Grip op data

Green paper Big Data

VERBOND VAN VERZEKERAARS

Inhoud

“De black box met Big Data wordt groter en zwarter. De data die de box in gaat wordt complexer en de besluiten op basis van de black box belangrijker. Zowel bestuurders als consumenten moeten de inhoud van de black box kunnen vertrouwen. Het is goed dat het Verbond van Verzekeraars zich daar middels dit discussiepaper voor inzet.”

Prof. dr. Sander Klous, Hoogleraar Big Data Ecosystemen aan de Universiteit van Amsterdam en Managing Director Big Data Analytics bij KPMG.

1 Samenvatting

1.1 Big Data komt op ons af

Verzekeraars[1] verzamelen dagelijks en al jarenlang data van hun klanten om risico's in te kunnen schatten. Het is de basis van verzekeren. Maar die basis is aan flinke verandering onderhevig: de hoeveelheid data neemt razendsnel toe en er komen snel betere technieken om daar verbanden in te vinden. We kunnen spreken over Big Data. Vraag is wat dat voor klanten van verzekeraars betekent. Het optimisme over Big Data is groot, maar 'de revolutie' roept ook maatschappelijke vragen op. Worden klanten beter bediend door Big Data of kleven er ook risico's aan? En welke dan? Met dit green paper wil het Verbond bijdragen aan het antwoord op deze vragen en de discussie over Big Data een stap verder helpen. Het doel: een maatschappij en klanten die optimaal de vruchten kunnen plukken van Big Data en verzekeraars die kunnen werken aan een sterke sector die is voorbereid op de toekomst.

1.2 Kansen en zorgen

Big Data biedt flink wat kansen voor de maatschappij. Denk aan producten die beter aansluiten bij de wensen van de klant, snellere schadebehandeling en meer preventie-mogelijkheden. Maar die kansen kunnen alleen goed worden verzilverd als er voldoende oog is voor de zorgen. Want die zijn er ook. Zo brengt Big Data privacyrisico's met zich mee: wat gebeurt er met al die persoonlijke gegevens? Wat als we weten dat iemand een groter risico loopt dan de rest? Kan iemand zich dan nog wel verzekeren? En wat betekent die kennis over risico's voor het verzekeringsmodel? Als alleen mensen die veel risico lopen zich nog maar verzekeren (anders is het toch niet nodig) dan worden de premies torenhoog.

Hoewel deze 'zorgen' terecht zijn, is niet gezegd dat ze ook realiteit worden. Het moet geen reden zijn om Big Data terzijde te leggen. Wel duidelijk is dat we Big Data verantwoord moeten gebruiken, met oog voor de mogelijke risico's. Mochten risico's zich daadwerkelijk voordoen, dan kan effectief en gericht ingegrepen worden.

"Het doel: klanten die optimaal de vruchten kunnen plukken van Big Data en verzekeraars die kunnen werken aan een sterke sector die is voorbereid op de toekomst"

1.3 Checks and balances

Om maximaal voordeel uit de data te halen voor zowel maatschappij, klant als verzekeraar moeten we er verantwoord mee omgaan. Daarom wil het Verbond de komende jaren in de frontlinie meedenken over de ontwikkelingen. Met dit green paper zetten we daarin een eerste stap. Hierin stellen we een aantal *checks and balances* voor, die ervoor moeten zorgen dat klanten meer grip hebben op de data. Zo zal het Verbond maatregelen nemen om in de branche het bewustzijn van privacy verder te vergroten en verzekeraars te helpen om het bewustzijn te vertalen naar daden, bijvoorbeeld door onderzoek te doen naar effectievere privacystatements. Vervolgens wil het Verbond monitoren of de segmentatie tussen klantgroepen die Big Data mogelijk maakt, leidt tot uitsluiting van groepen. Daarvoor introduceren we een jaarlijkse Solidariteitsmonitor. Tot slot wil het Verbond maatregelen nemen om ervoor te zorgen dat de branche optimaal kan inzetten op Big Data en zo kan werken aan een bedrijfstak die ook in de toekomst gezond blijft. Dat het bedrijfsmodel mee verandert met de ontwikkelingen in de maatschappij spreekt daarbij voor zich. Hiertoe doet het Verbond de suggestie aan toezichthouders en wetgevers om terughoudend te zijn met nieuwe wetgeving,

[1] Dit paper is niet van toepassing op zorgverzekeraars aangezien deze van een gehele andere aard zijn en ook een andere manier van omgaan met data kennen.

bovenop de aanstaande Europese privacy verordening.

