

# FinPro geeft met verantwoorde big-datamethoden zicht op onzichtbare onveiligheid

**Prof. dr. Anne-mieke Roobeek**, hoogleraar Strategie en Transformatie-management, Nyenrode Business Universiteit; en directeur van MeetingMoreMinds.

***Dit artikel gaat over de achtergronden van het publiek-private big-dataexperiment FinPro. Het is tevens een oproep aan de overheid en het bedrijfsleven tot het opschonen van data. We beogen input te geven aan de maatschappelijke discussie over de verruiming van het wettelijk kader om op een verantwoorde wijze big-datatechnieken toe te passen voor de aanpak van onzichtbare onveiligheid. Met nieuwe technieken kunnen patronen van ondermijning ontdekt worden. Dat geeft interessante aanwijzingen voor het gericht inzetten van menskracht en middelen voor prospectief veiligheidsbeleid en het tegengaan van systeemfraude.***

Op het eerste gezicht lijken lege kapperszaken, straten vol juweliers, garagebedrijven, fast-food-horeca en kinderdagverblijven niet veel met elkaar te maken te hebben. Dat geldt evenzo voor toeslagenfraude, handel in vastgoed en underground banking. Het ziet er niet bedreigend uit, zoals drugshandel en high impact crime dat wel doen. Toch zijn dit allerlei vormen van onzichtbare onveiligheid die in het straatbeeld van Rotterdam-Zuid aanwezig zijn.

Maar er is meer aan de gang. Er ontstaat een klimaat waar ondermijning zich nestelt en individueel frauduleus gedrag tot systeemfraude kan leiden. Dit is vaak niet direct zichtbaar en vaak wordt het ook niet meteen opgemerkt door bedrijven of de overheid.

Het is deze vorm van ondermijning die het juridisch verantwoorde big-dataonderzoek FinPro naar de oppervlakte bracht. Dit betekent echter niet dat met de uitkomsten directe verbanden gelegd konden worden, aangezien databestanden van deelnemende partijen onder de huidige wetgeving niet gekoppeld mogen worden. De kwaliteit van de data uit het RIEC en het Veiligheidshuis waren evenmin optimaal en de meeste van de deelnemende private en publieke partijen lijdten aan interne silovorming met data-systemen die niet met elkaar communiceren.

Toch kun je met slimme software, deskundige dataprofessionals en het benutten van de collectieve intelligentie bij de interpretatie van de gevonden patronen een eind komen. En binnen de lijnen van de wet blijven. We kunnen stellen dat de resultaten van dit big-dataexperiment aangeven dat er meer speelt dan wat er aan de oppervlakte te zien is.

## **Aanleiding: ondermijning van de maatschappelijke vooruitgang**

Terwijl er met vereende kracht door het Rijk en de gemeente Rotterdam miljoenen gepompt worden in Rotterdam-Zuid, komt de beoogde maatschappelijke vooruitgang nauwelijks op gang. Voor elke positieve stap voorwaarts zijn er telkens weer negatieve signalen die de boventoon

voeren en de sociaaleconomische ontwikkeling naar beneden trekken.

Dit ligt allerminst aan de goede bedoelingen van NPRZ (Nationaal Programma Rotterdam-Zuid), noch aan de inzet van ambtenaren en private partijen. Men werkt hier uitstekend samen. Wat houdt de ontwikkeling van dit meest multiculturele deel van ons land dan tegen?

