resultaten

Het aantal dank zij toepassing van Alert bespaarde uitkeringen was gering, 17 (Tilburg) en 3 (Lidde), met volgens vng k.h.n. een kleine 1,2 miljoen euro aan opbrengsten gerekend over meerdere jaren. Echter, ruim een derde van de uitkeringen was al pastopt om andere redenen.

Alert kwam geven 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 17 miljoen euro kassen op te rapen 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.⁹⁰

Verder bleek het hanteren van het systeem dermate complex dat gemeenten afhaakten. Grote belemmering was het gebrek aan kennis om de benodigde data uit de gehele gemeente bij elkaar te krijgen. Dit was mede te wijten aan uitbesteding van systemen en databoeken.

Met Alert liep het onder tussen ook mis bij een project van Veru Alert waarboven dien inzet van een rechtszaak. Een tweede betrokken partij bij de ontwikkeling van Alert, omc 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 Capgemini, vng k.h.n. was van de zaak west es niet op de hoogte, want bij de overheid ontbreekt coördinatie van de initiatieven in data analyse.⁹¹

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 Magda Goelj van Westland weten: “De resultaten zijn tegengevallen en het gebruik is tijdrovend.”⁹²

⁹⁰ Ruim 1 miljoen aan uitkeringsfraude opgespoord, nieuwsbericht Gemeente Zwolle, 16 februari 2015 <http://www.zwolle.nl/actueel/ruim-1-miljoen-aan-uitkeringsfraude-opgespoord> (geraadpleegd 16 februari 2016). Toelichting gemeente Zwolle.

⁹¹ Uitspraak Gerechtshof Den Haag 26 januari 2014 <http://deeplink.rechtspraak.nl/uitspraak/KZHECLI:NL:GHDHA 2014 71>.

⁹² Geïnterd in ‘Verdacht door data’-Van ten den Bergh stelt naar datafakes, iBestuur, 20 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 opzetting 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 'littledata', waar bij privacy overigens per definitie werd geschonden: tips van bureaus en mensen, geuit via bijvoorbeeld kliklijnen: de gemeente Den Haag ontving 3900 fraudetips over wettelijke uitkeringen in 2012 en ruim 10.500 in 2013. Dit leverde een veel belangrijker bijdrage aan de 700 speluitleitkeringen in 2013 (op een totaal van 20.000) dan de SmartBox, ook wettelijke uitkeringen in 2013. In 2014 was de fraudebestrijding in 2014 veel succesvoller was dan in 2013, maar niet door de inzet van de SmartBox. Dit werd nog steeds wel gebruikt, maar op een bescheiden wijze.

'Smartbox wordt gevuld met variabelen die zijn geselecteerd op basis van succesvol aangegonde fraudezaken in Den Haag. Uit deze fraudezaken zijn overeenkomstige kenmerken gehaald die tot op zekere hoogte een voorspeller kunnen worden hebben voor het vaststellen van fraude.¹⁹

Eigen informatie over uitkeringen uit het verloren ontsignalen van het bijzijn met behulp van Smartbox in één overzicht naast elkaar gezet.

Het Forensisch Instituut (nfi) onderzoekt in opdracht van Den Haag datacombinaties om fraudezaken te kunnen voorspellen. Ook moest er een vaste methodologie komen op grond waarvan bkw van Den Haag een voorstel voor invoering van data-analyse kon doen aan de gemeenteraad.

Een goed werkend systeem zou ook voor andere gemeenten tot beschikking kunnen komen, zo luidde de verwachting. In elk geval binnen de G4, voor Amsterdam, Rotterdam en Den Haag, die interesse toonden.

Het nfi onderzoekt of het combineren van data uit een aantal gemeentelijke systemen plus bkw-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 medische persoonsprofiel als voorbeeld. Dit onderzoek was negatief; koppeling van andere gemeentelijke systemen zou niet direct tot betere risicoprofielen en meer aan het fraudebestrijden leiden.²⁰

19
20

Gemeente Den Haag, verslaglegging Dienst Werk en Inkomen.
Interview met Kohn, 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. Alart in het geheel niet, maar, ondanks een positieve en optimistische Eindrapportage Analysegeschied Landheving van vng.khn.

Vooral de indicatoren aantal voertuigen, leeftijd, burgerlijke staat, aantal kinderen en aantal trejeden bleken belangrijke signalen te kunnen opleveren voor vermoedens van fraude. Ook nationaliteit gaf relevantesignalen, 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' moest zijn. Met andere woorden: aan de voorwaarden voor kwaliteit werd in het geheel niet voldaan, er was veel geleerd van een serie mislukkingen.

In de praktijk bleek immers weer barstig. Technici gisten wat het inhielden van verschillende databestanden en invulling van de benodigde velden een grote hobbel. In de praktijk was het auwel om geschikt 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 queries vaak niet werkbaar: een tekijde 'hit' (wielrij personen) levert onvoldoende op, terwijl ook hit veel te veel onder zoek bij individuen. Data uit de les getrokken dat het gebruik van minder data tot een hogere succesfactor zou kunnen leiden, ontbevelen beter toegedicht komt aan privacy bezwaren.

Dit laatste haakte 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 is uiterst nauw. Gemeenten ontberen ervaring en deskundig personeel in het formuleren van de juiste analysevragen. Bovendien is uit base data nog veel informatie te halen zonder de alomvattend oppeiling van bestanden. Er is veel 'aanhangend fruit' dat over het hoofd wordt gezien en dat bij minder inspanning geoogst kan worden.

De voorkeur voor hanteerbare systemen op gemeentelijk niveau bleek ook uit het kortstondige, grote succes van systeem dtps: Diagnose-, Plan- en Sturingsinstrument. Na een bericht over het Bijstandsonder van Boxmeer sloten gemeenten in der tijd om dtps te gaan toepassen. Boxmeer slaagde erin om aan de hand van risicoprofielen de uitstroom van wibontvangers te verhogen en de instroom te beperken.

Combinatie van data en analyse op grond van eenvoudige analyse – op grond van gerond verstand – bevelen het succes. Er werden heren opgetuimd met een hoog fraudeis op zoals – al dan niet werkloze – kapsters, bouwvakkers of automonteurs. De meerderheid van de gerechtigheden met kleine fraudekansen werd daarop minder lastige gevallen.

Vervolgens konden echt en vooral grote gemeenten niet met dtps uit de voet aan gezien de omvang van hun bestanden.

Er ontstonden vaak problemen met de data zelf en de verwerking, zodat igh (informatiesituatie 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 gericht op individuen gericht en niet op situaties en voor een hele groep.²⁰¹

10.5

privacykwesities

Bij de ontwikkeling van Alert in samenwerking met de steden was er ondersteuning van een privacyjurist om de eisen 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 impliceert de gegevens afkoppeling. De ap vindt louter concrete oordelen in geval 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 oordelijken provincie, met koppeling in 50 gemeenten. De ap voor de stad in 2007 dat de methode in stijd 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 InfoSupport, die de data niet mag gebruiken. Dit is vervolgens vastgelegd in een bewakersovereenkomst. Daarmee wordt aan de wet voldaan, maar dit voorkomt geen mogelijke privacyschending.

SmartBox en Alert leverden ook onderzoeksmateriaal digitaal beschikbaar. Er wordt niet op etnisch gescreend, maar indirect kunnen allochtonen op grond van

201 'Het bijstandsonderzoek van Boxmeer', Binnenlands Bestuur, 4 februari 2011.
<http://www.binnenlandsbestuur.nl/social/achtergrond/achtergrond/het-bijstandsonderzoek-van-boxmeer-8990081ynkx>

202 <https://www.apwv.nl/nieuws/bestandskoppeling-voor-fraudebestrijding-waterproof-onrechtmatig-WC2VAD0-parabicht>
 'Bevindingen ambtschape Operation Waterproof', 29 mei 2007.
<https://www.apwv.nl/sites/default/files/download/uit/z2006-00475.pdf>

203 <http://deelnikrechtpraak.nl/uitspraak/MFECLI:NLORV>
 Bij voorbeeld toegepast in Brabantse gemeenten met bestanden van Brabant Water.
<http://www.binnenlandsbestuur.nl/social/nieuws/waterverbruik-lekt-toe-stopzetting-uitkering-50740701ynkx>

vakantiebestemmingen, vakantiebeduur en/of gezinsgrootte wel min of meer als groep worden geformuleerd vanuit de indicatoren.

Zoals blijkt uit het voorbeeld van de indicator 'lengere vakanties in hetzelfde land', dat ook defactoriëthniciteit in beeld kon brengen met vakantieneer het thuisland door allochtonen. Gemeenteraadslid Fatima Faldin van de Haagse Stadsport had kritiek op de stigmatiserende werking van controles op familiebezoek gedurende vakantieperiodes: 'Gaar SmartBox deze mensen aanmerken als potentiële fraudeurs? Komen mensen van niet-Nederlandse afkomst vaker dan anderen ontbreken in de statistiek en als mogelijke fraudeurs?'²⁰⁴

Ook vreesde zij een jacht op buitenlanders – 40 nationaliteiten – wonend in Den Haag dreep familiebezoek gaan. Volgens Li en Haag waren louter de voor w.w.b.-gerechtigden verplichte meldingen van vakantie van belang als een van de mogelijk indicatoren.²⁰⁵

Gemeenten laven 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 D en Haag verwoordde het in de pers zo: 'We hebben nog honderd voorbeelden, maar wij willen de fraudeur niet op voorsprong zetten. Hierover wonsen wij niet te communiceren, omdat we ons eigen succes in deze ielen kunnen rijden. We kiezen niet voor groot uitmeten van onze methoden, want daarmee verliezen wij onze voorsprong op de klant die nu opbouwen.'²⁰⁶

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 worden onderzocht en verder ingezien om nader onderzoek naar te doen.

Volgens vng klinkt de privacy bij toepassing van de SmartBox echter apriori voorbomen. 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 D en Haag. In principe worden de 'negatieve' resultaten, dus personen die geen extra verdienking

²⁰⁴ Geonteerd in 'Verdacht door data - Van tan den berstel stellen naar datafukies, iBestuur, 20 oktober 2014 <http://iBestuur.nl/magazin/verdacht-door-data> (geraadslaagd 13 februari 2015).

²⁰⁵ Geonteerd in idem.

opleveren, steeds 'weggegooid', voordat ze voor degenen die het systeem hanteren, zichtbaar zijn geweest.

Dit 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 dervingingen. Echter, juist de opbouw van historische gegevens op grond van een reeks analyses kan extra signalen voor dervingingen opleveren.

Dit 'in beeld houden' of profileren van wervingklanten 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 ('30') van de Wmo en Jeugdzorg nieuwe taken, maar ook bestanden die kunnen bijdragen aan het in kaart brengen van een persoon beter overzicht te krijgen. Veel van deze wervingingen gaan samen met zorgbehoeften. Er ontstaan nieuwe behoeften en mogelijkheden voor fraudeonderzoek. Met de inventarisatie wordt nu een begin gemaakt.^{20, 21}

Gemeenten staan volgens vervingklanten tegenover elkaar als gevolg van onduidelijkheid van de regering over het koppelen van data om fraude op te sporen. Dit maakt het vervolgen voor commerciële partijen moeilijk om systemen te blijven ondersteunen. Weliswaar heeft zij zelf bestandskoppelingen met het systeem Syrius dat toelating geeft, maar op gemeentelijk niveau is fraudeonderzoek op grond van data-analyse hierdoor niet zonder meer gedekt. De regering heeft tot nu toe volgens vervingklanten nagelaten helderheid te scheppen. Mag, er wel koppelen, welke bestanden betreft dat dan en welke bestanden niet, mag het structureel?^{22, 23}

De Autoriteit Persoonsgegevens geeft zelf ook alleen maar advies af 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 Syrius. Nagelaten is ook te geven wat een gemeente zelf mag (dualis van een samenwerkingverband) op het gebied van datakoppelingen. Hoe ver mag het werken met systemen als Smart Box en Alergen om niet op gespannen voet te staan met de Wbp?

Syrius-wetgeving is volgens vervingklanten, dat namens gemeenten deelneemt in de toepassing, geen legitimatie van Big Brother, integendeel. vervingklanten, vindt dat met de komst van de wetgeving juist voldoende waarborgen voor privacy zijn ingebouwd, die de toepassing van het systeem zonder wetgeving ontbeert.

20 Interviews Hans Berkhout en Ad van Mierlo, vervingklanten.
21 Interviews Hans Berkhout en Ad van Mierlo, vervingklanten.

10.6

toekomst

Er heerst de nodige onzekerheid bij gemeenten over toepassing van (Dig) Data-analyse. Koppelen van veel databestanden staat op gespannen voet met het proportionaaltitsbeginsel van de Wbp. Een adviseur Cap stelde de 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, listen hun opleggen vanuit de privacywet [...] want het is een raar idee 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 is dat opofferen, op grond waarvan via nader onderzoek specifieke gevallen kunnen worden gerocht 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)erijken en/of de exploitatie van – inmiddels vele tienduizende – webshops samen gaat met het gerieten van een uitkering.

Ook andere fenomenen of (risico-) indicatoren, zoals bijvoorbeeld de organisatie van ballonnenraces, bijeenkomsten voor thuisverkoop en het organiseren van kinderfeestjes, geven aanleiding tot gemeentelijke speurders. Dat geldt ook voor diensten waarin geld omgaat, zoals Airbnb-kamerverhuur en Uber-gesede autoritten. Ook relatieonderzoek op LinkedIn en Facebook kan duiden op economische activiteiten, bijvoorbeeld in de freelancesector.

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 ander bestand en 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-

denking. In augustus 2014 bracht vngb.nl het protocol 'Internetonderzoek door gemeenten' uit, met antwoorden.²⁰⁹

De wvwb 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 Hinderregister en dergelijke lokale bronnen, zoals bij verhuurders van woningen, energiebedrijven en de voormalige werkgever (artikelen 63 en 64 wvwb).

Op grond hiervan worden personen gescreend voor wie op individueel niveau wordt onderzocht op internet naar aanwijzingen voor fraude. Het Internetonderzoek vindt plaats bij een vermoeden van misbruik / fraude. Uiteindelijk worden uit de wvwb op worden geselecteerd. Het onderzoek vindt plaats in voor ieder een redelijke, toegankelijk openbare ruimte, 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.

Grote schaal

Deloitte stelt dat de (gemeentelijke) overheidsaanpak van fraude te versnipperd is, wat nog toeneemt door de decentralisatie van overheidsdaken. 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. Zoals Deloitte dat voor gemeenten met minder dan 10.000 uitkeringsgerechtigden de data niet 'big' genoeg zijn en data-analyse naar fraudepatronen weinig succes biedt, na een analyse bij een middelgrote gemeente. Idellier komt er volgens Deloitte een nationale samenwerking op het gebied van data-analyse, met bundeling van de lokale bestanden, zodat analyse en risicoprofieling optimaal worden.

Daarbij dient de expertise centraal te worden wordt opgebouwd. Een nationale 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_door_gemeenten.pdf 20 februari 2015.
https://APweb.nl/sites/default/files/atoms/files/besluit_internetoonderzoek_gemeenten.pdf Besluit.
<https://APweb.nl/nl/nieuws/besluit-internetoonderzoek-door-gemeenten-nieuw-bericht> 17 april 2015.

210 'State of the State', Deloitte
<http://www2.deloitte.com/nl/nl/pages/data-analytics/topical/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 Wvop niet toegestaan. Anonimiseren vermindert de slagkracht van een analyse volgens Deloitte; je vergelijkt dan gemiddelden. Uiteindelijk gaat het in de data analyses ten behoeve van fraudebestrijding om tot concrete verdachten te komen of die te onderscheiden met bewijs.