Naast deze concrete waarborgen, spant het Verbond zich er ook voor in om de dialoog over gegevensverbruik te voeren. Dat is niet eenvoudig: discussies over datagebruik gaan al snel over in zwart/wit-stellingnames. Wens is dat dit paper bijdraagt aan wat meer helderheid in de discussie. Het Verbond roept zijn leden ook op het gesprek hierover te blijven voeren. Daarnaast is het Verbond nauw betrokken bij de *High Level Expert Group Big Data* van het ministerie van Economische Zaken. Ook voor de totstandkoming van dit paper is met veel externe partijen gesproken, waaronder de Autoriteit Persoonsgegevens, TomTom, TNO, het Rathenau Instituut, Bits of Freedom, diverse universiteiten en ministeries. Hoewel geprobeerd is zoveel mogelijk recht te doen aan deze verschillende perspectieven, is hiermee niet gezegd dat deze partijen het paper ondersteunen.

Big Data

Er zijn diverse definities van Big Data. Een veelgebruikte gaat uit van drie V's: volume (hoeveelheid), variety (diverse bronnen) en velocity (snelheid waarmee data gegenereerd en geanalyseerd wordt). Andere definities combineren twee assen: interne/externe data en gestructureerde/ongestructureerde data. Hoewel de definities variëren en er ook vele varianten zijn voor de term Big Data, gaat het samenvattend over de toename van de hoeveelheid data en de toename van de mogelijkheden om verbanden tussen al die data te vinden. Dat levert nieuw soort informatie op waar zowel bedrijven, overheden als consumenten iets mee kunnen. Lees in hoofdstuk 4 meer over Big Data.

Het Verbond zal:

- een klankbordgroep Big Data oprichten, die de opzet en werking van deze waarborgen zal invullen en toetsen;
- jaarlijks een Solidariteitsmonitor uitvoeren;
- onderzoek doen naar het precieze onderscheid tussen discriminatie en premiedifferentiatie op grond van risico;
- onderzoek doen naar privacy by design;
- in de update van de Gedragscode Verwerking Persoonsgegevens bijzonder aandacht schenken aan effectievere privacystatements;
- in zijn onderwijs en opleidingswerk rekening houden met een kennisbehoefte omtrent data;
- het principe dat de klant in controle is over eigen data, verder uitwerken in toekomstige dossiers;
- bij toekomstige wetgeving opletten of datamonopolies ontstaan.

Het Verbond adviseert zijn leden om:

- Privacy Impact Analyses's te gebruiken waar nodig;
- waar mogelijk anonieme Big Data-toepassingen in te zetten;
- bij het aanbrengen van onderscheid tussen groepen klanten goed op te letten dat er geen onbedoelde discriminatie plaatsvindt en ernaar te streven dat ook mensen met een groter risico een verzekering kunnen aanschaffen tegen een betaalbare premie;
- bij gebruik van *observed data* klanten goed te informeren en in de gelegenheid te stellen eventuele fouten te corrigeren;
- verkregen data goed te beschermen;
- open te communiceren over gebruik van Big Data en dialoog aan te gaan met klanten en stakeholders;
- een communicatietoets te hanteren: is het resultaat van de Big Data. analyse nog uit te leggen?

2 Inleiding

Verzekeraars gebruiken sinds jaar en dag data om risico's van hun klanten goed te kunnen inschatten. Maar met recente nieuwe technieken, die elkaar steeds sneller opvolgen, worden de mogelijkheden steeds groter. Daar zoomen we in dit paper op in. Hoe kunnen verzekeraars daar op in spelen? En vooral: wat betekent dat voor de klant? Het paper verkent de grote krachten die de Big Data-revolutie heeft losgemaakt en de kansen en zorgen die deze voor klanten en verzekeraars brengt. Daarbij is het belangrijk om in het achterhoofd te houden dat Nederlandse verzekeraars nog maar in beperkte mate gebruikmaken van Big Data-analyses, zeker vergeleken met bijvoorbeeld het Verenigd Koninkrijk en de Verenigde Staten. De ontwikkelingen op dit vlak gaan echter razendsnel. Dit paper is dus een eerste stap, maar afhankelijk van de ontwikkelingen en de maatschappelijke reacties, kunnen inzichten veranderen. Het Verbond zal nieuwe ontwikkelingen en discussies op dit vlak op de voet volgen, aanjagen en daarbij waar mogelijk stelling nemen.