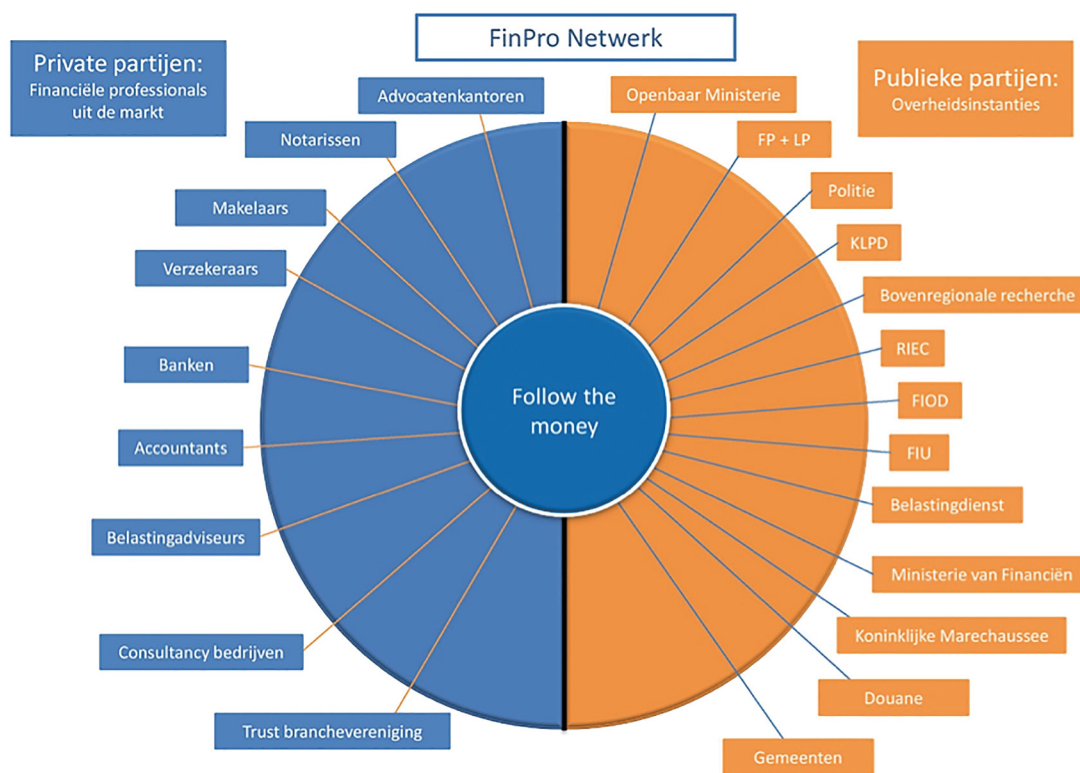
Deze vraag legden directeur Marco Pastors van NPRZ en stadsmarinier Marcel de la Haye eind 2014 voor aan netwerkadviesbureau MeetingMoreMinds, dat de afgelopen jaren als ontwikkelaar van FinPro de rol van innovatieve buitenboordmotor vervulde voor het OM. Met de opgedane kennis uit de eerdere FinPro-projecten kon nu in kortere tijd big-dataonderzoek verricht worden. Het was de start van het tot nu toe grootste maatschappelijk verantwoorde big-dataexperiment in Nederland dat met de publieke en de private sector is uitgevoerd in 2015-2016.

Het doel: patronen van onzichtbare onveiligheid ontdekken met behulp van geavanceerde data-technieken, en daarna duiding te geven via collectieve intelligentie met de betrokken professionals uit de publieke en private sector.

## **FinPro: het publiek-private netwerk rondom Follow the Money**

In het kader van FinPro, dat staat voor Financiële Professionals, is een schat aan kennis en inzichten ontwikkeld in de samenwerking tussen de publieke en de private financiële sector. Het OM heeft het voortouw voor FinPro genomen in 2011, door MeetingMoreMinds de opdracht te geven om alternatieve methoden uit te vinden die meer zicht kunnen geven op financiële fraudes die onder de radar blijven. Netwerkend werken tussen publieke en private sector en daarmee action research doen, zijn sleutelbegrippen in de diverse FinPro-projecten die tot 2016 hebben plaatsgevonden.