Wellicht kan een 'Data Darkroom' uitkomst bieden: individuele gegevens in een afgesloten omgeving koppelen, waar bij laatste de resultaten van de analyse 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 er een iets andere term gevonden: Informatiegestuurd werken genoemd, kortweg igw. Het moet gezegd zijn op zijn lijnen bij misbruik, maar ook op het voor komen. Immers, staat de gemeente bekend om adequaat optreden, dan heeft dat invloed op de educatie om te gaan frauderen. Om die reden wordt gesuggereerd betrokken die in een te onderzoeken doelgroep vallen, te blijven informeren. Probleem is vooral het gebruik van eigen gemeentelijke data, zoals vergunningverlening of belastingen zoals de ozb voor een pand dat wettelijk wordt verhuurd. Maar ook honderd belasting, 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 (intelligent gestuurd), met gebruik van volledige klantenteksten, dat wil zeggen persoonlijke profilering die actueel blijft door voortdurend gebruik van bestanden en risicoanalyse. Onderzoek is behalve op deze signalen mogelijk op grond van gekozen themaprofiel (bijvoorbeeld waterverbruik, niet-erkende kinderen) of groepsprofiel (eenouders gezinnen, 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 benummers van alle burgers. Dit staat echter op gespannen voet met privacyprincipes gezien de enorme omvang ('in strijd met proportionaliteit') en de wettelijke 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 variabel en zijn op uitkomsten. Echter, zoeken naar persoonsgegevens kan personen wakker schudden. De optie wordt genoemd om gebruik te maken van een afgeschermd onderzoeksomgeving om dit risico te vermijden, bijvoorbeeld het In n (internet recherche Nederland).²¹

I lgh In Amsterdam

Amsterdam werkt met een actieprogramma Informatiegestuurde handhaving. Het doel is om met onder andere informatie wettelijke capaciteit van de handhaving efficiënter en effectiever in te zetten, maar misbruik voorkomen en bestrijden door mensen en middelen slimmer in te zetten. Behalve vergroting van de publieke veiligheid doelloos met vergaarde informatie over de oorzaken en omstandigheden van ongevoerd gedrag het nalevingsgedrag te bevorderen. Voorbeeld: buurparkeren beter aanpakken, maar ook parkeren op de stoepen zoals met verbetering van de bewegingsruimte naar de 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 illegale huis

Amsterdam had naar schatting twaalfduizend illegale huizen en een onbekend aantal panden zonder vergunningen. Met behulp van data analyse trok de gemeente in kaart te brengen waar de verdachte panden zich bevonden. De panden waren in het verleden, op grond van meldingen, al in 10 procent, waardoor capaciteit van handhaving inefficiënt werd ingezet. In dit project 100 procent gekaaid op elke twee keer dat controle plaatsvond, later één illegale exploitatie opgevoerd.

De informatie wordt 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. De informatie is gecombineerd met adres- en pandinformatie, waarna de verdachte panden in beeld konden worden gebracht.

Dit is zonder specifieke analyse te worden gedaan, dus het was arbeid intensief. Verrijking was ook mogelijk slimme een factor: verdachte panden werden op tijd bezocht dat de kans op aanwezige toeristen het grootst is in de ochtenden de avond. Om een zaak tegen een illegaal hotel rood te krijgen werden aangevraagd toeristen gaten veld over hun boekingen.

De informatie werd voortaan naar afnemen 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 horeca overlast

Gespoeld is meer patronen te ontdekken van de horeca overlast, om handhaving bij structurele problemen mogelijk te maken. Zo heeft de eenheid gespoeld om, letterlijk, de routes van de kroegentochten in beeld te brengen.

211 Nota Focus op i g w v, vng Kenniscentrum Handhaving en Naleving, Den Haag, augustus 2016.

De aanbidders van deze drinkgeleg, bijvoorbeeld aan groepen die vijfzellersavonden vieren, zijn bereid om informatie te verschaffen over vaste routes. In combinatie met politiemeldingen van overlast zou een meer structureel beeld ontstaan van orderelstof naar in de openbare ruimte en in de kroegen.

Een voorbeeld is het gemiddelde aantal van getuigenissen van de politie bij het vaststellen van de noodzakelijke informatie. Wel heeft het een analyse van honderd klachten op zich gebied tot een efficiëntere inzet van de inspectie. Zo werden zowel 'beroept' agenten opgemerkt, als agenten die het vakke biont maken. Ook succesheid de poging om geluidde verlaten bij evenementen te koppelen aan toekomstige vergunningverlening. Het ingewikkeld wordt natuurlijk niet, maar tot op heden kwam niemand op het idee.

3. Aankomst verlaten

Voorheen werd de in de lokale (verkeers) politie gecontroleerd en bevestigd. Bijvoorbeeld voor het welzijn van ritten. De verantwoordelijkheid is verlegd naar de dataorganisaties die worden aangepakt op grond van de informatie verzameling over hun chauffeurs. De risico-indicatoren over de 'rotte appels' worden verzameld per bedrijf dat chauffeurs aan de regels moet houden.

Voor het handhavingen van de informatie wordt de informatie gestuurd werken het uitgangspunt. Bestaande van verschillende diensten van de gemeente Amsterdam (Programma Team Taxi, Dienst Infratructuur, Verkeer en Vervoer (divv), Dienst Openbare Orde en Veiligheid (oo v), Dienst Stadsinspectie en Dienst Basis Informatie (dib) en de stadsdelen) zijn daar voor beschikbaar alsmede die van de Inspectie Leefomgeving en Transport (ilt), Politie Amsterdam-Amstelland, het omroep veld van de Belastingdienst. Daarmee kunnen analyses met risico-indicatoren voor chauffeurs worden opgesteld met eventuele verkeersovertradingen, strafblad, belastingangiften, woon- en familietoestand. De gegevenspakketten zijn ter de handhaving van het gedrag van de chauffeur op straat, al ontbreekt er ook bijvoorbeeld als belastingontduiking.

Opdracht in dit project was de inzet van het platform van de politie in Amsterdam als de data voor de controleurs. De data van de politie en de data van de politie en de data van de politie en de data van de politie van hun rit (al dan niet weggevoerd) en uitvoering.²²

4. Parkeerdienst

Rijst Parkeren heeft de gemeente uitbestaand aan Orion. Dit bedrijf fotografeert voertuigen van parkeren voor digitale controle. Rijpende camera's leggen de kentekens van alle staande auto's vast met het oog op de politie parkeren. De kentekens worden ook bij het inleiden van kentekens bij het betalen van het parkeren bij de palen of via de mobiele systemen zoals Parkmobile en Yellowbrick al opgeladen.

De gemeente en de lokale parkeren kunnen ingezet worden van de lokale data van het Nationaal Parkerenregister (npr), opgezet door het Servoetuis Haken- en Verlof (haken- en verlof) en beheerd door de rijk. De database bevat ook de zones van gemeenten, eigenaren, en een parkeren vergunning, onder meer gekendepaten, bepalen en de lokale gebieden gebieden, zoals bijvoorbeeld. Extra aandacht krijgen de parkeren vergunningen. De kentekens worden vergeleken met de bestanden van de rijk met gesloten voertuigen en voertuigen die sluitte worden zijn gebied. Routeparken worden doorgegeven aan de handhaving.

22 Nota handhavingen Taxi, 4 september 2016
<http://www.amsterdam.nl/parken-verkeer/taxi/taxi-archief/handhavingen-beleid/>
 (laatst geraadpleegd 16 februari 2016).

Hinderpaal Amsterdam

igh isgezet bij bundeling van krachten 'integral beleid'. Dat was een belangrijke conclusie van bijvoorbeeld het project Emargo voor het 'schoonvapeen' van de wahlen in Amsterdam. Emargo was niet met bundeling en analyse van databeelden van de politie, het omstadsbestuur, de Belastingdienst, de Sociale Dienst, uitbestedingsinstanties, kadaster et cetera om afwijkende profielen van panden, bedrijven en personen in beeld te krijgen.

Zowel technische inhoudelijke als juridische problemen. Een team van specialisten had bijna drie jaar nodig om tot eerste resultaten te komen. Methoden en uitkomsten waren niet transparant.

Belangrijke aanbevelingen luiden:

- doorgaan met bundeling en analyse van informatiestromen;
- versimpelgeving van de regelgeving voor de noodzakelijkheidsduidelijkheid over wat wel en niet het gebied van informatie uitlozing is.²¹³

Over de problemen met de data schreef de betrokken criminoloog Cynille Fijnaut: 'I let was niet mogelijk om op basis van het convenant dat was gesloten, onmiddellijk gegevens binnen Emargo uit te wisselen. I let duurde ruim een jaar voordat het juridische kader voor de verzameling, de uitwisseling en het gebruik van informatie voltrekt helder was gemaakt en de technische voorzettingen waren gerealiseerd om de onderlinge informatie samenwerking te kunnen automatiseren'.²¹⁴

Dit project is opgegaan in het riet, de regionale samenwerking voor criminaliteitsbestrijding. Ook de convenanten zijn voortgezet. Over de koppeling van bestanden in de uitvoering van het werk van de politie is nauwelijks 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 zikt hierop voor de buitenwereld gering.

Diverse factoren (ontbreken van eenduidige regulatie, beperkte toegankelijkheid van informatie om een eenduidige opslag van informatie) zorgen ervoor dat informatie niet optimaal wordt uitgewisseld. I laatste is 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 door de veelheid aan niet eenduidige gegevenslastig. Ook wat betreft het delen van informatie ten behoeve van bestrijding van uitkeringsfraude doordende i bestaat deze onduidelijkheid in combinatie met gebrekkige transparantie.

B is een potentieel van vele bestanden geschikt voor koppeling voor vele vormen van handhaving. Echter, de doebinding van de privacywet – dat mogentekale inroen gebruik voor het aanvechtloos en gemaakte doel – verhindert de koppeling van bestanden en masale inzet voor analyse in den data tot personen te herkennen zijn.²¹⁵

- 213 <http://www.hetcoo.nl/instrumenten/bestuurlijke-aanpak/amsterdam-ein-drapport-emargo>
<https://zoek.officielebekendmakingen.nl/blg-160298> (laatst geraadpleegd 16 februari 2016).
 'Het project Emargo: maar eenvoudig aanpakken van georganiseerde misdaad', Toine Spapens, uit 'Kantlijn in de frontlijn - Ervaringen met praktijkonderzoek in de politiek', p. 14-150 uitgever: Politieacademie
<https://pure.uvt.nl/portal/en/publication/a/het-project-emargo/62828540a84932438d-b0d-6f6f000442929.html> (laatst geraadpleegd 16 januari 2016).
- 214 'Dienst tegen de zware misdaad', Cynille Fijnaut, 2011 www.urban.nl/system/files/fijnaut_-_de_strijd_tegen_zware_misdaad.pdf (laatst geraadpleegd 10 januari 2016).
- 215 Interview met Ronald Kerbergen, projectleider igh Amsterdam.

Big data tegenfra-**II**

Ook het stadsbestuur van Rotterdam heeft zich recent bij Big Data voorgevoegd. In een artikel in *De Persuur* van maart 2016²⁶ 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 gemeentelijke organisatie heen en het proberen om niet uit te gaan van voorwaarden en beperkingen door software en datapassadissen.

Wie (seen externe) afsluiting geschiedt. Met hem (seen) test met dataanalyse in het sociale domein opgesteld, ten einde effectieve indicatoren op te stellen die fraude kunnen bijdragen sociale verzekering fraude te traceren.

Dankzij deze methode is de 'vinkjeslijst' die de Sociale Dienst gebruikt om fraude te detecteren, volgens betrokkenen 'veel kleiner' te maken: meer gestandaardiseerde indicatoren die op fraude kunnen duiden. De methode is beschuldigd moet foutieve uitslag opleveren (al data voor komen). Een ander uitgangspunt is de data worden (ad) als iemand ouder is dan 63, de kans groot is dat die persoon fraudeert. Dan is die persoon vijf jaar oud, maar nu niet meer met de politie op het gebied. Maar dat is juist het probleem: het is niet natuurlijk dat vaak, zonder dat dat betekent dat de sprake is van fraude. Bijvoorbeeld om dat een van de twee in een bejaardentehuis is opgenomen. Dat maakt duidelijk dat je altijd inhoudelijke deskundigen nodig hebt om verbanden te duiden.²⁷

Aan een tweede probleem, privacy, werd volgens betrokkenen tevens getild uitgang voor politieke problemen. In de woorden van de adviseur: 'Er mag veel meer dan men denkt of wil. Bijz. natuurlijk vaak een bestuurlijk afbreukrisico aan. Zo van: "Het mag niet, want ik denk dat ik anders gaasur krijg met mijn methode."'²⁸

Vaak volstaat tijdig anonimiseren van data om vervolgens patronen te ontdekken die de controleurs kunnen helpen om niet a priori een lijst met te controleren mensen te genereren. Denken in data helpt, bijvoorbeeld met een vroege signalering van aanvragen. Zie je bij wijze van spreken de abonnementen op de Donald Duck opgezegd worden? Het zijn heel veel vanoudse dingen waar je niet kunt kijken. Hiernaast weten ook onmiddellijk waar de pijn zit. Omdat dan met zijn allen anonimiseren en met elkaar delen om de patronen te laten herkennen.²⁹

26 Big data in Rotterdam: zonder 'allo's', *Frank Blankens*, 17 maart 2016 <http://bestuur.nl/nieuws/big-data-in-rotterdam-zonder-allo-s>.

27 Idem.

28 Idem.

29 Idem.

inleiding

Het ministerie van bzk zet twee van zijn onderdelen tot u, 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 (alst op adresbestanden).

De intrigerende wisselwerking tussen het op orde brengen van adressen en diverse vormen van fraudebestrijding van een aantal overheidsvormen. De hoofdthemaat van dit onderzoek. Overigens is ook hier niet in letterlijk zin sprake van een Big Data-toepassing: er worden (nog) geen data-analyses toegepast op de bpr als geheel om risico's op fraude (vervalsingen) 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 anti-fraudestrategie uit van 'een goede balans tussen gerechtvaardigd vertrouwen, goed dienstverlening en fraudebestrijding'. Ictu is de uitvoeringsorganisatie, opgericht door het ministerie van bzk en devng 2001, die kennis en kunde op het gebied van icu 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 vloeden 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 (bpr).²²⁰

Het belangrijkste doel was om de bpr (voorzien gba) op orde te krijgen. Ook voor fraudebestrijding is een juiste adressering van personen noodzakelijk. Veel fraude wordt gepaard door gebruik van woonadressen, bijvoorbeeld voor uitkeringen,

²²⁰

Brief van minister Opstelten (VenJ) aan de Tweede Kamer over de aanpak van fraude met publiek middelen, 18 december 2013 (<https://www.rijksoverheid.nl/documenten/kamerstukken/2013/12/18/rijksbrede-aanpak-van-fraude>).
Interview met Mattie Blauw van bzk.

studie inaderingen 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 br. bij 15 gemeenten is geen enkele afwijking geconstateerd – alle 15 met een inwonersaantal van onder de 35.000. Er waren echter ook 31 gemeenten die onder de minimale norm van ten minste 90 procent juiste dataprestaties deden.

Voor alle data tezamen was het percentage van 99 procent haalbaar, maar voor de tacto- of adres maximaal 96 procent, zelfs met een steeds verdergaande controle methode. 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

Officieel bleek in een kleine 3 procent van de gevallen het geregistreerde adres in de br. 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 selectie een klein tekort aan resultaat. Om die reden is het nut van het opstellen van risicogestuurd adresonderzoek beproefd, om een hoger percentage onjuiste adressen te kunnen traceren.

De Rijksoverheid voor Identiteitsgegevens (Rvlg), voorheen Agentschap br. en onderdeel van het ministerie van bzk., leidde het project voor verbetering van de br. del. a.a., 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 gerade verdenking van foutieve adressering. Als er opzet in het spel is, dan ligt in kaart dit veelal de fraudebestrijding.