3 Verzekeraars en data: business as usual

'Data' betekent volgens de Dikke van Dale: *1. gegevens; feiten; 2. voorstellingen van feiten die in de informatietechniek verwerkt kunnen worden.* Essentieel voor verzekeraars. Zij leggen elke dag veel gegevens en feiten vast om hun kerntaak te kunnen uitvoeren: risico's inschatten en het contract uitvoeren. Dat is nu zo, maar dat was vijftig jaar geleden ook al zo. Twee voorbeelden:

1. Een autoverzekeraar vraagt in zijn acceptatieproces eerst naar het kenteken. Op grond daarvan kan de verzekeraar bij de Rijksdienst voor het Wegverkeer enkele basale kenmerken van de te verzekeren auto ophalen: merk, model, type, bouwjaar, brandstof. Dat scheelt de klant wat invulwerk en voorziet de verzekeraar van correcte gegevens. Vervolgens vraagt de verzekeraar aan de klant in te schatten hoeveel kilometer hij per jaar rijdt. Verder is de leeftijd van de bestuurder van belang, diens postcode en het aantal schadevrije jaren. Op grond van deze gegevens schat een verzekeraar in welke premie gerekend moet worden, zodat een offerte afgegeven kan worden. Voor de uitvoering van het contract zijn er nog wat aanvullende gegevens nodig, zoals de volledige naam van de verzekerde en diens contactgegevens. Op grond hiervan controleert een verzekeraar of de aspirant-verzekerde eerder betrokken is geweest bij een frauduleuze claim.

"Data zijn essentieel voor verzekeraars. Dat is nu zo, maar dat was vijftig jaar geleden ook al zo."

2. Een overlijdensrisicoverzekering (ORV) is vaak verplicht als iemand een hypotheek wil afsluiten. Als degene die de hypotheeklasten betaalt overlijdt, dan kan met de uitkering van de verzekering de hypotheekschuld deels of helemaal afgelost worden. Om de premie van zo'n ORV te kunnen berekenen, vraagt de verzekeraar naar de geboortedatum van de kandidaat-verzekerde(n), de hoogte van het verzekerde bedrag, hoe lang de verzekering moet lopen en eventueel of de te verzekeren personen wel of niet roken. Op basis van deze gegevens kan de verzekeraar de premie vaststellen en een offerte uitbrengen. Als de consument vervolgens de verzekering wil afsluiten, start het feitelijke aanvraagproces. Bij dat aanvraagproces speelt ook de gezondheid van de kandidaat-verzekerde een rol. De gezondheid wordt vastgesteld aan de hand van een gezondheidsverklaring die de te verzekeren persoon naar waarheid in moet vullen. Op basis van de gegeven antwoorden stelt de verzekeraar de definitieve premie vast. Als de gezondheid aanleiding geeft om een andere premie in rekening te brengen dan in de offerte was vermeld, krijgt de consument daarvoor een voorstel. Voor hogere kapitalen

kan zelfs een medische keuring van de te verzekeren persoon vereist zijn. Voor de uitvoering van het contract zijn nog aanvullende gegevens nodig, zoals de volledige naam en het geslacht van de verzekeringnemer (de premiebetaler), zijn adresgegevens en de volledige naam van de te verzekeren persoon.

3.1 Waarom verzamelen verzekeraars data?

Een verzekering kan niet afgegeven worden zonder data over de klant en/of het te verzekeren object. Een verzekeraar moet immers inschatten hoe groot de kans op schade is en dus hoeveel premie er nodig is om in geval van schade te kunnen uitkeren. Het is echter niet zo dat er een recht evenredig verband is tussen de hoeveelheid data en de mate waarin de verzekeraar de schadekans kan inschatten. Op grond van de data uit het voorbeeld van de autoverzekering kan de motorrijtuigen-verzekeraar namelijk al behoorlijk precies inschatten hoe groot de schadekans is. Aanvullende data over bijvoorbeeld de onderhoudshistorie van de auto, maken die inschatting niet per se beter. Dat komt door de ervaring die verzekeraars door de jaren heen hebben opgebouwd en door de wet van de grote getallen (zie kader). Verzekeraars weten op grond van deze beperkte dataset dat van alle klanten met bepaalde kenmerken, er in het komende jaar x mensen schades van y euro zullen hebben.