Het OM<sup>1</sup> heeft de mogelijkheid geschapen om binnen de lijnen van de wet vernieuwende action-researchprojecten uit te voeren rondom het overkoepelende onderwerp 'Follow the Money'. FinPro is bewust ontwikkeld als een netwer-



Afbeeldingen: Annetiekke Rooibeek, MeetingMoreMinds

De kracht van FinPro ligt in het creatief ontsluiten van professionele inzichten in een interdisciplinaire en interorganisatorische setting (het FinPro-netwerk), waarmee veel sneller het totale plaatje rond een fenomeen gezien kan worden.

kend ecosysteem, een netwerk van netwerken, met topmensen uit de private wereld van financiële professionals samen met zeer ervaren praktijkdeskundigen uit de publieke sfeer.

Door creatief nadenken, associaties te maken en verbindingen tussen de professionals te laten ontstaan, zijn nieuwe inzichten opgedaan. Er zijn effectieve interventiestrategieën ontwikkeld, waarbij vanuit het vraagstuk (financiële fraude) de casuïstiek wordt aangevlogen. Denk hierbij aan het in kaart brengen van trustconstructies, het volgen van internationale witwasroutes en het onderzoeken van misbruik van toeslagen, waarbij de overheid als financiële flappentap gebruikt wordt.

In het kader van FinPro kwam al vroeg naar voren dat het goed zou zijn om experimenteel big-dataonderzoek te gaan doen. Na een intensieve periode van overleg gaf het ministerie van V&J toestemming een methode te ontwikkelen om verantwoord big data toe te passen voor patroonherkenning in verdachte financiële transacties.

In het FinPro-netwerk zijn experts samengebracht uit de criminaliteitsbestrijding, forensische accountancy, data-analyse en privacywetgeving en regelgeving. Er is intensief afgestemd om een juridisch verantwoorde, interdisciplinaire aanpak voor een big-datamethode te ontwikkelen die binnen de wetgeving valt onder Artikel 9 lid 3 WBP 'Wetenschap en Statistiek'.

### Big data en collectieve intelligentie versterken elkaar

Big data verwijst naar de enorme hoeveelheden gegevens die verzameld en opgeslagen worden in digitale systemen. Denk hierbij aan transactiegegevens van aankopen, logboeken van activiteiten, verkeersgegevens van RDW en talloze ongestructureerde data uit sociale media en emailverkeer.

De toepassing van algoritmen om door grote databestanden te zoeken en de mogelijkheden om data-analyse te doen, zijn de afgelopen jaren enorm toegenomen. Dit opent nieuwe wegen voor onderzoek naar complexe onderwerpen zoals fraude. Big-data-analysetechnieken kunnen uit grote gegevensbestanden verbanden naar voren brengen die vooraf mogelijk niet bekend waren. Deze verbanden kunnen leiden naar nieuwe hypothesen.

Belangrijk is dat data-analyse onderzoekt waar de verbanden zitten (correlatie) en niet direct inzicht geeft in de betekenis van deze verbanden (causaliteit). Met behulp van actuele kennis van experts kan de betekenis achter de verbanden wel worden onderzocht en kan worden bepaald of verbanden relevant zijn binnen een onderzoek. Hier komt het belang van het organiseren van collectieve intelligentie met experts om de hoek kijken. Big data is dus geen vervanging van de huidige opsporingsmethoden, maar kan wel een waardevolle aanvulling hierop zijn.

### Rotterdam-Zuid

We hebben in het onderzoek in Rotterdam geheel in de sfeer van NPRZ de partijen uit de publieke (gemeente) en private sfeer samengebracht om de collectieve intelligentie aan te boren en te mobiliseren. Een woningcorporatie kijkt op een andere manier naar dezelfde doelgroepen dan het onderwijs of een verzekeraar. Breng je de verschillende invalshoeken samen, dan zie je meer en leer je meer van elkaars inzichten. Dat is in een notendop de kracht van collectieve intelligentie. Het feit dat NPRZ werkt in een netwerkverband met ondernemingen en maatschappelijke organisaties was behulpzaam om de top van organisaties mee te krijgen voor dit

» *Het is onderzoek naar de verbanden, en geeft niet direct inzicht in de betekenis*

## Ecosysteem Collectieve Intelligentie en Big Data Rotterdam



experiment. Doel was om patronen van onzichtbare onveiligheid te ontdekken. Er is gewerkt met geavanceerde big-datatechnieken in combinatie met traditionele, kwalitatieve onderzoeksmethoden.