Binnen het project I.a.a. werden op basis van een risicoprofiel vier categorieën adressen geselecteerd door de Rvlg. Deze risicoadressen werden geselecteerd voor huisbezoeken door gemeenten. Soms volgend 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 vliekveldmotors. 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-Bildad, 25 november 2007, Kamerstuk 31.200.VII, nr. 34.

²²² Actieplan Kwaliteit g.b.a., 11 juni 2008, staatssecretaris Bijleveld aan de Tweede Kamer, Kamerstuk 30.985 Beleidsoriëntering Binnenlandse Zaken en Koninkrijksrelaties Nr. 18. Lijst van vragen en antwoorden, 21 april 2016. https://zoek.officielebekendmakingen.nl/dossier_30985/ksl-30985-18

werden opgesteld, zoals personen die briefadressen hanteren. Een derde indicator waren de 'verworde adressen' van de Belastingdienst, die sterke aanwijzingen bieden dat gegevens van één of meer bewoners onjuist zijn. Dit voorbeeld bij de combinatie van toeslagen, of onbestelbare brieven.

Ook het cijb leverde deeldata van verdacht adressen. Een belangrijk element was uiteraard ook het adressenbestand dat bij gemeenten valt onder 'vertrouwen onbekend waarheen' in de brp. Niet minder dan ruim 400.000 personen waren begin 2014 geregistreerd als zogeheten 'vow'ier.

Gemeenten kregen ondersteuning. In het rapport 'Samen sterk tegen adresfraude' staat dat het fraude team van de Rijksoverheid tussen mei 2014 en januari 2015 14 gemeenten bezocht zowel om deze te informeren over fraude signalen en de wijze waarop fraude het best te beperken kan worden als om zelf inzicht te krijgen in de mate waarin de gemeenten al genomen hebben tegen adresfraude die de brp treft.

Door vijf gemeenten werden risicoprofielen gebruikt in het proces van inschrijven aan de balie. De gemeenten gebruikten een gedetailleerd proces waarmee beschrijft hoe verschillende signalen van fraude kunnen worden herkend en moeten worden afgehandeld. De overige bezochte gemeenten gebruikten een dergelijk proces met minder risicoprofielen toen niet.

Zijn 43 procent van de gemeenten gebruikte ook andere media bij het uitvoeren van onderzoek. 25 procent had (eveneens) een anoniem meldpunt. Het overgrote deel van de gemeenten had op overblijfsel van de woningbouw, en pakt deze voor de komende adresfraude aan.

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

- 6000 ~~de~~ ~~risico~~ ~~adres~~ ~~bezoek~~ ~~en~~ ~~in~~ ~~huis~~ ~~bezoek~~ ~~en~~ ~~door~~ ~~de~~ ~~eerste~~ ~~91~~ deelnemende gemeenten op grond van risicosignalen bleek bij top de 3 adressen sprake van onjuiste adresregistratie, dus geen 3 procent treffer, maar ruim tien keer zoveel!
- Vooral de verworde adressen geleverd door de Belastingdienst bleek tref bijna 30 personen van wie de gegevens niet kloppen bij 100 gecontroleerde verworde adressen. Ofwel: inzet van deze risicofactor uit data-analyse was bij controle van de brp ruim 6 keer zo effectief dan met een andere steekproef.
- Bij de geleverde 'verdachte adressen' was registratie, inschrijving, traden bij 23 procent onregelmatigheden naar voren; vervolgens zijn bij huisbezoeken bij 100 cijb-adressen gemiddeld 0,2 personen aangehouden van wie de registratie gegevens niet kloppen.
- Risicoprofielen ~~bleek~~ ~~gebruikt~~ ~~te~~ ~~zijn~~ ~~aan~~ ~~de~~ ~~hand~~ ~~van~~ ~~signalen~~ ~~van~~ ~~de~~ ~~registratie~~ ~~van~~ ~~'vertrouwen onbekend waarheen' (vow)~~ in de gemeentelijke brp. Een indicatie

ter 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 hooggeachte bevoorrecht (minder dan 12m2 per bevoor) als risicopositief ingeschat. Een derde gedeelte van de adressen bleek niet oordeel gehanteerd, met gemiddeld 108 personen op de 100 adressen van wie de data onjuist bleken.

- Zo blijkt uit **hijp** **met** **de** **gegevens** **die** **indici** **er** **te** **zijn** **dat** **er** **iets** **niet** **klapt** **op** **een** **adres**. Het bezoeken van selectieve (verdachte) 100 briefadressen leverde gemiddeld 60 personen op van wie de geregistreerde gegevens niet klopten.

Conclusie: risicogestuurd handhaven, ofwel de databelanden analyseren om foutgerichte veronderstellingen te maken van foutieve adressering, sorteert effect. Gevolg: in december 2014 rapporteerde de Rijksoverheid dat het succes van de risicogerichte aanpak van adresfraude leidt tot landelijke uitrollen van het project I.a.s. 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 hoort te zijn, en de uitrol van de aanpak wordt nu in 2015 opgevoerd.²²³

11.3

Landelijke aanpak adreskwali

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 ontvingen gemeenten van het ministerie van bzk een vergoeding voor een afgeleid adresonderzoek ter hoogte van 70 euro. De Rvlg

223 Samenwerken aan Adreskwaliteit 2014, Eindrapport, 28 november 2014, <http://www.rvlg.nl/documenten/circularen/2014/1128/eindrapport-adresonderzoek-2014>. Samen sterk tegen adresfraude, Rapport over de aanpak van adresfraude door de Rijksoverheid voor Identiteitsgegevens (Rvlg) en gemeenten, 20 april 2015 <http://www.rvlg.nl/documenten/rapporten/2015/04/20/rapport-samen-sterk-tegen-adresfraude>. Interview met M. de Blaauw, J. de Meester en M. de Blaauw van bzk. Kamerstuk 30 962 Balaad doorlichting Binnenlandse Zaken en Koninkrijksrelaties Nr. 18 Lijst van vragen en antwoorden, 21 april 2015 <https://zoek.officielebekendmakingen.nl/dossier/30985/kst-30985-18>. Kabinet inverteert 13 miljoen in aanpak adresfraude, verwachte opbrengst 42 miljoen, persbericht, 21 december 2014 <http://www.rijksoverheid.nl/actueel/nieuws/2014/12/21/kabinet-inverteert-13-miljoen-in-aanpak-adresfraude-verwachte-opbrengst-42-miljoen>.

produceerde op grond van data-analyse en risico-profiel-ingde "Vv-aal-er-fraude-patronen" voor gemeenten, met daarin 10 signalen voor mogelijke fraude. Deze handleiding voor fraude-detectie wordt veel gebruikt door gemeenten en andere bij het bestrijden van adres-fraude-betrokken partijen. Derisico-profielen uit de waaler worden door de Rvlg steeds verder gespedificeerd en aangevuld.

Bij het inzetten van bestanden van derden voor adrescontrole en vergelijken van data uit verschillende bestanden voor het voorkomen en bestrijden van adres-fraude wordt vooraf een juridische toets uitgevoerd, met de vraag: is het qua privacy in de haak?

Derisicoanalyses maken van gemeenteamtbanen ook spurdien. Ziekunnen daartoe opleidingen volgen. De ldu had het voornemen om gemeentelijk ambtelaren Burgerzaken te onderhouden in het preventief signale en van fraude-indicaties tijdens realtime transacties in de brp. Doel was ook om bekend fraudepatronen zoals die van de fraudekaart (waaler) bij gemeenten te automatiseren, zodat een ambtenaar beter wordt ondersteund in zijn taak en aan de balie zoveel mogelijk op unifor miewijz wordt gewerkt.²²⁸

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 onopgevoerde. Zij mochten zich nu inschrijven in de brp wanner ze verwachtten de komende drie 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-ingezette en in de brp (onderdeel r n), registratie niet-ingezette).

In Bestuurlijke Overleggen tussen kabinet en gemeenten over su-arbeidamigratie 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 overbanning. 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 (r v-a) en waarbij het eerste klantcontact bij het r n-lokaal wordt gebruikt om aan personen te vragen naar zijn/haar eerste verblijfsadres. Deze pilot is begin 2014 begonnen bij de gemeenten Knorsterken, Den Haag, Westland, Schiedam en Vlaardingen. Inmiddels doen ruim dertig

224

Waaler fraudepatronen, 10 signalen van mogelijke fraude, folder, 27 februari 2015
<http://www.rvlg.nl/documenten/brochures/2015/02/27/waaler-fraudepatronen>

gemeenten meen is de verwachting dat begin 2016 alle 19 inwoners zullen meedoen aan de pilot.²²⁵

Het Algemeen Rekenkameronderzoek was kritisch over het gebrek aan inzicht in de effectiviteit, efficiëntie en proportionaliteit van gegevensuitwisselingen - analyses.²²⁶

Daarop zijn maatregelen genomen, zoals de invoering van een werkgroep Batenbekekeningen en 'Batenmonitor', waar meer resultaten van het I.a.a.-project uitvoerig worden bijgehouden. In een externe audit was nog niet voorzien. De participatiegraad van gemeenten is hoog, vindt de projectleiding: 100 deelnemers, samen goed voor 10 miljoen inwoners. Zelfs 240 gemeenten deden niet mee ondanks de financiële stimulans.

In 2015 zijn samen 7200 schorsende zaken uitgevoerd, met 2200 vrijwillig inschrijvende gistraties als resultaat (stand december 2015).

Het project I.a.a. is volgens de minister van Verkeersmiddelen, zo rapporteerde hij eind 2015 aan de Tweede Kamer.²²⁷ Bij 30 procent van de onderzochte adressen verschilden de inschrijving van personen met de werkelijk daar wonende personen. Tot en met oktober 2015 is voor ruim 7 miljoen euro aan baten berekend, die momenteel toelaten, tegenover ruim negen miljoen euro aan kosten. Begin 2016 wordt een evaluatie uitgevoerd.²²⁸

Overigens valt het project I.a.a. juist een aantal door de Rekenkamer geopperde problemen bij de bronnen, voor wat betreft de bron. Het aantal terugmeldingen op de bron waarbij afnemers van gegevens uit de bron - veelal overheidsdiensten - melden dat zij gewetensloos 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 bron met 50.000 in de anderhalf jaar tussen begin 2014 en medio 2015.

Dankzij samenwerking met onder andere de Belastingdienst, de Nationale Politie, het cijf, de Rijksoverheid en de v.b. 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/10186/79470/covers.html>

²²⁶ Rapport Batenregistraties, Algemeen Rekenkamer, 29 oktober 2014

<http://www.rekenkamer.nl/Publicaties/Onderzoeksrapporten/Introduktie/2014/10/Batenregistraties>

²²⁷ Kamerbrief over voortgang rijksbrede aanpak van fraude van minister van der Staar (Verkeersmiddelen) aan de Tweede Kamer, 21 december 2015

<https://www.rijksoverheid.nl/documenten/kamerstukken/2015/12/21/ik-voortgang-rijksbrede-aanpak-van-fraude>

²²⁸ Interview met Mattie Blauw van bzk.

De Belastingdienst zou na een beperkt testart met 1 a.a. met 200 signalen nog 750 signalen leveren. Van de nieuwe deelnemer politiewerden 'enkele honderden adressignalen' verwacht in de pilotfase, het cijfer naaert 250 nog eens 750. De svb, duo, Zinl (Zorginstituut) en het uuv werken mee aan verfietslevenssignalen of hebben de intentie daar toe uit te spreken. Zeggen na hoeze vanuit hun bestanden verdachte adressen kunnen selecteren. Ook wordt gesproken met partijen van buiten het overheidsdomein, zoals de Stichting Netwerk Gerechtsdeurwaarders (n.g.), die onjuist geachte adressen kunnen doorspelen. Na succesvolle proeven met politisignalen van openstaande boetes in enkele Utrechtse gemeenten en Almere volgde ook inbreng van de politie in andere gemeenten.²³

De middelen die de Rvlg inzet in het project, laten breiden zich uit. Zo kan voor 1 a.s. sinds augustus 2015 het instrument webbrowser om frauduleuze online-advertenties te vinden in grote openbare bestanden. De webbrowser haakt voort van vooraf bepaalde delen van advertenties af binnen, bijvoorbeeld marktplaats.nl/ woningen en selecteert hieruit de relevante advertenties. Bijvoorbeeld: 'Gezocht: inschrijftadres. 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 bekend door middel van en uitkeringen aan te vragen (of te houden) die afhankelijk zijn van het woonadres zoals bijstand, huutoelag of studietoelagen. Omdat iemand zich onvindbaar wil maken van een bijvoorbeeld (belasting)schulden, uitstaande boetes of politievervolg. Met een toegenomen aantal advertenties zijn afspraken gemaakt om het misafdeaanbod te verwijderen en de advertentie hiervan op de hoogte te stellen. Op Marktplaats.nl (waarmee de eerste afspraken zijn gemaakt) zijn in 2015 meer dan honderd advertenties verwijderd. Misafdeaanbodes worden overigens weinig tot geen persoonsgegevens. Volden een naam en soms een telefoonnummer. Het gaat de Rvlg niet om analyse van persoonsgegevens van adverteerders. Dit instrument is volledig gericht op de advertentie zelf.²⁴

Voorbeeldgemeenten

Bij de lokale projecten voor opzoning van adresbestanden liepen parallel zoals van de Dienst Basisinformatie van de gemeente Amsterdam. Daar heeft zijn grote bestanden gekoppeld, bijvoorbeeld de politiediensten van het uuv en de svb. In de verkenningen in de persoonsregistratie komen vaak juiste adressen voor dan in de gemeenteadministratie. Ook de Belastingdienst, de Sociale Dienst, uitzendbureaus en woningcorporaties werken mee met de vergelijkingen.

Tilburg digitale gedragsanalyse

Tilburg begint met risicoanalyse van digitale contacten met burgers, dat wil zeggen van 'vreemd' gedrag van de inwoner. Aanpak dit vraait het minder zichtbaar is dan aan de balie heeft Tilburg in het project 'Adres op orde' 20 inkomsten en een red om de kostbaarheden te beheersen, waar naar nu Thelen lukt een daling van de inschrijving 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 l.o.o. project structureel te maken, gaat het tot die tijd door met 'risico-geïcht adresonderzoeken' binnen hetzelfde budget.

Naar verwachting zijn er in maart 2016 ten minste 11.000 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 van 5000 adressen administratief gecontroleerd; met naar verwachting circa 7500 adresgegevens uit de fraudegevallen. Administratieve controle is geschrapt. Nu wordt nog geraamd dat 10.000 huisbezoeken 40 procent onjuist adressen zal opleveren.

De kosten met de uitkomsten gemiddeld en de fraudephrengst wordt door de partners in beeld gebracht en verhaald. De baten daar van worden landelijk gerepresenteerd 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 adresfraudegerelateerde 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 l.a.a.-project, in maart 2016 liggen tussen de 40 en 50 procent. In 2014 was dit nog 30 procent, in 2015 opgevoerd 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: du.o. levert gemeenten verdachte adressen aan, waar na vervolgens de buitendienst van de gemeentelijke onderzoek doet of een student thuis of uit huis woont. du.o. betaalt 280 euro per aangemeld dossier. Bij fraudezet leidt du.o. de studiebeurs stop en kan de eerder uitgekende beurs worden teruggevorderd.

ving Kenniscentrum Handhaving en Naleving brengt bijvoorbeeld interne afdelingen van gemeenten en aannemers 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 bron opdat het stult men op ontbrekend vastrecht tot oorzaken of uitkeringen.

11.5 project aanpak fraude bij ict u

Het doelproject Innovatie van ict u in het kader van fraudeaanpak, aldus gepubliceerd in een vacature in januari 2016, zet in het veld van fraudebestrijding data-analyse op 'business forensics' in. Met pilots wil de afdeling Burgerzaken & Informatiebeleid (b&i) van het ministerie van Buitenlandse Zaken dat het mogelijk is om kleine en grote data-sets in de aanpak van identiteits- en andere fraude te zetten door middel van data-analyse in open bronnen.