Uit de vele interviews bleek dat er veel gemeentelijke diensten in het gebied actief zijn. Echter, vaak weet de ene organisatie niets van wat de andere organisatie doet. Ieder is gefocust op een heel klein en vaak praktisch onderdeel en doet dat zo goed mogelijk. Door het werken in silo's en op afgebakende taakgebieden is het effect van al deze inspanningen op de veiligheid uiteindelijk heel beperkt, want aan de onderliggende problematiek van onzichtbare onveiligheid wordt niet gewerkt. Het is een sympathieke manier van symptoombestrijding in de hoop dat de problematiek van achterstand en ongelijkheid niet erger wordt.

Dit verschijnsel is niet uniek voor Rotterdam-Zuid, maar eerder illustratief voor multi-probleemwijken in stedelijke gebieden. Veel organisaties zijn er druk bezig om de dagelijkse problematiek binnen de perken te houden. Ondertussen gaat het structurele verschijnsel van onzichtbare onveiligheid wel door en ontstaat er een voedingsbodem voor criminaliteit die in de haarvaten van een kwetsbare wijk gaat zitten. Sluipenderwijs wordt niet gewenst gedrag genormaliseerd. Meer mensen op woonadressen laten inschrijven die er niet wonen, maar wel uitkeringen ontvangen is een voorbeeld. Doen alsof er een kinderdagverblijf gevestigd is, gaat een stap verder. Hoe krijg je daar zicht op? Meer blauw op straat helpt dan niet. Er moeten intelligentere, eigentijdse werkwijzen ingezet worden. Vandaar dat we het big-dataexperiment met collectieve intelligentie hebben uitgevoerd.

### Samenhang tussen microdata en big data

FinPro-activiteiten zijn uitgevoerd volgens de uitgangspunten van action research. In dit kader is in 2014 een eerste experiment gedaan naar drugsrunners uit de Rotterdamse wijk Delfshaven. Dit betrof een reeds afgesloten strafrechtelijke casus en het big-dataexperiment stond los van vervolgingsonderzoeken rondom betrokken personen. Doel was om meer te zien met big data dan op de traditionele manier van opsporing en aanhouding te zien is.

Zo kwam uit deze data-run naar voren dat een bepaalde

huisarts in een ander deel van Rotterdam een proportioneel zeer groot aandeel personen behandelde uit de drugshandel uit Delfshaven. Uit het declaratiegedrag van deze groep kon de drugsroute van Rotterdam naar Maastricht afgeleid worden. Zij stopten blijkbaar vaak bij zorgverstrekkers onderweg en declareerden vervolgens bij de zorgverzekeraar. Of het echt logisch is dat je onderweg van Rotterdam naar Maastricht vaak bij zorgverstrekkers langsaat, is de vraag, maar we namen het slechts waar als een opmerkelijk patroon. Een 'anomalie' in big-datavaktermen. Deze informatie was voorafgaand aan de data-run bij de verzekeraar onbekend.

In het FinPro-experiment over Delfshaven is goed samengewerkt met de stadsmarinier aldaar, die de microstraatkennis kon inbrengen. Hij nam ook actief deel aan het FinPro-netwerkteam big data, met financiële experts en datadeskundigen. Daarin is een concept gemaakt hoe micro-kennis en macro-big data met elkaar in verband gebracht kunnen worden.

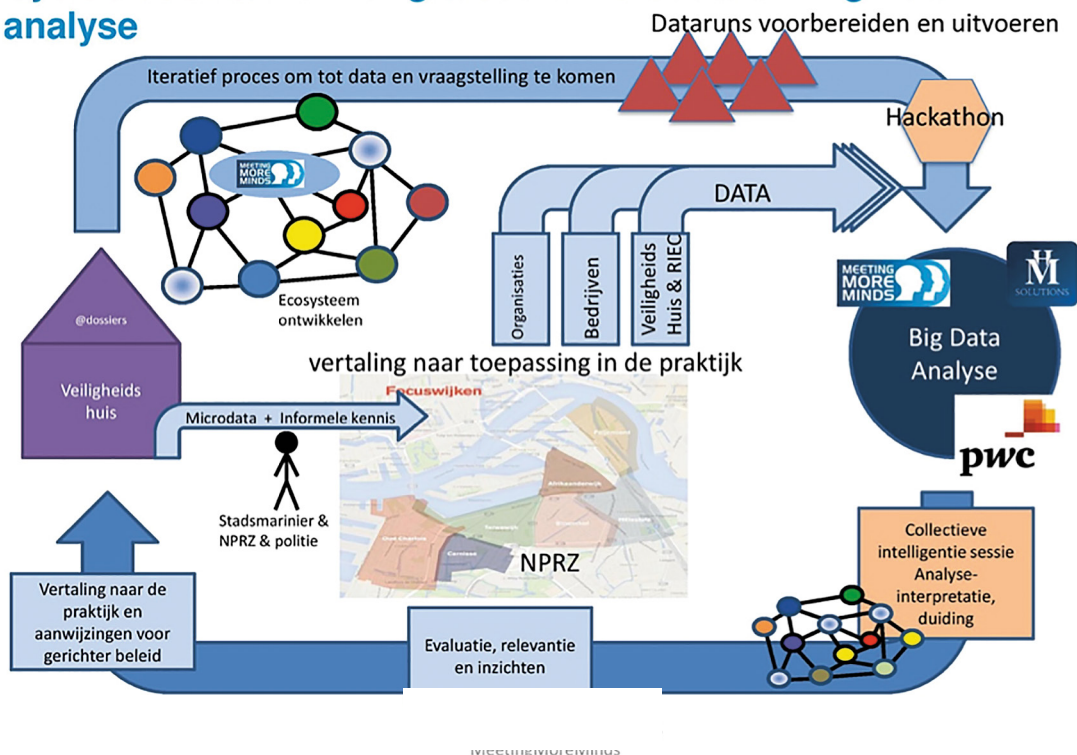
De 'action' in de action research zit hem ook in het feit dat het daadwerkelijk zo uitgevoerd is, en dat de duiding en reflectie met het FinPro-netwerkteam gedaan is. Dezelfde stadsmarinier is daarna in Rotterdam-Zuid aan de slag gegaan en werkt hierbij nauw samen met NPRZ, en ze zitten in hetzelfde pand. Door de opgedane ervaringen in FinPro was het mogelijk om snel te schakelen. Bovendien kon de stadsmarinier de verschillende experts binnen de Gemeente Rotterdam betrekken bij het big-dataexperiment in Rotterdam-Zuid.

### Tweede onderzoek

In het tweede, omvangrijke big-dataonderzoek in Rotterdam-Zuid in 2015-2016 kon voortgebouwd worden op de FinPro-kennis en de eerste big-dataruns die in dat kader met financiële dienstverleners en verzekeraars in 2013-2014 uitgevoerd zijn. Toen we in mei 2015 een CEO-ronde tafel organiseerden om een select aantal bedrijven en organisaties te interesseren voor deelname aan het onderzoek, was het een groot voordeel dat we al enkele private partijen konden laten vertellen welke inzichten zij bij het eerste FinPro big-dataexperiment in Delfshaven hadden opgedaan.