Het project Aanpak Fraude van ict u draagt in opdracht van het ministerie van Buitenlandse Zaken onderzoek, wetenschappelijke methodes en innovatieve ideeën en technieken aan die de huidige aanpak van id- of adresfraude kunnen aanvullen of verbeteren. In 2016 begon Buitenlandse Zaken 'proef' op gebied van analyse van databestanden, begeleid door ict u. 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 dat gebruik beter te regelen.

De geanonimiseerde gegevens van Wmo en brp worden gebruikt om te zoeken naar fraudepatronen waar van de relevantie door ambtenaren van Zaanstad wordt bepaald. Door niet-relevante patronen weg te gooien worden alleen vermoedelijke vergoedingen, fouten of fraude mogelijk gemaakt. 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 vergoedingen. 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 te handhaven in de huidige fraude in de zorg (Indie 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 Nalavang & Handhaving van de vng, het ministerie van vws, tweezorgkantoren en de pgb-belangenvereniging Per Sado. De drijfveer is minimalisering van variëns van het knappe zorgbudget aan fraude. De resultaten zouden in het voorjaar van 2010 aan het ministerie van vws worden aangeboden, ten behoeve van inzet voor alle gemeenten in Nederland. Erasmus Universiteit begeleidde het project en bracht begin 2010 het rapport 'Na rechtmatige zorg in het gemeentelijk sociaal domein' uit. De eur-onderzoekers stellen vast dat frauderisico's het grootst zijn aan de kant van zorgaanbieders en dat hier beter op getit moet worden. Ze adviseren gemeenten om hun kennis beter te bundelen en uit te wisselen binnen de keten met zorgaanbieders, zorggebruikers en zorgverzekers. 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-analyse bij bak

Vastateregwen doorgang goede informatie over de richting van organisatie, zoals de Data-analist cybersecurity ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Logius Functieschrijving. Wil jij verder bouwen aan een veilige e-overheid? Samen met jouw collega's van het Fraudesteam, 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 beveiligingsaanpak van de dienstverlenende Boverheid. Bij het behouden van veiligheid en een proactieve preventievisie. Denk aan early detection, intelligente analyse van grote data sets en ondersteuning van security by design adviezen. Anderzijds heb je ook een meer reactieve zijde en werk je aan brandstapen 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 Fraudesteam wil nieuwe technologische mogelijkheden 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 2010: http://www.cromstrijen.nl/actueel/gemeenteniets/3359/item/gemeenten-erken-samen-bij-aanpak-fraude-in-de-zorg_6886.html
- 236 'Na rechtmatige zorg in het gemeentelijk sociaal domein', Erasmus Universiteit, Faculteit der Sociale Wetenschappen, januari 2010: http://www.eur.nl/fsw/bestuur/nuke/nieuws-detail_bskv/artikel/8585-onderzoek-na-rechtmatige-zorg-in-het-lokale-sociale-domein/

- [...]
- de hebt kennis en ervaring op het gebied van analyse van grote datasets (big data), modellering of van technisch-forensische analyse;
 - de hebt ervaring met één of meer programmeer- en/of scripttalen;
 - ervaring met verscheidene actieve monitoring en detectie, incident response, computer network defense/investigational een pre;
 - de hebt bij voorkeur kennis van en ervaring met malware, cybercrime, identity fraud, hacking en phi

11.6

basisregistraties: heel veel dat

De belangrijkste data van de overheid zijn vervat in basisregistraties, vijf in totaal.

Het geheel wordt samengevoegd in een stelsel van basisregistraties. Dit stelsel moet voorzien in het borgen van onderling 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 overheidsdelen, vele publieke organisaties en in een aantal gevallen ook door private partijen.

Geofgzeegd staan de basisregistraties nu nog op zichzelf, maar door samenvoeging moeten de gegevens met toelating 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 melding voldoende. Provincies, gemeenten en waterschappen hebben toegang tot deze gegevens en kunnen ze bij hun eigen werk gebruiken.²²⁷

Het gaat daarbij om:

- brp – Basisregistratie personen;
- nrhr – Handelsregister;
- bag – Basisregistratie Adres en Gebouw en (tweevoudig);

²²⁷ [www.werkenvoormediatienl.nl/januari2016/\(inmiddelsnietmeeronline\)](http://www.werkenvoormediatienl.nl/januari2016/(inmiddelsnietmeeronline)).

²²⁸ 'Stelsel van basisregistraties'
<http://www.digitaaloverheid.nl/onderwerpen/stelselinformatiepunt/stelsel-van-basisregistraties>
 'Stelsel van overheidsgegevens', bericht DigitaalOverheid.nl
<http://www.digitaaloverheid.nl/onderwerpen/stelselinformatiepunt/stelsel-van-overheidsgegevens>
 'Efficiënter werken door samenvoegen basisregistraties', nieuw bericht Rijksoverheid.nl
<https://www.rijksoverheid.nl/onderwerpen/digitaal-overheid/inhoud/efficiënter-werken-door-samenvoegen-basisregistraties>

- br t – Basisregistratie Topografie;
- br k – Basisregistratie Kadaster;
- br v – Basisregistratie Voertuigen (kentekenregister);
- blau – Basisregistratie voor Lonen, Arbeidsverhoudingen en Uitkeringen;
- br i – Basisregistratie Inkomens;
- woz – Basisregistratie Waarde-Onroerende Zaken;
- bg t – Basisregistratie Grootschalige Topografie (voorheen gbkn);
- br o – Basisregistratie Ondergrond (voorheen ook weldino).

*) De bag bestaat uit twee basisregistraties, adressen en gebouwen. Daarom zijn er twaalf basisregistraties.

Het ministerie van Luchtwind heeft (U)it Stelsel van Basisregistraties. In een stelselcatalogus heeft Logius, het onderdeel van het ministerie van Luchtwind, 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 in een kalender geeft de planning weer voor de hele beoogde digitale overheid. Industrielijke registraties.²⁴⁰

De uitgaven van de ministeries belopen tot 2021 ongeveer 100 miljoen euro per jaar, in 2010 120 miljoen euro, de komende jaren iets minder dan 100 miljoen euro, totaal 600 miljoen euro. Daarmee komt een kleine 800 miljoen euro bij aan kosten – minus van de boden op grond van de registraties behoren – 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.

Informatie-veiligingen en privacy vormen samen belangrijk onderdeel van de dienstverlening van deze knooppunten. Een voorbeeld van een knooppunt is het bkw (Bureau Keteninformatisering Werk & Inkomens), beheerder van Surinam, dat gegevens deelt voor overheidspartijen binnen het domein werk en inkomens zoals het uuv, 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

indruk te krijgen van bestaand 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 Digicommissie 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 fraudebestrijding

Dit stelsel voldoet niet aan de 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 volgen. De grens tussen inzet van data voor opsporingsdoel voor meer generieke opsporing is niet helder. De Big Data mogelijkheden van de basisregistraties zijn verschillend eken aan de ordegekomen 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 la carte*, maar analyse daarvan op grond van de principes van Big Data analysevormen nu nog een 'wip op de haren'.

²⁴¹ Knooppunten
<http://www.digitaleoverheid.nl/onderwerpen/stelselinformatiepunt/stelselthema/knooppunten>

'Stelsel van Overheidsgegevens', De Digicommissie is, Erik Jonker, 28 september 2015

<https://digitaleoverheid.plan.nl/files/download/34410482>

Knooppunten en het Stelsel van Basisregistraties

<https://wiki.stelselvanbasisregistraties.nl/wiki/bin/view/document/Visieophet>

«Stelsel van Overheidsgegevens»

²⁴² 'Notitie Stand van zaken financiering stelsel van basisregistraties', 15 januari 2015, Digicommissie <https://digitaleoverheid.plan.nl/files/download/41035952>

Demogelijkheid 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 stelt 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 nadere voorwaarden voor data-analyse volgen er te gemakkelijk verkeerde denkingen. De Rekenkamer noemt als voorbeeld Schoon Schip in Amsterdam, dat nakoppeling van bestanden van het uitsluiten (weedsuicide) van de (vluchtige) opkeverde, met uiteindelijk 25 werkelijke fraudegevallen.

Justiële demogelijkheden voor adequate opsporing moeten en beveiliging optimale aandacht krijgen. Zo moet ook transparant worden wie er welke gegevens opvraagt en verkrijgt.

Ook moet het corracteredict van burgers en bedrijven goed geregeld worden, omdat kleine fouten grote gevolgen kunnen hebben, niet zelden voor langere periodes. 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 is: de gegevens beschikbaar als open data, maar dit zonder bewaren (zoals privacy) mogelijk is, mede om zo de gegevens wettelijk te breder toetsbaar te maken.

Al in mei 2012 en in januari 2013 zijn sessies over fraudebestrijding met basisregistraties georganiseerd met bestuurders, managers en informatie specialisten van inspecties, uitvoeringsorganisaties, expertisecentraal politie. Zo lichten een aantal sprekers toehoe fraudecijfers uit de grote dataverzamelingen te distilleren en te toepassen zijn met uitkomsten op naam en op adres, in netwerken en elders.

Een van de sprekers was van Toov, 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 verdieningen te formuleren.

243 'Basisregistraties als fundament voor modernisering toezicht bij Inspectie azw', Roud Boot (iet u) en Wimfred Grahoff (Servicepunt Basisregistraties), zonder datum http://www.digitaleoverheid.nl/images/stories/staats_van_basisregistraties/best-practices-wp.pdf (geraadpleegd 8 februari 2016).

244 'Basisregistraties van uit het perspectief van de burger, fraudebestrijding en governance', Rekenkamer, 29 oktober 2014, <http://www.rekenkamer.nl/Publicaties/onderzoekrapporten/Introductions/2014/10/Basisregistraties>

Bijvoorbeeld van personen met een laag inkomen en zeer dure huizen, mogelijk gefinancierd met buitenlandse hypotheek. Basisregistraties zijn hier van belang, in het bijzonder door ze met andere registraties te verknippen en in samenhang te bezien.

Het loev kijkt dan ook met belangstelling uit naar het leggen van verbandingen binnen het Stelsel van Basisregistraties [1]. Als Kadaster, Handelsregister en w.o.z. aan de bag worden gekoppeld, ontstaan er nieuw analysemogelijkheden. Ook het ib, dat eveneens elders in dit stuk aan bod komt (hoofdstuk 5), zag mogelijkheden om met de bag (Basisregistraties Adres en Gebouwen) frauderisico's met bijsand te distilleren, zoals schijnverhuizingen, veracht gebruikersdoel van panden en oppervlakte van een pand.²⁴⁵

11.0

privacykwesties

Zoeken op 'privacy' op het domein digitaleoverheid plain n 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 daarvan van 'visuals' in de vorm van verduidelijkingen. Dat bij is ook een grens geslecht door VenJ.D. e minister van VenJuging in september 2015 dikkoord met een mochtiging tot bpr terugmiddeling voor de politie. De mochtiging behelst toestemming om bepaalde politiegegevens over adresbezoek te verstrekken aan (b&w van) gemeenten ten behoeve van de bpr-kwaliteit. Dat bes uit verscheen in de Staatscourant 'om onduidelijkheid weg te nemen'. Immers, oawet politiegegevens staat niet met toedat opsporingsdata worden gedeeld buiten het justitiedomein.

Verbetering van adreskwaliteit gaat meer en meer hand in hand met fraudebestrijding. Dat word evident met de samenvoeging tussen het project i o a n de Landelijke Stuurgroep Interventieteams (i ai), geleid vanuit de inspectie zw. Diezelfde inspectie opert meer mogelijkheden voor dat gebruik vanuit basisregistraties. Bij koppeling van bestanden kan eenvoudige vergaande profilering van (recht)s 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 verduidelijking te komen of een verdienking te onderbouwen.

²⁴⁵ Presentatieseminar bag Fraudebestrijding
<http://wiki.stelselvanoverheidsgegevens.nl/index.php/Fraudebestrijding> (Geraadpleegd 11 februari 2016).

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

Niet als met het project I.a.k. kunnen de basisregistraties vroeg of laat ook beschikbaar komen om analyses op los te laten om tot risicofactoren te komen zonder concrete verdenking, niet 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 Persoonsgegevens heeft zich over het laatste ritstich uitgelaten. Voor 'een paar euro' is er inzage in naam, adres, burgerlijke staat, koopsoort, w.o.z., hypotheek en bouwvergunningen. Per 1 oktober wordt dew.o.z. openbaar met alle voor fiscale heffing geschuldte waarden van woningen.²⁴⁷

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 Intobox Crimineel en Onverklaarbaar Vermogen (icov), het grootste en belangrijkste samenwerkingsverband ten behoeve van de bestrijding van alle belangrijke vormen van fraude, waar onder andere 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 bodien en de Finandial 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 als nog te innen.

Een meer structureel doel van het samenwerkingsverband is 'om de deelnemende partijen in staat te stellen betekenisvolle intervensies 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 openbare instellingen van de Nederlandse Vereniging van Vlaanderen tot het

248

Compilatie van informatie over icov, waaronder een gesprek met Gees Grootsholten (Hooft), Arjen Cuijpers (plv Hooft) en met lid verantwoordelijk voor iot) en Mieke van der Vegt (Senior beleidsmedewerker / privacy) van icov. Citaten zijn eveneens van deze voorvoorders.

(n.v.a.), de Inspectiesz.w. en de Inspectie Leefomgeving en Transport (ILT) bij het samenwerkingsverband aan. Andere overheidsorganisaties tonen interesse in daarmee, zoals toezichthouders en nog meer inspecties. Icoov, dat zijn onderkomen heeft in een gebouw van de Belastingdienst in Utrecht (en voorheen in Hoofddorp bij de Douane), bouwt daels voort op de inzichten die zijn opgedaan in het experimentele project Vastgoed Intelligence Center (vic), vooral te zied primair op vastgoedfraude, terwijl Icoov alletypen van vermogensdelicten bestrijdt. Het gaat om *financial intelligence* in de volle breedte, die haar beslagrijkt in rapportages, criminaliteitsbeeldanalyse, risico-indicatoren en groepsprofielen. Om aan die brede Icoov-taak vorm te geven moet een professionele en resultaatgerichte samenwerkingsorganisatie worden gecreëerd, die op basis van een stevig juridisch fundament haar werkzaamheden verricht. Icoov is gesteld op een convenant²⁴⁹, gepubliceerd in augustus 2013, waas ariptuulvullen voor gegevensverwerkingen onderzoek²⁵⁰ zijn toegevoegd, evenals twee mandaatregelingen voor beheer en voor privacy.²⁵¹

Icoov kan snel benodigde informatie uit veel verschillende bronnen leveren en dat is de voorname reden voor partijen om deel te nemen. Er werken op dit moment zo'n dertig personen afk om stiguit de verschillende partidurende organisaties.

Het bestaansrecht van Icoov 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 Icoov zelf dat de staat naar schatting jaarlijks 15 miljard euro schade lijdt door fraude.

249 Convenant Icoov 2013

<https://zoek.officielebekendmakingen.nl/stor-2013-24607.html>

250 Protocol gegevensverwerking Icoov product w2013

<https://zoek.officielebekendmakingen.nl/stor-2013-24608.html>

251 Regeling tot mandaat, volmacht en machtiging Hoofd Icoov Beheersaken 2013, Staatscourant Nr. 24635, 29 augustus 2013

<https://zoek.officielebekendmakingen.nl/stor-2013-24636.pdf>

Regeling tot mandaat, volmacht en machtiging Hoofd Icoov Wet bescherming persoonsgegevens 2013, Staatscourant Nr. 24630, 29 augustus 2013
<https://zoek.officielebekendmakingen.nl/stor-2013-24630.pdf>

De overheid heeft een fors begrotingstekort, staat voor grote bezuinigingen in bijvoorbeeld de zorg (circa 16 miljard) en wordt tegelijkertijd voor de 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 (i-Info), het Anti-Money Laundry Centre (amldc) en het Financieel Expertise Centrum (fec).