## Cyclus voor samenhang tussen Microdata en Big Data analyse



Ook het feit dat het OM kon uitleggen onder welke juridische voorwaarden dit onderzoek zou plaatsvinden, hoe de privacy gewaarborgd werd en dat er met de resultaten uit de dataruns geen strafrechtelijk onderzoek zou gaan plaatsvinden, werd als geruststellend gezien. Grotere organisaties zijn zich bewust van de privacywetgeving. Zij willen gegarandeerd hebben dat zij door deelname aan het experiment zich niet op glad ijs gaan bewegen. Door de big-dataexperts werd op de CEO-bijeenkomst, en later ook met de ICT- en juridische medewerkers op locatie in de betrokken bedrijven, toegelicht hoe er met encrypted informatie gewerkt wordt, dat de informatie op persoonsniveau geanonimiseerd wordt en dat het onderzoek niet gericht is op het zoeken naar verdachte personen, maar op het ontdekken van (afwijkende) patronen uit geaggregeerde data die verband kunnen houden met verdachte financiële activiteiten.

Het ging in alle runs bij de bedrijven om offline historische data van mensen die reeds strafrechtelijk vervolgd zijn. Deze data, afkomstig uit Veiligheidshuis en RIEC, fungeren als een soort teaser om in combinatie met data uit bedrijven en organisaties patronen op het spoor te komen. De data van de deelnemende bedrijven en organisaties mogen in dit experiment niet onderling gekoppeld worden, noch komen zij het bedrijf uit. Daarom zijn de big-dataruns door ons ter plekke, in elk bedrijf afzonderlijk uitgevoerd. Vaak zijn daarbij, naast de ICT-deskundigen uit het bedrijf, ook personen van de juridische afdeling aanwezig geweest. Na afloop is er telkens een debriefing in het bedrijf of de organisatie geweest om de voornaamste bevindingen met elkaar te

delen. Hierbij kwam vaak naar voren dat de bedrijven zich niet bewust waren van onzichtbare onveiligheid.

### Uitkomsten van het publiek-private big data experiment

Uit de afzonderlijke data-onderzoeken bij publieke organisaties en private bedrijven in Rotterdam zijn ongebruikelijke patronen naar voren gekomen. Hoge aantallen ingeschreven volwassen bewoners op woningen van beperkte omvang zijn opmerkelijk. Dat geldt ook voor het voorkomen van meerdere huurcontracten op één naam, met name als die persoon er niet zelf woont en het ook geen instelling is. Het lijkt op onzichtbare brievenbusfirma's voor diegenen die een adres nodig hebben, maar onder de radar blijven.

Net zo bevreesd de grote hoeveelheid bij de KvK opgegeven locaties voor kinderopvang, omdat die niet in die omvang te zien zijn in het straatbeeld. Wel kunnen hiermee legaal dan wel illegaal verkregen toelagen voor kinderopvang gestald worden.

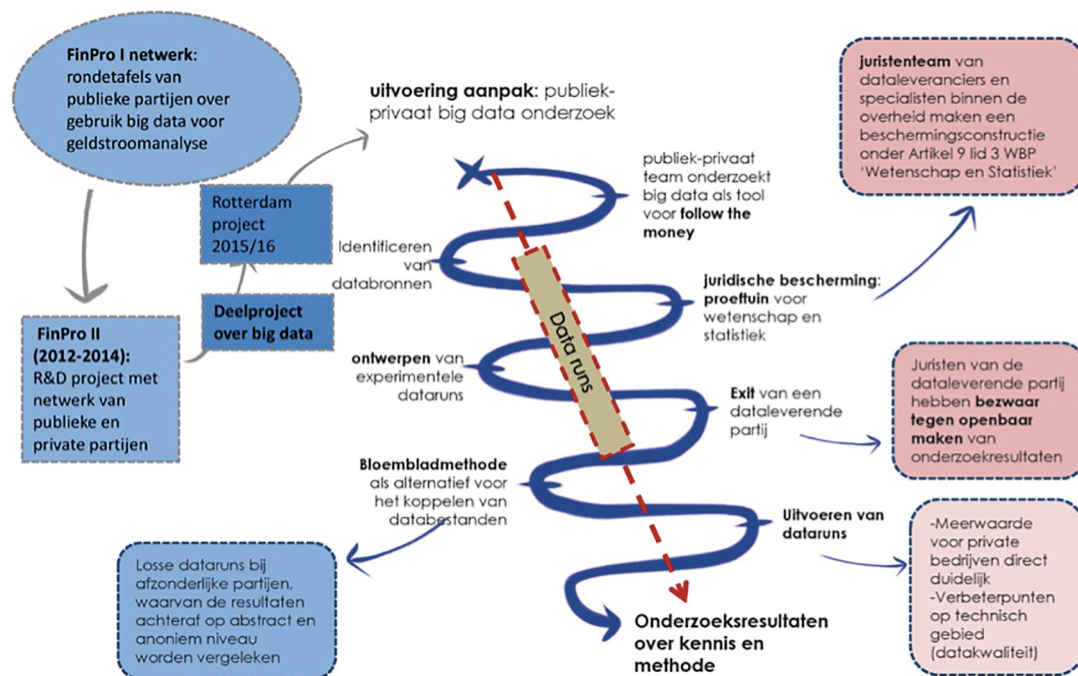
De ongebruikelijke declaraties voor complexe zorgbehandelingen bij een zorgverzekeraar kwamen eveneens weer naar boven. Bij verzekeraars laten de dataruns een veelvoorkomend claimgedrag zien om allerlei soorten schade te melden die net onder de limiet blijven. Doordat er silo's zijn binnen de systemen van de verzekeraars, valt het niet op, behalve wanneer je er met slimme software doorheen kunt kijken.

We vonden een concentratie van hits van ingeschreven studenten bij opleidingen met een lage toegangdrempel. Inschrijving houdt in dat je studeert en dat je studiefinanciering ontvangt. Van de experts uit het onderwijs hoorden we dat juist op deze opleidingen de uitval groot is en dat men zich een tijdje later eenvoudig weer bij een andere laagdrempelige opleiding inschrijft. De silo's in de onderwijsorganisaties geven daar geen zicht op. Die hebben bovendien ook financieel baat bij veel inschrijvingen.

We vonden ook reisbureaus die zelf tickets voor slechts twee bestemmingen uitgaven (Suriname en India), maar uit het onderzoek bleek dat op die tickets nooit loyalty-punten zijn afgegeven. Dat kan erop duiden dat de reizigers niet deelnemen aan loyalty-programma's. Of dat er nooit op de tickets gevlogen wordt, want alleen bij het inchecken kunnen de punten verkregen worden. Is dit een vorm van wit-

» *Er ontstaat een sfeer van normaliteit dat de overheid en bedrijven als flappentap dienen*

## Roadmap van het FinPro Big Data experiment



wassen? Wij hebben het opmerkelijke gegeven slechts met data- en businessintelligencesdeskundigen geconstateerd.

Het interessante van de teaser is dat de gevonden patronen uit de dataruns zich concentreren rondom geanonimiseerde personen in een beperkt aantal postcodegebieden. De vraag of de uitkomsten gerelateerd zijn of niet, kan niet onomstotelijk vastgesteld worden, omdat het big-dataonderzoek met encrypted, geanonimiseerde data van personen uitgevoerd is en er uitgebreide privacyvoorwaarden in acht genomen moesten worden. Ook mochten er geen koppelingen van bestanden tussen de verschillende dataruns van de private en publieke partijen gemaakt worden. De gevonden data en patronen moesten na afloop van de dataruns op de locatie door de betrokken private en publieke partijen direct vernietigd worden.