12.2

opbouw en uitvoering van het

iCoV is een dienstencentrum en geen casusoverleg zoals het i-Info, dat meer op grond van een wettelijke basis en daarbij behorende (financiële) samenwerking informatie uit verschillende bronnen bundelt.

Ten einde witwassen en fraudegebed 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 opvragers en verzoekers aan iCoV worden juridisch getoetst op rechtmatigheid van onder meer gegevensgebruik. Per product is er per mogelijke aanvrager een digitaal rechtmatigheidsbesluit opgesteld in samenspraak met de juristen van de deelnemende partijen, verenigd in de zogenoemde Rechtmatigheidscommissie.

Daardoor is duidelijk onder welke voorwaarden welk product met welke gegevensbronnen kan aanvragen. Deze voorwaarden zijn opgenomen in de aanvraagformulieren, waardoor de aanvrager alle voorwaarden zelf moet door nemen vóór diep deelt de 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". Daar mee 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 fiscaal geheimhoudingsplicht de aanvraag in de weg staat.

252

²⁵² Fraudekosten Nederland jaarlijks 30 miljard. Aanpak loont!, Schalké & Partners, zonder datum <http://www.schalke.nl/pdf/RAUD-El-totaal-overzicht%202014.pdf> (geraadpleegd 17 februari 2015).

²⁵³ Deze zeer ruwe en ook relatief schatting van Schalké & Partners die ook valabron 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 Dienstingdienst kan echter niet alle gegevens van de politierijgen, omdat daarop geheimhouding vanuit de Wet politieke gegevens rust: dan wel het opsporingsbelang in een concrete zaak aan verstrekking in de weg staat. Ook de onderzoek- en ontwikkelings (& c.)-activiteit is vraaggestuurd: dednemers kunnen vragen onderzoek te doen naar volgens hen belangrijke aspecten voor hun taken, die zien op toezicht, handhaving en opsporing. Dit onderzoek moet passen binnen de doelen van loov. Dat staat in die bewoordingen bevestigd van in jaarplannen en in projectvoorstellen.

loov werkt met legio bestanden van de deelnemers. Het gaat op dit moment om specifiek de volgende databelangen:

- bestanden over vermogensposities van de Belastingdienst;
- Informatie over de status van Koophandel;
- verdachte transacties en handhaving- en antecedent informatie van de politie.

loov werkt met de kopieën van de bestanden van de deelnemers, waaronder belangen in met data van alle belastingplichtigen, en belangen in de zelf. Ze staan op een apart deel van de rekencomputer van het om.

Er is een 'godsdienst van de aardelijkheid' voor de juistheid van de data. In eerste instantie levert die bij de aanleverende partner. Nadat data concreet zijn overgedragen, is de aanvrager hier voor vervolgens verantwoordelijk.

Door deze werkwijze met kopieën van dumps (of wel databases) zijn de producten die bij loov worden gemaakt, niet altijd even actueel. Dit hangt onder meer af van de frequentie waarmee de bestanden of gegevens daaruit worden aangeleverd; soms zijn die dan niet actueel te verkrijgen (de databankangifte bijvoorbeeld doet men slechts één keer per jaar).

Intelligentieproducten helpen dus te prioriteren en te filteren, maar voor wettelijke juridisch bewijs moet de aanvrager terzake gaan bij de bronbestanden. Hij weet dan inmiddels wel in welke bestanden hij de grootste kans heeft om dat te treffen.

loov laat steeds verschillende combinaties van indicatoren loov op deze databases en beschikt over steeds verschillende toelating om alle bestanden in één keer te ontsluiten, en daarmee snel vastgoed, ander vermogen en transacties van personen in kaart te brengen.

Bank en leuven gaan bestanden met transacties van loov. Het leverantietransacties waarover loov beschikt, zijn afkomstig van de Financial Intelligence Unit-Nederland (F.I.U.-N). Bank en andere instellingen zijn wel verplicht om ongebruikelijke transacties te melden aan de F.I.U.-N. Het is de taak van de F.I.U.-N om deze transacties te analyseren en de transacties die verdacht zijn, beschikbaar te stellen aan de opsporingsdienst.

Ook het o.j.b. levert geen bestanden aan. Het o.j.b. vraagt wel producten op om betalingsregelingen te kunnen treffen, datageregelingen leggen en om belastingprioriteren. Voor dat laatste wordt bijvoorbeeld een lijst van personen aangeleverd met openstaande ontnemingsvorderingen. Icoo v kan heel snel laten zien bij welke personen de meeste verhaalmogelijkheden zijn.

De techniek om data bijeen te brengen is nauwkeurig vastgelegd en belangrijk. Icoo v en deelnemende partijen moeten samen bestanden technisch aanpassen voor verwerking tot de formaten die Icoo v hanteert voor bundeling van data tot een informatie geheel.

De datastroom begint bij de bronbestanden vanuit de belastingdienst, oorspronkelijk de data. Deze worden samen opgeslagen in een staging database, waarop bewerkingen worden uitgevoerd voor een slimme upslag, oftewel zodanig gebundeld dat ze functioneel zijn. Dit resulteert in een bronnen database, 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 vermenigvuldiging plaats en koppeling op naam (bsn), oftewel analyse met verschillende tools.

Daaruit volgt dan bijvoorbeeld een rapportagevermogen en inkomen, een vrijgevroegd product waar in data vermeld en gekoppeld zijn. Sommige data worden toegelaten, andere data worden geweigerd of verkloord. Daar toe zijn er twee soorten van verwerking van data: voor productie op naam en toenaem (bsn) en anonimiseren.

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 bekend zijn, worden deze als kennistools in de productieomgeving geplaatst.

Icoo v maakt geen gebruik van open internetdata van bijvoorbeeld LinkedIn, Facebook en Google. Het eventueel gebruik van deze bronnen wordt overgelaten aan de participanten, oftewel de klanten van Icoo v die dat opvragen. Icoo v heeft ook geen toegestuurde interne bestanden waarin het random zoekt naar specifieke patronen. Icoo v werkt met grote hoeveelheden gestructureerde data, die grotendeels afkomstig zijn van deelnemende partners.

12.3

data analyse in de praktijk

Icoo v hanteert drie productgroepen of rapportages:

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

dergelijk rapportage staat informatie over onder andere loon, vastgoed en vermogen.

Op dit moment zijn in dit overzicht opgenomen: (eventueel) loon, bezit vastgoed, bedrijven, stichtingen, hypotheek en box 3-vermogen, winsten, alimentatie, auto's, aandelen, toeslagen en verdschtransacties. Handsameoordening en werkgeveinden 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 af te betalen en voldoen).

2. Relaties: relatienetwerk rondom of tussen personen en/of organisaties. In 'duizelingwekkende snelheid' wordt in de systemen zakelijke contacten, vastgoed en andere in kaart gebracht en grafisch weergegeven. In de loop van vier lagen diep kunnen binnen een minuut relaties op niveau van adres, werkgever en collega's, vastgoed, Kamer van Koophandel in kaart worden gebracht. Crimineel verkeer 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 informatieparing beperkt. Iedereen is op verdrillende wijze met anderen verbonden. Denk bijvoorbeeld aan werkgevers met duizenden werknemers, waarbij niet iedereen dikwijls persoonlijk komt. Om die reden is bij dit product ingebouwd dat de computer bij een specifiek aantal werknemers een 'stopflag' plaatst.

De aanvrager komt bijvoorbeeld langs om samen met experts van de overheid te kijken naar de 'brutoversie' van de relaties om daarbij aan de aanvrager aangeven welke relaties wel, en niet van belang zijn voor zijn onderzoek. De niet-relevante (juridisch gezegd: niet-noodzakelijk) 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 brutoversies worden wel bij de aanvrager 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 bestendvergelijking kan het gecoördineerde thema met risico-indicatoren causalistiek 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 bijvoorbeeld risicoindicatoren toegepast op de toegestane bronnen (open, gesloten en privaat, alleen voor zover die voor de aanvrager gebruikt mogen worden).

Het beeld dat hier uit ontstaat, biedt mogelijk heden voor nadere analyse en het bepalen van interventiestrategieën. Dit is het tijdrovendste product van loov, 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 themasonderzoek: het geld lenen van jezelf kan (maar hoeft niet te) vallen onder een typologie van witwassen die de Financial Action Task Force (f.a.t.f.) onderscheidt. Om diens reden wordt dit gegeven gecombineerd met diverse andere indicatoren, waaronder informatie dat een particulier in 'risicolanden' gestelde 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 f.d. is hiernaar onderzoek gaan doen.

12.4 & development research

Naast het leveren van producten (vermogen en inkomen, relaties en thema's) doet loov ook aan Research & Development (r & d; Onderzoek & Ontwikkeling).

Deze afdeling binnen loov 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 (toegepaste) wetenschappelijk onderzoek (criminaliteitsbodendynos).

Deze afdeling kent een eigen regimede 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 laatste genoemd 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 w.o.d.o en/of universiteiten.

Bij het ontwikkelen en valideren van indicatoren wordt onderzocht wat elders al bekend is, bijvoorbeeld bij de Financial Action Task Force (f.a.t.f.), waarin 34 deelnemende landen zich bezighouden met de bestrijding van witwassen op de financiering van terrorisme. In het project Operationaliseren Witwasindicatoren f.a.t.f. worden de indicatoren afkomstig uit de typologieën van de f.a.t.f., gepersonaliseerd in de data die bij loov beschikbaar zijn.

Deze indicatoren kunnen vervolgens worden gebruikt om bijvoorbeeld een themascan te maken (al blijft tekens 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 vraagtuning 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 gevraagd, aangezien (ook hoofdsakelijk 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 klinkbordgroep.

Daarnaast zijn er momenteel twee promovendi werkzaam bij iCoov. De onderzoekers werken in een geschieden omgeving, één of twee bijna afgestudeerde criminologen en/of forensischekundigen kunnen gelijk tijdig stage bij iCoov lopen, voor meer stageplekken (en hun begeleiding) heeft iCoov geen ruimte.

Een voorbeeld van fenomeenonderzoek is het onderzoek dat in samenwerking met de Landelijke Recherche is gedaan naar de kenmerken van Outlaw, Motorcruide Gangs, in vergelijking met driehonderd anderemannelijk en motorrijders uit dezelfde leeftijdscategorie. Uit het onderzoek kwam naar voren dat 82 procent van de clubleden een jas-registratie (justitie documentatie, voorheen: strafblad) had, tegen 33 procent gemiddeld binnen de controlegroep. Binnen de Outlaw Motorcruide Gangs zijn er veel vaker dubbelvuzedubbeleuren – 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 heeft 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 iCoov om de 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 politiestystemen, wat ongetwijfeld invloed heeft gehad op het grote percentage registraties. Vanuit Big Data-oogpunt blijft de cruciale vraag: welke praktische betekenis heeft dit? Je kunt de groep nader onderzoeken en inzoomen op details.¹

12.5

resultaten

In 2014 heeft iCoov ruim duizend verzoeken omtrent vermogen en inkomen van de deelnemende organisaties in behandeling genomen, 52 procent van deze vragen was afkomstig van de politie (incl. de Rijksscherche), 14 procent van de Belastingdienst, 11 procent van de Belastingdienst en 23 procent van het om (incl. het cijb).

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 loov in het leven is geroepen.

Levering van een rapportagevermogen en inkomen vindt binnen twee dagen plaats. Van relatieswerken 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 loov toe moet komen. 43 procent van de aanvragen was afkomstig van de politie (indirect) of een andere, 20 procent van de d... , 33 procent van de Belastingdienst en 10 procent van het om (indirect) of een andere.

Deze dataverzameling en -verwerking gebeurt een tijdje instop van weken en maanden ten opzichte van traditioneel onderzoek 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 langer tijd: weken of maanden, tegenover een druk op de knop en andere analyse bij loov.

Een rapportage is een "niet intelligente voorbeeld", dat volgens loov te beschouwen is als "stuuringsinformatie", maar niet als bewijsvoering. In rechtszaken levert loov-informatie alleen waarschijnlijkheid op de feiten. Voorbeelden van op deze manier in beslaggenomen criminele vermogens zijn niet voor handen. Dat komt deels omdat het intelligente product een schakel in een veel groter geheel en deels omdat er relatief veel tijd verstrijkt tussen de bestaatslegging en de uiteindelijk veroordeling/ executie: loov bestaat pas sinds 2013.

Uit tevredenheidsonderzoek onder de deelnemers blijkt dat loov in het algemeen wordt gewaardeerd met een 7,6. Vooral de snelheid wordt zeer gewaardeerd. loov is in de loop van anderhalf jaar wel relatief maar bij complexe zaken betrokken geraakt, zoals ondermijnende criminaliteit van de xto-productie en hennepcultuur, en terrorismefinanciering.

Het aantal aanvragen is nu nog goed te behappen, maar bij voorliggende groei kan er een probleem ontstaan en zal loov bij gelijk blijvende capaciteit de aanvragers/deelnemende organisatie mogelijk moeten gaan bewegen selectiever te worden in hun aanvragen.

De waardeering voor themaonderzoek blijft achter, wat loov zelf ook onderscheidt: de themaonderzoeken zijn nog onvoldoende ontwikkeld en tijdrovend. Daar door brengen ze (nog) niet altijd de gehoopte uitkomsten en aansluiting bij behoeften, omdat er teling op moet worden gewacht.

loov voert hooguit tien tot vijftien thema's per jaar uit, want ze zijn arbeidsintensief. Voor loov is dit het product waarvoor nog het meest ontwikkelen valt en daarmee wordt in 2016 een aanvang gemaakt.

Overigens meldde het kabinet in een brief aan de Kamer dat een investering vanaf 2016 in de strafrechtelijke van 20 miljoen euro voor de beslagname op crimineel vermogen moet leiden tot 60 miljoen meer in beslaggenomen crimineel vermogen. De doelstelling is dat er vanaf 2016 jaarlijks ruim 100 miljoen aan crimineel vermogen in beslag wordt genomen. In 2016 was dat bijna 60 miljoen euro volgens het om, in 2014 al 166 miljoen en in 2015 143,5 miljoen.²⁵³

12.6 **hinderpalen en vraagtekens**

loov is een jong partnerwerkingsverband, dat vooral wordt steun met juridische grondslagen: er is ontzettend veel, maar wat is toegestaan op grond van vooral privacyregels? De vraagtekens op een rij:

- Complex maatschappelijke vraagstukken vereisen een multidisciplinaire oplossing.
- Complex maatschappelijke vraagstukken (waaronder fraude, ondermijning, criminaliteit, problematiek in het zuiden van het land etc.) kunnen niet door één enkele overheidsinstelling alleen worden opgelost, ze vergen een multidisciplinaire en gezamenlijke of afgestemde aanpak, aldus het hoofd loov. Daartoe werken verschillende overheidsorganisaties verregaand samen vanuit verschillende disciplines/ expertise 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 loov in de praktijk ook: een aanvrager van een loov-intelligentieproduct mag alleen die informatie ontvangen die hij op basis van zijn wettelijke bevoegdheid mag aanvragen. Binnen loov worden alleen gegevens verwerkt als daar door een deelnemende organisatie om wordt verzocht (100 procent vragenlijsting), zodat helder is op grond van welke taak, welke bevoegdheid en met welk doel gegevens verwerkt worden.

De doelstellingen van veel participanten overlappen wel, maar zijn meestal niet eenduidend. Gechargeerd: de politie is niet of minder geïnteresseerd in belastingontduiking of zwart geld, de Belastingdienst niet in de crimineel verzege inkomsten, zolang er maar belastingover wordt betaald.

²⁵³ Voorlopig Rijkswaarde aanpak van fraude (ht://www.tweedekamer.nl/vergaderingen/commissievergaderingen/details?id=2016A00538).

Daardoor is er geen toereikende, eenduidige grondslag om complexe problematiek in zijn geheel (bijvoorbeeld desanpak 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 loov, te weten het opsporen van crimineel en onverklaarbaar vermogen dan wel het blootleggen van witwas- en fraudeconstructies of het als-nog-innen van overheidsvorderingen. Anders kunnen ze niet toezien tot het convenant.

loov zelf beschouwt deze doelbinding op zich niet als een probleem. Wel de 'niet-eenduidige doelstellingen' van de samenwerkende partners, waarvoor een toereikende, eenduidige grondslag ontbreekt om complexe problemen als geheel aan te pakken.

Proportionaliteit en determinisatie

Benative 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 oninzigheid kunnen worden en men tevoren ook niet gezegd kan worden van welke gegevens moeten worden opgevraagd. Dit doet jope bij de aanvraag van het product. Van die Nederlanders zijn veel data voorhanden.

Het aantal 'productieopdrachten' van loov, dat wordt aangevraagd door de deelnemende partners, bedraagt drie vijftienhonderd per jaar. Minder dan een promille van de personen van wie grootschalig data is bijgebracht zijn, zijn ook onderwerp van onderzoek.

Het is dus enerzijds noodzakelijk om alle gegevens klaar te hebben staan onder verantwoordelijkheid van de aanloovende partij, maar anderzijds worden deze zeker niet allemaal gebruikt. Als gezegd, worden alleen die vragen beantwoord die op basis van de juistewettelijke bevoegdheid mogen worden beantwoord.

Wellicht ten overvloede: er is dus eerst een verduidelijking nodig en een vordering van de officier van justitie om fiscaal data te kunnen ontsluiten en te mogen verstrekken aan de politie. Deze toestemming van het om is een afdoende juridische verklaring en de inzet van deze wettelijk bevoegdheid wordt getoed door de strafrecht. Met de toename van de hoeveelheid data bestanden wint deze bevoegdheid aan belang.

Juridische voorzichtigheid

Juristen worstelen met de grenzen van de regelgeving en kijken snel voor voorzichtigheid, wellicht te snel volgens de uitvoerend diensten. Maar, zo raden ook loov, vertrouwen komt te voet en gaat te paard.

En daarom zeggen de deelnemende partners binnen loov te kiezen voor zorgvuldigheid en het wikkelen en wegen van de inzet van middelen. Ook vereisen de juiste werking van het juridische kader en nieuwe juridische vragen continuïteit en aandacht. loov 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 loov wordt twee tot drie keer per jaar over de voortgang en activiteiten van loov verantwoordt gelegd aan de opdrachtgevers in een besloten opdrachtgeversoverleg, de hoogste leidinggevenden van de participerende overheidsorganisaties die aan loov deelnemen, hebben hierin zitting. Als toezichthouder kan de Autoriteit Persoonsgegevens besluiten tot een onderzoek naar privacy bij loov, net als bij alle andere overheidsinstellingen. loov heeft op eigen initiatief eind 2013 een presentatie gegeven bij de opzet van de productieomgeving. De ap had daarbij vooraf aandacht voor de geëceerde verantwoordelijkheid in de productieomgeving. Sindsdien is binnen loov verder nagedacht over de mogelijkheden van datamining.

Transparantie

loov wil de exacte werkwijzen voorzicht houden om te voorkomen dat verdacht en en te intimideren de wet, kunnen of hoe zedig de apen werk kunnen ontlopen. Openbaarmaking van deze 'keukengeheimen' staan op gespannen voet met het rocherdewerk. Slagvaardigheid en succes komen dan in het geding. loov vreest dat verdachten en veroordeelden het vastleggen van relevante data zullen ontwijken, zodra ze kennis hebben van de methoden. Zo zijn van drie producten de beschikbare en gebruikte data van participanten exact beschreven, maar niet openbaar. Vanzelfsprekend kan loov de gevestigd gevraagd worden teksten uitleg te geven in bijvoorbeeld een strafzaak waar van loov-producten gebruik is gemaakt. De processen zijn nog niet onder controle onder of getoetst. In 2016, doorlopend in 2017, zal een audit plaats vinden. De audit 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 mandatenregelingen zijn wel openbaar. De daaruit voortvloeiende praktische criteria voor soort product zijn vastgelegd in een productenoverzicht dat vertrouwelijk is. Ook de beschikbare bestanden, waarvan een aantal is genoemd, zijn niet openbaar gemaakt. loov valt onder de Wet openbaarheid van bestuur (wob), de beantwoording daarvan loopt via de ministeries van Financiën en Veiligheid & Justitie).

Afstemming om tot (re-)onderzoek te komen vergt soms (te) veel tijd. Als voorbeeld kan dienen het project Subjectgericht Aanpak Beropstrafzaken, 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 bredere organisatie van de politierechtssamenhang en vele juridische vragen, vertraging op. Ook speelt bij sommige partijen de oude afwering om de data beschikbaar te stellen, een rol.

Doorspelen van informatie

Goederenpartners halen hun informatie op tal van plaatsen. Zo komt het voor dat onderzoekers werken met (verschillende) informatie uit verschillende bronnen verkrijgen (eigen systemen, open bronnen, bijvoorbeeld traditie, etc.). Icoov heeft een beperkte scope van partijen met wie zij samenwerken aan welke zij Inteligenoproducten mag verstrekken. Tegelijkertijd nemen de deelnemers aan Icoov ook aan andere samenwerkingsverbanden deel. Dat maakt de kans op het doorspelen van informatie van een Icoov-product – zonder dat opnieuw goed getoetst is of die informatie wel met al die andere partners gedeeld mag worden – niet ondenkbaar. Zou kan een GUL – analist van de vermindering van de Belastingdienst de verkregen informatie ook in een andere context inbrengen, bijvoorbeeld in een Regionaal Informatie en Expertise Centrum (r-ico).

Icoov kan voor doorverzekering geen verantwoordelijkheid dragen; het is aan de gemeinde die Icoov-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).

Icoov waarschuwt bij verstrekking wel voor oplettendheid op dit punt. Uiteindelijk is het aan de rechter om te oordelen of het doorspelen van informatie rechtmatig was. Uiteraard houdt op ook hierop toezicht en hebben alle organisaties privacyfunctionarissen in dienst, die adviseren over informatie-uitwisseling en informatieverstrekking.

Er wordt daarbij getracht gewerkt: een brokje vragen informatie met een concrete verdenking wordt gemengd met eigen onderzoek en keert terug in een uitgebreidere vervolgvraag, bijvoorbeeld om dat daarmee een verdenking sterker is geworden of zich heeft uitgebreid tot andere personen.

Gebruiksgereguleerder

Het samenwerkingsverband wordt niet ook met de vraag om, zoals, 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 despedtiek aanvragen die bij i.o.v. worden gedaan en dat leidt tot belangrijke informatie, maar niet tot een totaalplaatje. Voor het oplossen van complexe (ondermijnende) maatschappelijk epiproblematiek bestaat bij samenwerkingsverbanden als i.o.v. grote behoefte aan een meer generiek grondslag waarmee ook complexe fraude- of wettigheidsproblemen gezamenlijk aangepakt kunnen worden. Ook de op handen zijnde Kadewet zal daarin – op basis van de huidige uitgangspunten – vermoedelijk niet voorzien.

Dat brengt het risico mee, aldus i.o.v., dat de informatieproducten losse puzzelstukken blijven, die niet of slechts deels in elkaar passen. Daar maak ik het doel om tot een beter inzicht te komen in de problematiek en tot een gezamenlijk aanpak, niet worden bereikt. Nu moet steeds weer despedtiek grondslag van de aanvragers als uitgangspunt dienen.

Elke deelnemende organisatie is gebonden aan specifieke restricties in gegevensuitwisseling. Vanuit zijn taakstelling is i.o.v. er vooral in geïnteresseerd dat er wel een generiek grondslag komt, zodat het de deelnemers aan het samenwerkingsverband beter van dienst kan zijn.

i.o.v. is nu beperkt in de mogelijkheden om bijvoorbeeld de wettigheid van politieverzoek om data van de Belastingdienst te beantwoorden in de fase waarin een onderzoeksvondeling nog ontbreekt. In hoeverre en dan de fidele gehandhaving worden opgeheven?

Voor een verkennend onderzoek (themasonderzoek op grond van aanwijzingen) bestaat geen juridisch titel, behalve voor terrorisme (Artikel 189g, nh Sv), waarvoor wel bestanden gevorderd kunnen worden. Voor ernstige vormen van (grootschalig) witwassen of fraude bestaat zo'n grondslag niet.

Over waar die grondslag aan pick 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 uit te aard met voldoende aanpak, 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 nieuw 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 2016 aan de Kamer: "Om gezamenlijk effectiever te kunnen aanpakken wil het kabinet de informatie-uitwisseling verbeteren. Samenwerk-

kingsverbanden als de Regionale Informatie en Expertise Centra (rieo's) en de Infobox Criminal en Omveelbaar Vermeden (ioov) kunnen hier best bij helpen. Het kabinet denkt eraan om een nieuw wet te maken die gegevensuitwisseling voor de aanpak van fraudebestrijding moet versimpelen [...] Nieuwe wetgeving kan de gegevensuitwisseling vergemakkelijken, zodat bijvoorbeeld politievoetballen gegevensuitwisseling niet meer persamenwerkingsverband hoeven te regelen.²⁵⁴

Naast het aanpakken van een aantal bekende beroepsfraudeurs wordt in het kader van dit rijksbrede project medio 2016 ook een verkenning afgerond naar een meer innovatieve manier van dataanalyse met als doel breder gebruik van indicatoren van beroepsfraudeurs in het Nederlandse publieke domein vast te stellen. Het doel van de verkenning is om risicoprofielen op te stellen die tot nieuwre inzichten en een meer effectieve aanpak van beroepsfraudeurs kunnen leiden.²⁵⁵

12.7

toekomstige opties met 'big data'

ioov heeft een 'potentieelverkenning' & d' laten uitvoeren om mogelijke ontwikkelrichtingen in kaart te brengen. Daarbij is gesproken met universiteiten, onderzoeksinstituten, met de vigen particuliere en de organisatie in het samenwerkingsverband, waaronder met betrokkenen bij Syrië-Law (Universiteit Leiden), tu Twente, de Vrije Universiteit Brussel, n f (Kazda), het Rathenou Instituut en de ind.

Deze verkenning levert een aantal inzichten op:

- Het potentieel van **data mining op bestaande data** wordt enorm geacht door de experts.
- De technieken kunnen zowel beschrijvend als voorspellend worden. Fraudebestrijding vraagt om dynamische modellen, gezien de voort veranderende kenmerken van dit fenomeen.
- Op hoofdlijnen zijn er twee analysemethoden te onderscheiden wa informatie uit de data gehaald kan worden, te weten één waarbij met bestaende en bestaanden wordt gewerkt, de andere waarbij in nieuwe netwerken gebruik wordt gemaakt van kunstmatige intelligentie. Deze methoden kunnen elkaar aanvullen.

254 Deze op handen zijnde Kadernet gegevensuitwisseling zal er wellicht in voorzien dat samenwerkingsverbanden gegevens mogen doorgeven aan de politie en aan het omzondagerechtelijke vordering. De Autoriteit Persoongegevens kritisch, evenals privacyorganisaties. Ze willen betere waarborgen en restricties.

255 Voorzorg Rijksbrede aanpak van fraude <http://www.tweedekamer.nl/vergaderingen/commissievergaderingen/detail?id=2016400888>

- Het is verder mogelijk om door het gebruik van technologie vooroordeel 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 privacy risico's daarbij worden beperkt.
- Geautomatiseerde besluitvorming is verboden volgens de Wet bescherming persoonsgegevens.
- Uitkomst van toepassing van nieuwe technologie kunnen ook gebruikt worden om juist een grens te creëren: dat betekent het niet rust laten of belonen (bijvoorbeeld door een snellere behandeling/toekenning van middelen aan of) van degenen die een diefstalindicator vuldoet. Bijvoorbeeld door bij de Belastingdienst toestaten de aanvragen die 'groen' zijn, versneld te behandelen en de aanvragen die 'rood zijn' helemaal extra te bekijken. Aangezien looijust tot dood 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 in witwassen en fraudestructuur geven. Die kennis kan door de deelnemende organisaties worden ingezet om opsporing, handhaving, toezicht en bedrijfsprocedures te verbeteren.
- Op subjectniveau zouden dergelijke analyses kunnen bijdragen aan een pak kans, slimmere selectie van zaken en ook om anderen in beeld te krijgen, dan degenen die te zien zijn in de 'criminele achteruitkijkspiegel'.

Op dit moment is het echter juridisch niet mogelijk om dit met de data die op subjectniveau te doen: de bevoegdheden van de organisaties zijn hiervoor in het algemeen niet toereikend. Om dit mogelijk te maken is eerst een goed wettelijke grondslag nodig. Daarvoor is een politieke en maatschappelijke discussie over het gebruik van dit soort technieken in een combinatie van verschillende data bronnen vereist. Vandaar dat looijust doet op subjectniveau.

Dit probleem doet zich niet voor bij het verkrijgen van nieuwe kennis uit & d op grond van geanonimiseerde data die opgeen enkele vrijzette personen herleidbaar zijn. Ook dit kan leiden tot betere efficiëntie en keuzes in opsporing en uiteindelijk tot toename van terugterwinst van vermogen.

looiijust 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 afgeschieden omgeving met beperkt data en leidt dus tot anonieme resultaten. De opdrachtgevers van looijust zijn voorzichtig, omdat ze zich realiseren dat negatieve beeldvorming over deze pilot een negatief verslag kan hebben op de pro-

duidelijke omgeving die zich al bewezen heeft. ("Denk aan Syr i, waarbij besldvorming op de loop ging met de methode")

De benodigde expertise zal ook vervoer modelijk - deels - buiten de deelnemende organisaties moeten halen door bijvoorbeeld samen te werken met een onderzoeksinstituut. Aangezien ook veld 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 verkaren nog in het stadium van verkenning en peeshtevorming. Het is nog niet duidelijk hoe een en ander daadwerkelijk vorm zal krijgen.

12.0

risicocomdngen malafide bedr

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: Risico profielen,

Automatizedanalyse, Distributie van afnemers en Aanvraag op verzoek. Radar produceert risicocomdngen over mogelijk malafide bedrijven en stichtingen op grond van data uit de volgende bronnen:

- Nederlands Handelsregister (
- Basisregistratie Personen (
- Centraal Inkoopantiregister (
- Justitieel Doelregistratiesysteem (

Bij verdenking doet screeningsautoriteit Justis van het ministerie van Veiligheid en Justitie onder handmatig onderzoek naar de rechtspersoon, met aanvullende informatie uit (gepubliceerde) bronnen, zoals van de Belastingdienst, het Kadaster en de Rijksdienst Wegverkeer. Justis en de leverandier van Radar formuleren en vertijlen risico profielen.

Van de meldingen duidt 80 procent op risico op faillissement of fraude, de rest betreft verdenkingen van witwassen, belastingfraude (ook btw), beleggingsfraude, drugs- en mensenhandel.

Justis zegt niet te weten wat de resultaten van deze operatie zijn, omdat de afnemers van risicocomdngen die niet willen of kunnen terug melden. Er is alleen bekend dat de Belastingdienst, de Justitie, het nrm, de dnm, notarissen en andere partners (mede) mede dank zij de tips van Justis de nodige acties verrichtten, 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.²⁵⁵

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.²⁵⁶ De exploitatie is in handen van diendienst Justis.

Al in de evaluatie van de Wet op controle op rechtspersonen van januari 2014 is verslag gedaan van de aantallen verstrekte risicomeldingen en gevolgen.²⁵⁷

1 juli 2011 tot 1 juli 2013

- 1 miljoen rechtspersonen:
 - 1,5 miljoen wijzigingen Handelsregister gedurende twee jaar
 - 20.000 wijzigingen in automatische analyse door Radar;
 - 688 systeemmelding;
 - 37 risicomeldingen verstrekt aan één of meer afnemers.