### Lessen trekken

Welke lessen trekken we uit dit maatschappelijk verantwoordigde big-dataonderzoek naar onzichtbare onveiligheid? Misschien is de eerste les wel dat een dergelijk onderzoek met publieke en private partijen niet eenvoudig is en zeer tijdrovend, en dat er ook veel tijd in de relatie met de betrokken partijen gestopt moet worden om het vertrouwen te krijgen. Aanvankelijk zat niemand echt te popelen om het onderzoek te doen. Na de runs zijn de ogen open gegaan en zijn veel partijen zelf actief data-analyses gaan plegen.

De tweede les is dat dergelijk onderzoek niet betekent dat je met een druk op de knop allerlei spannende patronen ziet. Er is sprake van veel vervuilde data, zowel uit het RIEC en het Veiligheidshuis en bij overheden in het algemeen. Bij bedrijven treffen we vooral silo's aan in de vorm van aparte bedrijfs-onderdelen die vaak ieder weer een eigen datasysteem hebben. Onderlinge communicatie is dan lastig, maar met slimme software en algoritmen komen er toch afwijkingen naar boven.

De derde les is dat er in zwakke economische gebieden veel meer aan de hand is, en dat er op allerlei manieren wegen bewandeld worden om oneigenlijk gebruik te maken van financiële geldstromen van publieke en private partijen, vaak zonder dat die partijen dat zelf doorhebben. Er ontstaat daardoor een sfeer van normaliteit dat de overheid of gemeente, maar net zo goed de zorgverzekeraar, als flappentap gebruikt kan worden. Zolang dat gedrag onder de radar blijft, gaat het door.

Het onderzoek legde de silo's bloot in de publieke en private sector. Het bleek dat, ondanks de grote financiële verliesposities die we op het spoor kwamen, de betrokken partijen zich er niet of nauwelijks van bewust waren. In veel opzichten is het doen van dit onderzoek een eyeopener geweest voor bedrijven en gemeentelijke organisaties om onzichtbare onveiligheid serieus te nemen. Inmiddels is er door het Verbond van Verzekeraars afgekondigd dat fraudes beboet gaan worden en dat er meer data-analyse gepleegd kan worden.

### Vervolg

Met de verschijning van het artikel met resultaten van ons meerjarig onderzoek in *het Financieel Dagblad* op 9 mei 2016 is de grote vraag: hoe nu verder? Vooral binnen de overheid is er behoefte om er meer mee te gaan doen. Onzichtbare onveiligheid is op het netvlies gekomen. De meerwaarde van experimenteel, juridisch verantwoord big-dataonderzoek en het ontsluiten van collectieve intelligentie is door de minister van Veiligheid en Justitie positief ontvangen en ook vanuit Binnenlandse Zaken (ICTU) en Financiën is er vraag naar hoe met de inzichten ook andere onderwerpen prospectief onderzocht kunnen worden.

Wil je echt verder kunnen gaan met big-dataonderzoek, dan zullen de uiterst beschermende condities waaronder wij het onderzoek gedaan hebben, wel iets verruimd moeten worden. Het is daarom goed dat er ook door de WRR in het rapport over big data dat in het voorjaar van 2016 is verschenen, een verruiming van de kaderwet geopperd wordt. De technische ontwikkelingen gaan snel, en computersoftware kan patronen uit koppelingen van data laten komen. Wanneer het gaat om maatschappelijke vraagstukken zoals ondermijning, financiële fraudes en onveiligheid, dan biedt big-data-onderzoek als methode het perspectief om meer te zien dan alleen met conventionele opsporing. De combinatie kan tot een veel gerichtere inzet van kennis en middelen zorgen met een groter effect op de veiligheid in de samenleving. <<

*Er is een boek over FinPro in de maak.*

### Noot

1 Ik dank het Openbaar Ministerie en in het bijzonder Marc van Nimwegen, Vincent Leenders en Marianne Bloos voor hun meerjarige commitment om het experimentele FinPro-onderzoek tot een succes te maken.