Daarnaast op verzoek van afnemers:

- 28 risicomeldingen;
 - 118 netwerk analyses verstrekt.

Justis verstrekte cijfers over 2013 en 2014:²⁵⁸

- 1 miljoen rechtspersonen;
 - 2013:
 - 359.886 wijzigingen Handelsregister in Radar;
 - 1942 zaken door Justis opgepakt
 - 118 risicomeldingen aan partners verstrekt.

²⁵⁵ Alert van Capgemini wordt ook genoemd als niet goed aangelegde toepassing voor data-analyse bij bestrijding van uitkeringsfraude in het hoofdstuk over gemeenten.

²⁵⁷ 911 Bestrijding georganiseerde criminaliteit 2016: 116 brief van de staatssecretaris van veiligheid en justitie aan de Tweede Kamer, 27 augustus 2015.

²⁵⁸ http://zoek.officielebekendmakingen.nl/dossier_29511_kat-29511_10

Evaluatie Wet controle op rechtspersonen, 23 januari 2014

<http://www.rijksoverheid.nl/documenten/rapporten/2014/01/23/evaluatie-wet-op-rechts-personen>

‘Toezicht op rechtspersonen verstevigd’, Nieuwsbericht Justis, 3 april 2015

<http://www.justis.nl/Nieuws/2015/toezicht-op-rechts-personen-verstevigd.aspx>

²⁵⁹ Lijst van vragen en antwoorden over het Jaarverslag Ministerie van Veiligheid en Justitie 2014
<https://www.tweedekamer.nl/kamerstukken/detail?id=2016Z00008&did=2016Z002894>

2014:

- 986000 wijzigingen Handelsregister in Radar;
- 2004 zaken door Justis behandeld;
- 282 risicomeldingen aan partners;
- 110 "netwerk takeningen" geproduceerd.

Justis vestrekt risicomeldingen efficiënter, sneller en meer op maat. Hierdoor kunnen samenwerkingspartners sneller en gericht 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 maken van genoemde verbeteringen. Als resultaten werden genoemd: [...] concretere vervolging door het oplossen van een druglaboratorium voor amfetamine, inbreukking van vergunningen of nader onderzoek naar witwassen en Europese geldstromen. Verder zijn nieuwe oplichtingen geblokkeerd om omzetbelastingfraude te voorkomen, verdachte netwerken in beeld gebracht, niet eerder waargenomen bestuurswettelijke 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 fraude zoveel mogelijk te voorkomen. Ons doel blijft het voorkomen fraude, 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 datauitwisseling 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 onbegrijpelijk 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 deigerende wet- en regelgeving zijn af te leiden. En ook zijn er koppelingen van bestanden weggelaten, als dan niet relevant.

260

Bijlage bij Kamerbrief over gekoppeld databestanden van Minister van der Steur. Inventarisatie gegevensbestanden en koppelingen
<http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2015/03/25/ik-inventarisatie-gegevensbestanden-en-koppelingen.html>

ligheid of andere vitale belangen, zoals opsporingsbelangen, erdoor geschaad konden worden.

Dovendien 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 data koppelingen.

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 toemenen'.²⁶¹ Dat delen door overheden en het daartoe optuigen van samenwerkingsverbanden vormen een absoluut noodzaak, aldus de minister, aangezien 'maatschappelijke problemen zich niet storen aan de reikwijdte van data en van individuele overheidsorganisaties. Daarom is het wettelijk dat deze organisaties, waar nodig en mogelijk, steeds meer als een georganiseerd geheel optreden'.

De in 2010 opgerichte Toev. 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 uitroepen van een wettelijke plicht of als de data verwerking (en daarmee koppeling) noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak.

Ook aan de vereiste van doelbinding, het louter verstrekken van tekoppelen data als dit niet onverenigbaar is met het doel waartoe ze aanvankelijk zijn verzameld, wordt volgens hem voldaan. De organisaties moeten het doel van deze samenwerking onderstreven en aan de verwerking moeten strikte voorwaarden zijn verbonden, zoals bijvoorbeeld in de Wet Suw i voor Syrië is vastgelegd.

In deze overheidssbrede data koppeling – dat niet in het overzicht stond – spreekt volgens de minister het Stelsel van Basisregistraties wel een cruciale rol voor de wettelijke transparantie en uitwisseling van gegevens en koppeling van bestanden binnen de overheidsverhouding.

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/2015/03/23/tk-gekoppeelde-databestanden.html>

Naar een nieuw regime

Enkele maanden eerder lag er wel een inzichtelijk overzicht van samenwerkingen met het delen van data, zij het beperkter van omvang. Het is een bijlage in de verkenning voor een nieuwe 'Kaderwet gegevensuitwisseling'. Aangezien de uitbreiding van het delen van data steeds meer spanningen veldt oplovert met bestaande wetgeving, zal 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 ambtelijk werkgroep, bestaande uit vertegenwoordigers van de ministeries van Justitie en Financiën, het om de gemeente Tilburg.²⁵²

Het intrigerende stuk werd niet opgemerkt door de parlementaire pers. Het handelt om de vraag of legitimatie mogelijk is voor een 'verdeling van' voor 'alle hi samenwerkingen die gegevens binnen en tussen het bestuurrechtelijke en strafrechtelijke domein willen uitwisselen'. De doelstelling is het wagnemen van knelpunten die optreden bij de uitwisseling van data, met name opgeworpen door de Wet bescherming persoonsgegevens (Wvbg) en de op handen zijnde Europese privacyverordening.²⁵³

Het gaat vooral om het inrichten van een 'zorgvuldig proces' voor data uitwisseling tussen instanties en toepassing voor analyse, zoals is gebaseerd op het onderdeel Syri van de Wet Suwi. Ingezet wordt op een wet die de algemene principes, voorantwoordelijkheid 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 tegelijkert, faciliteert en normaliseert de data uitwisseling. Vooral de antwoordvragen 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-

252 Kennisdeelen geeft kracht – Naar een betere en zorgvuldige gegevensuitwisseling in samenwerkingsverbanden, Rapport van de Werkgroep Verkenning kaderwet, 6 december 2014, verzonden door minister Opatstein aan de Tweede Kamer, 16 december 2014. <http://www.twedeekamer.nl/kamersstukken/dato/17dec2014/D481056.did:2014D48105>

253 Algemene wet inzake rijksbelastingen (Awr), Wet politiegereguleering (Wvpg) Richtlijn 95/46/eg van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van het 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=39721048283>

dingsbepalingen en andere beperkingen 'buiten toepassing' te verklaren moet ruimte ontstaan voor data-uitwisseling in samenwerking. Regelgeving voor opsporing moet transformeren van 'nee, tenzij' naar 'ja, tenzij'.

De geheimhoudingsbepalingen worden in feite vervangen door een algemene grondslag voor data-uitwisseling in een kaderwet. Wat moeten partijen die data uitwisselen dan nog een convenient opstellen, waarbij ze zich beropen op de ruimte in de kaderwet. 'Accountability', later rekenschap geven o.g. verantwoordelijkheid afleggen is belangrijk. Dus moet de beoogde kaderwet ook voorschrijven dat de samenwerkingverbanden 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 eerste 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 verklaring nemen partijen daarbij soms een te rampachtige 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 in geval van onverenigbaarheid van doelen in een samenwerkingsverband toch gegevens te kunnen uitwisselen.

Ook de verstrekking aan opsporingsinstanties en het om wordt eenvoudiger. Daarnaast worden barrières weggenomen voor samenwerking tussen bestuurlijk en strafrechtelijk instanties, wat 'bij uitstek' meer waarde zal hebben bij fraudebestrijding en andere activiteiten op het terrein van 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 samenwerkingverbanden, aldus de werkgroep. Het College van procureurs-generaal van het om was eerder op dit probleem. Door de bepalingen in geval 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 aderwet het mogelijk gaan maken dat strafrechtelijke gegevens door de politie, bijzondere opsporingsdiensten en het ook aan andere partijen binnen het samenwerkingsverband ten goede komen. Dit bestaat mogelijk heden zijn te beperkt.

Zo moeten voor bijvoorbeeld de verstrekking van politiegegevens aan de Regionale Informatie- en Expertisecentra (rie'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 vaststaan kunnen worden vastlegging van de verstrekking van politiegegevens, strafrechtelijke gegevens en justitiegegevens bij convenant en nadere uitwerking daarvan in een informatieprotocol, zo meent de werkgroep.

Tevens zal de beoogde aderwet voorzien in een betere legitimatie van het gebruik van moderne analysetechnieken. Samenwerkingsverbanden wistelen met de vraag of en, zo ja, in hoeverre de huidige regelgeving geavanceerde analysetechnieken toelaat. Zo moet loof voor de bestrijding van 'beroepsfraudeurs' data van personen en geleerde bedrijven en netwerk en vragenda kunnen matchen.

Ook komt dan van pas dat de kaderwet de informatieplicht van de privacywet en -wet orderingswet (Innoma), verplicht informatie van personen over de verwerking van hun data leidt uitte aard tot calculerend gedrag bij verdachten en daarmee vermindering van de pakkings.

Ter compensatie van het wegvallen van de verplichting de burger individueel te informeren, denkt de werkgroep aan een passage in de kaderwet: de algemene informatie over de gegevensverwerking door samenwerkingsverbanden voor-schrijft en op de website publiceert. Dan weet iedereen te voren dat die gegevens onderworpen onderzoek en data-uitwisseling kunnen zijn.

De noodzakelijk bepalingen over noodzakelijkheid van uitwisseling op de beginselen van proportionaliteit en subsidiariteit van de privacywetgeving aan de 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 aderwet een expliciete legitimatie zal geven aan gegevensverwerking in de vorm van data-analyse en profilering teneinde intelligentie verbeteren. Zo 'kan met een kaderwet het signaal worden afgeven dat er meer mogelijk is dan wordt verondersteld'.

Legen naar betere mogelijk heden tot gegevensverwerking staan ook bereikbaar-borgen 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 samenwerking nog moeten stemmen over nieuwe wetgeving om meer voor 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 loov om de mogelijkheden voor data-analyse en daarmee bestrijding van criminaliteit aanzienlijk uit te breiden.

Het is niet uitgesloten 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 mediatie al te doorgaans ruime aandacht krijgen.

Het uitstel biedt wel de mogelijkheid om lange tijd te debatteren over 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 veruimde – mogelijkheden voor data-analyse.

inleiding

Ten minste 2,6 miljard aan onjuiste declaraties in de zorg, bijna een half miljard jaarlijkse belastinginstap plus een miljard verwachte omstige extra winst, 100 miljoen aan crimineel vermogen en honderden miljoenen minder uitkerings- en toeslagenfraude per jaar. O ja, ook 60.000 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 gaat om uitsluitend analysericht, op concrete zaken, gaat het meer en meer richting Big Data. Dit geldt meest 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 opgemerkt verslagen en Kamerstukken.

Dit roept te 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 natievergawerk gebaseerde uitkomsten als 30 miljard fraudeschade, die als bron wordt genoemd voor spijtoorzaak.

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 ambigue begrip. Het gaat om de eerste plaats om zinnige en verspreide dieven uit analyse van data ontstaan. De vervolgens werkdijk vastgesteld fout en kunnen een gevolg zijn van onwetendheid, slordigheid en pure opzet. In het laatste geval volgt meestal geen strafzaak, medegezien de te groot geachte inspanningen en tijdsbeslag.

131

politieke wens

De Tweede Kamer legt de afgelopen jaren de nadruk op de 'integratie inspanning' voor fraudebestrijding en op minder versnippering. Het kabinet antwoorde met 'rijk breed anti-fraudestrategie' van een ministeriële commissie-Aankpak Fraude; onder voorzitterschap van de premier en de minister van Van Jaarsveldt. Ook deministers van szw., et., v.w.s. bzk., oow. Vrouwen en Jijdsdienst en de staatssecretaris van Finandien zijn vaste deelnemers aan de ministeriële commissie Aankpak Fraude. Verslaggeving van dit gaelschap is overigens niets meer vernomen. Bk w aan een reeks domingoverschrijdende voor nemens.

Dit leidde in de praktijk tot het steeds sterker inzetten op de toepassing van gezamenlijke straf-analyse door overheden en zelfstandige bestuursorganen, eventueel samen met de politie. Dit kan tot problemen leiden voor de privacy van de betrof-fene (vervolgen van de privélevens). Mid-termeterminingen zijn van belang (vanuit de Belastingdienst), ook (identiteits- en adresfraude), zw (uitkeringstraude) en VenJ (criminaliteit, witwassen) smeden verbanden voor gezamenlijk gebruik van data en andere.

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 u.w.v. de desbije kaderminde omvangrijke en intensief dan voor de bijde- en (w.b.) maar de bijnige kaden voor grootschalige analyse zijn aanzienlijk. Vooral het u.w.v. wordt voortgangende gedetailleerde plannen om dat in te zetten voor fraudebestrijding en daar ook kennis voor in huis. Desbije een stuk bescheiden met haar ambities en komt op achterstand door problemen met uitvoering (ggg) en mislukte. Desbije waarschuwt ook voor te hoge verwachtingen van opbrengsten en 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) miljaardenopbrengsten met behulp van onder meer data-analyse die in de zorg, met het wisselen en al dan niet bewerkstelligen van ontwikkeling en –ontduiking haalbaar zijn.

Dit is waarbinnen de publieke opinie, waarin de verantwoordiging over fraude met uitkeringen het grootst is. Direct betrokkenen wijzen op de gevolgen van deze maatschappelijke eenreunde over het trekken van uitkeringen. In reactie tot de omvang van de fraude is de data inzet voor bijstandsfraude volgens hen vóór of na het trekken van uitkeringen.

Interim, welke afhangt van de aard van de analyse en koppeling van bestanden aan data-analyse-
bestrijding levert, is moeilijk hard te maken. Voorlopers als Belastingdienst, zorg-
verzekeraars en locov (financiële en infaalbestrijding) spreken van enorme bij-
dragen. Dit nauwelijks te specificeren zijn wat betreft het succes van data-analyse,
omdat ze een onderdel vormen van processen. Eerder genoemde bedragen worden
er (of niet) deels aan oegehangen.

13.2

zoveel mogelijk data

Teneinde fraude en risico's daarop in beeld te krijgen, willen fraudebestrijders en hun organisaties over zoveel mogelijk relevante data verzamelingen beschikken. Gecombineerd gebruik vergroot de mogelijkheden voor bepaling van verdieningen 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 Finandien (belastingen en toeslagen) raken verweven met criminaliteitsbestrijding, het domein van Vond Dit wordt gevoerd door maatschappelijk contact.

Meest recente voorbeeld vormt de strijd tussen openbaar bestuur en criminaliteit in gemeenten in met name het zuiden van Nederland, zoals geschiedt in de media. Samenwerkingsverbanden voor lukwelen op criminele afvalbestrijding (r l e d s) moeten alle zaken bijzetten en krijgen daartoe inzage in uitgebreide databestanden.

Zowel direct als indirect, zeker kunnen gebruikmaken van organisaties die data analyse uitvoeren en van samenwerkingsverbanden die sluiten creëren tussen verschillende vormen van opsporing met data-analyse. Analogaan deze aandacht zijn er twee dataorganisaties met de grootste verzameling van databestanden voor fraudebestrijding, het Inlichtingenbureau, dat gemeenten helpt om uitkeringen frauduleus te bestrijden en looy, dat vooral vermogenscriminaliteit bestrijden. Samenwerking voor fraudebestrijding mislukt ook meer dan eens, zoals bijvoorbeeld in de zorg het afgelopen decennium. De introductie van samenwerking in de zorg heeft ook in de fraudebestrijding geleid tot het zoeken naar de juiste verhouding tussen publiek en privaat, van opsporing 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 verspreidste data and list binnen de overheid. Koppeling met externe bestanden groeit. Profileren, expliciet en impliciet, is een logisch gevolg daarvan. Zo werd zeer recent bekend dat vanuit data-analyse honderd belastingadviseurs met hun 75000 klanten in het vizier kwamen die voor meer dan 400 miljoen euro aan onterechte aftrekposten hadden gedaaid. Dit is één van de grootste successen tot nu die wordt toegeschreven aan analyse van grote databestanden die leiden tot verdieningen van fraude.

De grootste post vormen de goddelijke zorgkosten. Hierop openbaart zich een mogelijk ebehoefte om bestanden van zorgverzekeraars en Belastingdienst te koppelen. Zo is er steeds meer denkbaar, tot de ultieme data-analyse mogelijk is, afgezien van de wettelijke held.

13.3

beperkte politieke invloed

De directe politiek 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 verordeningen op grond van data-analyse. Stemmingen over concrete toepassingen en koppelingen waren niet traceerbaar, met uitzondering van wetgeving aangaande Syr i die unaniem instemming kreeg.

Exemplarisch voor de besluitvorming is de zaak over gebruik van parker data 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 stak dit dit programma.

Eerst de rechter, vervolgens een persoonlijke opvatting van de dienst als grondslag voor een belangrijk besluit. Zowel het parlement als toezichthouder apstonden hier buitenspel.

Echter, persoonlijke beoordeling van vraagstukken aangaande data-analyse en privacy in de praktijk van de fraudebestrijding speelt een groter rol. Dit treedt naar voren uit gesprekken met functionarissen die ook kennen bij data-analyse in fraudebestrijding. Ze ervaren een gebrek aan houvast en proberen een evenwicht te vinden tussen verdien van opsporing en van privacy.

Wetgeving voor fraudeopsporing wordt indertien veelal onopvallend verbreed. Het treffendste voorbeeld was de uitbreiding van bevoegdheden in opsporing in het sociale domein (wijken, arbeidsmarkten, uitkeringen) met Systeem Risk-Indicatie of Syr i. De wetswijziging ten behoeve van Syr i is bekrachtigd als de introductie van de Big Brother staat.

Echter, het instrument is jarenlang toegepast zonder wettelijk oedkking, wel met instemming van de senaat dat onttok zich aan de aandacht. Syr i 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 demediatie, vaak in de vorm van verontwaardiging.

13.4

transparantie en verantwoording

Transparantie verhoudt zich volgens de fraudebestrijders slecht met de noodzakelijke slagkracht. Terughoudendheid - debij andere partijen vaak nog groter was - is aan de eenkant begrijpelijk: de wetsovertreeders die de overheid willen moet vangen, hoeven niet gwaarschuwd te worden welke mazen in de wet en opsporing open en dicht staan.

Zeker de introductie van 'business cases', projecten waarbij de investering ten minste terugverdiend moet worden, noodzaakt tot opbrengstmaximalisatie. Icoov, het Ibm en vele andere verbanden en instanties die fraude opsporen met data-analyse, beropen zich op zowel hun snelheid en efficiëntie van werken als op hun zorg voor de omgang met bestanden. Hoe dat in de praktijk uitpakt, is echter vooral onbekend.

Transparantie over procedures en gebruik te bestanden neemt in de toekomst, niet vanwege politieke druk maar vanuit een besluit van betrokken ambtenaren. Bijvoorbeeld met de website met ruim informatie van het Inlichtingenbureau.

Van Icoov is daarentegen weinig openbaar, tenende de grote wetsovertreders die het doelwit vormen, niet wakker te schudden. Elke openbare aandacht kan het werk in de wettelijke lijnen. Gelukkig is de transparantie te data verduidelijkt, door een wettelijk vacuüm.

Zo is er voor Syrië een uitdrukkelijk wettelijke ondergrond maar veel andere data-uitwisseling wordt gedekt door conventanten dan wel eenmalige publicaties in De Staatscourant, die nimmer een parlementaire toets doorlopen.

Zo zijn de jaarverslagen van het Ibm niet openbaar, Icoov kent het fenomeen verstoppen van openbare verantwoording in het geheel niet. De interventie teams (Syrië-Inspectie) rapporteren wel in de media maar geen details over toegespeelde data-analyse.

Van veel organisaties die fraude bestrijden met data is niet duidelijk hoe ze procedures ontwikkelen en wat de uitkomsten zijn. Terugkoppeling met beleid is niet of nauwelijks zichtbaar. Openbaarheid is gering.

Zowel van het genoemde gebruik van vastlegging van kentekens bij parkeerplaatsen noch de aanvang van het vastleggen noch het stoppen aan de belastingplichtige autobezitters medegedeeld.

Zelfs met de meest in de publiek dat geraakte Big Data zaak voor misdadebestrijding, de 'Beveiliging' van telecom- en internetdata, nam de Europese Commissie, die wel geveerd in Den Haag en uiteindelijk ook de rechter besluiten voor het invoeren en ophetten. Zonder enig zicht op het werkelijke resultaat; op de baten van het vergaren en inzetten van grote databestanden noch op de werkelijke privacy-overschendingen die hiervan het gevolg waren of konden zijn.

13.5

privacybotsing

Fraudebestrijders en hun chiefs benen zich op de fast een weg tussen de snel groeiende mogelijkheden van analyse en normalisering, vaak streng ervaren privacy-regels.

Vooral de doelbinding en in minder mate proportionaliteit worden wellicht in de praktijk met voeten getreden: er bestaat gerade twijfel of de steeds bredere inzet van bestanden zich verhoudt tot de privacyvereiste dat data louter gebruikt worden voor het doel waar toe zij zijn verzameld.

Is bovendien het bundelen van tientallen databestanden in nieuwe domeinen, zoals van 100 v, nog proportionaal? De bestanden worden letterlijk overgedragen naar andere systemen voor data-analyse. Het risico op ongewenste praktijkgevalen neemt toe. Het 'shoppen' in data door individuele beampten wordt als een groot 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 welke data-analyseaanvraag.

Fraudebestrijders toonden allen hun goede bedoelingen. Privacyregels vormen hun belangrijkste grenzen. Niet dat zij die moedwillig aan hun laars lieten, maar ze zochten logischerwijs vanuit hun taakopvatting de privacyregels een belemmering.

Eigen privacyofficers bevelen grenzen, dienen het, beseft men. Voor hoeveel geldt bijvoorbeeld het getraceerde risico op 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 sporen op het open internet. Maar het online sporen door andere instanties, zoals de Belastingdienst dat zeer intensief doet, valt niet onder andere regels of toetsing.

Ook voor de Autoriteit Persoonsgegevens (ap) lijkt het dwalen met de kran open. Bij wet voorstellen toont de ap een uitgesproken en voor ieder een zichtbare invloed met advisering. Die vindt meer dan eens steun in de advisering van de Raad van State.

Editor, een aantal gesprekken waarvoor de redactie had contact met de privacywaakhond en vernam min of meer informeel over de toetsbaarheid van de methoden in relatie tot privacyregels. Die 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 valt de ap open op de hoofdredacties over privacygrenzen. Zoals de hoofdredacties op vragen open een verzoek om commentaar op een zeer uitgebreid overzicht van

alle uitwisseling van informatie, bestanden tussen verschillende overheden en zelfstandige bestuursorganen waarvan sprake is in paragraaf 10.9.²⁵⁴ Als toezichthouder doen wij gericht onderzoek naar ernstige overtredingen die structureel van aard zijn, die veel mensen treffen en waarbij de p door de inzet van handhavinginstrumenten effectief verschil kan maken. Over welke informatieve predes 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.²⁵⁵

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 consumentklacht, of verzoek om advies voor een wetsvoorstel is. Daar ontbreken ook tijd en capaciteit, voor aldus te spreken.

Op grond van tips en aandacht voor incidenten ver richt de a p soms nader onderzoek naar datagebruik. Ook voor nieuwe wetgeving wordt de a p 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 bestaande koppelingen van de toezichthouder. Die evenmin etaleert dat de deskundigheid o.p. capaciteit in gelijke mateig veel met de mogelijk heden voor toepassing van g o l e h u w e l l e h e n d a t e . Onder tussen neemt de toepassing van Big Data in de praktijk nieuwe horden. Zo publiceerde het f d op 9 m a j j l . o v e r g r o o t s c h a l i g B i g D a t a o n d e r z o e k i n h e t g e b i e d Rotterdam-Zuid.²⁵⁶ Onder leiding van het ombudsendelen overheden, banken, (zorg)verzekeraars en andere private ondernemingen hun data voor risicoanalyse. Groot schalige fraudepatronen kwamen aan het licht.

De data reeksen waren al g e e n o n m i s e e r d m a a r z i j n o o k n a h e t o n d e r z o e k d i r e c t v e r n i e t i g d v a n w e g e p r i v a c y r e g e l s . O o k l e v e r d e d e B e l a s t i n g d i e n s t g e e n d a t a . H e t o m k a n d u s r e s u l t a t e n u i t h e t o n d e r z o e k c o n c r e e t n i e t g e b r u i k e n v o o r m i s d a d e b e s t r i j d i n g . D u s w i l h e t o m r u i m e r s m o g e l i j k h e d e n v o o r t o e p a s s i n g v a n B i g D a t a r i s i c o a n a l y s e .

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 opgaan naar fraudebodeffoos hebben

254 Bijlage bij Kamerbrief over gekoppeld databestanden van Minister van de Stuur Inventarisatie gegevensbestanden en koppelingen

<http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2015/03/25/tk-inventarisatie-gegevensbestanden-en-koppelingen.html>

Word voorstel a.p. Marië Eliaander.

<http://fd.nl/economie-politiek/115070/v-big-data-leg-onzi>

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 Kadaster en 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 baten en lasten 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 uiv, de Belastingdienst, oaks, obs, oiz, oijb, Zorginstituut Nederland, Dienst Justis, r.v.o.i.n.t., duo, de indi, Kadaster, Kvk, der dw, desvb, obr, bkw en r.sj om onderlinge data-uitwisseling te bespreken. Toepassing van verdere analyse van bestanden, ook als Big Data bestanden, is onderwerp van gesprek.

Niet als in vrijwel alle tientallen samenwerkingen die zijn opgeleid 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 'datamocd' van de overheid kan het gevolg zijn, maar de vraag is of de rein 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 overwicht tussen fraudebestrijding en privacybescherming moeilijk generiek vast te stellen is. Immers, de verantwoordelijkheid van de baten en lasten van de grootchalige data-analyse, de zogeheten 'accountability' ontbreekt.

Instanties die bijdragen aan dit onderzoek, wans en uiteindelijk veel graag een verruiming van mogelijkheden om data in te zetten voor spoorwerk. Echter, een aantal van de geïnterviewden bepleit ook striktere regulering voor verantwoording. Ze zouden meer houvast willen hebben, want ze testen nu vaak in het duister over hun grenzen.

De huidige versnippering met houter, wet, twee 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 breed 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 w.b.-uitkeringen wordt het stoplichtmodel gehanteerd: rood, oranje en groen voor hoog, gemiddeld en laag risico op fraude. De Belastingdienst werkt met een 'green lane': dagbaten met een laag risicooprofiel voor belastingontduiking worden met rust gelaten bij controle. Dit

beschouwt de Belastingdienst als een gunst voor degenen die berdwijlilig data laten analyseren en 'niet te verbergen' hebben.

De komende jaren kunnen bepalen worden hoe de samenleving in de hiernavolgende decennia de voordelen van datagebruik plukt zonder daarvan blijvende schade en nadelen te gaan ondervinden.

De oplossingen waarvoor gedachten uitgaan lopen uiteen van technologie voor anonimiseren 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 dataverzamelingen uitwisseling met behoud van meer privacy, maar wordt gebrachd als Haarlemmer uit voor veel digitale vraagstukken.

Het is echter zeer de vraag of technische oplossingen afdoende zullen zijn om principiële vraagstukken op te lossen, zonder diaggende 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, gegevensbeveiliging van – al dan niet – vermeende – veiligheid en vermindering van fraude?

We beschouwen jaarlijks ontkende 800 doden en ruim 10.000 zwaar gewonden als een aanvaardbaar malschappelijk, 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 20^{de} eeuwse product, waarvan de opkomst samenvalt met onder meer vooropgaande voorstedelijking en individualisering. Het belang dat individuen aan privacy hechten, lijkt aanzienlijk verminderd met het intensieve gebruik van onlineplatforms die – onderrecht? – sociale media worden genoemd. Zowel de expliciete als impliciete – betaling voor 'gratis' diensten – bereidheid om persoonlijk edata te laten in ruil voor voordelen lijkt aanzienlijk toegenomen te zijn.

Zo aanschouwen we eveneens in de 21^{ste} eeuw een snelle toename van het etaleren van medische kwalen, onder meer in videotelevisieprogramma's. Dit werpt de vraag op: in hoeverre zijn mensen bereid om hun medische privacy op te offeren in ruil voor aandacht in grote kring, zelfs openbaar, maar ook voor medisch onderzoek? En op beperkte schaal voor fraudebestrijding om die – ook eigen – medische kosten te beperken?

En willen we belastingaangiften transparant maken, zoals een bekende Nederlandse deed in de media? En daarmee fraude en ontwijking met 'soe de 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 omtrent het evenwicht tussen fraudebestrijding en privacy/bescherming zijn louter mogelijk met een reële berichtgeving van feiten omtrent de datagebruik in de media. Niet aan de hand van incidenten en roepstoelen komen de bestaande regels voor toepassing van data-analyse tot stand, maar vanuit geobjectiverde afwegingen tussen potentiële vóór- en nadelen.

bijlage 2 financieel resultaat

21 interventieteamprojecten
waarvoor met behulp van de
voorloper van 'syri' bestanden zijn
gekoppeld en vervolgens een
risicoanalyse is gemaakt

Project	Bedrag bevestigings- aanvragen - basis	Correcties op toeslagen	Uitbaringsbedrag: 1 erugvoorwaarden en bevestigde uitbarings - 2008 (gemeenten, n = 81)	Geconstateerde gelden van overdracht Vlaamse VMI
Katholieke	3.531	2.356	820.144	N.v.t.
Middelgroot, Vlaanderen	130.696	525.270	40.830	308.000
Koninkrijk, Utrecht	130.798	5.591	724.915	85.000
DeVerg, Zelfbeheer	785.514	---	142.297	16.000
Meerdaan Nieuwsgen	103.213	---	150.958	Geen financiële resultaten
Dondersburg, Formand	983.86	66.529	22.061	4.000
Vrijheids/DeGroot/Passer	160.006	n.b.	53.92	Geen financiële resultaten
Marie Desandres, IJssel van Hambaken/ Laren	611.364	25.294	191.811	Geen financiële resultaten
Den Groot	420.542	Geen financiële resultaten	4594.67	84.000
Tweede/Anders de Poot/ Nieuwdaan/ Culemborg	Geen financiële resultaten	Geen financiële resultaten	Geen financiële resultaten	Geen financiële resultaten
DeRiet, Almelo	81.727	Geen financiële resultaten	46.060	n.v.t.
Baarle Naasau	132.1634	52.282	503.225	90.000
Sondriesen/ IJssel Amersfoort	1.322.702	3.776	110.478	8.000
Roelhaas/ Vlachof, Tilburg	569.4	61.800	18.242	24.000
Vlaanderen noord	470.516	70.558	31.140	880.000
Lutse Spectator, Utrecht	486.527	1605.567	553.384	361.125
Kern Veld	238.567	87.676	155.678	Geen financiële resultaten
Tongeren, Eindhoven	1.918.042	2.550	533.748	Geen financiële resultaten
Schiedamsloot	95.837	604.000	99.103	Geen financiële resultaten
Meerdaan, Zelfbeheer	313.306	46.570	132.497	Geen financiële resultaten
Dauwenstein, Middelburg	24.051	75.279	46.475	Geen financiële resultaten
Totaal	12.344.882	3.287.110	4.789.624	1.543.125