De wet van de grote getallen

De wet van de grote getallen vormt een belangrijk fundament onder het fenomeen verzekeren. Verzekeraars schatten van hun klanten op grond van een beperkte hoeveelheid data de kans op schade. Vervolgens brengen zij een groep klanten bij elkaar met een voldoende gelijk risicoprofiel. Als klant x dan eerder (of juist later) overlijdt dan geschat, wordt dat gecompenseerd door een ander die langer (of juist korter) leeft (en dus langer premie betaalt). Zo creëert of faciliteert de verzekeraar solidariteit.

Bij het verzamelen van de benodigde data leggen verzekeraars overigens ook data vast om te voldoen aan allerlei (internationale) wetgeving. Zo moeten verzekeraars potentiële klanten uitvoerig identificeren om te voorkomen dat criminelen met levensverzekeringen geld witwassen. En na de acceptatie moeten bepaalde polissen of klanten gemonitord worden om witwassen en terrorismefinanciering te voorkomen. In geval van verdachte transacties moet dit gemeld worden bij nationale toezichthouders.

3.2 Welke data?

Kunnen we zeggen dat verzekeraars anno 2016 over veel data beschikken? Ja en nee. De grootste verzekeraars in Nederland hebben miljoenen klanten. Omdat van elke klant wel gegevens worden vastgelegd, beschikken verzekeraars over veel data, maar vergeleken met internetbedrijven, zoals zoekmachines of sociale media, beschikken verzekeraars niet over veel data. Verzekeraars hebben gegevens over de identiteit van een klant (naam, adres en woonplaats) en informatie over het verzekerde risico (de woning, de auto en misschien de leefstijl), maar dat is niets vergeleken bij wat bijvoorbeeld een social media-bedrijf van klanten weet. Dit verschil wordt ook duidelijk als we kijken naar de bron van data. Data zijn volgens het World Economic Forum *volunteered*, *observed* of *inferred*[2]. In het Nederlands: data zijn door het datasubject (de klant) zelf geleverd, het komt uit observatie (wellicht zonder dat de klant dit door had!) of het komt door analyse van patronen. Verzekeraars beschikken veelal over *volunteered* of *inferred data*. Dat betekent dat klanten van verzekeraars vaak zelf wel inzicht hebben in wat de verzekeraar van hen weet.

Alleen door de wet van de grote getallen toe te passen, kunnen verzekeraars analyseren hoe groot het risico van de individuele klant

[2]http://www3.weforum.org/docs/WEF_IT_RethinkingPersonalData_Report_2012.pdf

waarschijnlijk is. Het gaat dus om patronen; de *inferred data*. We zullen later in dit green paper zien dat verzekeraars met de komst van Big Data de overstap zouden kunnen maken naar de (voor hen nieuwe) categorie van *observed data*.

Overigens kopen verzekeraars net als veel andere bedrijven ook allerlei anonieme geaggregeerde data in, en gebruiken zij informatie van Centraal Bureau voor de Statistiek (CBS). Denk aan criminaliteits-informatie, woningwaarde of gezins-samenstelling op bijvoorbeeld gemeente- of wijkniveau. Dit stelt verzekeraars in staat hun producten beter af te stemmen op de wensen van de klant.

4 Big Data

Data is dus niets nieuws voor verzekeraars. Waarom dan nu een apart paper over het onderwerp? Dat komt omdat er iets bijzonders aan de hand is met het fenomeen data, en dan vooral met de snelheid van die ontwikkeling. Ongeveer negentig procent van alle data in de wereld is in de afgelopen twee jaar tot stand gekomen, aldus IBM[3]. Deze snelle toename wordt veroorzaakt door het internet en de apparaten die daar gebruik van maken. Computers worden steeds kleiner en sneller. Ook het vermogen om data op te slaan, is door diverse uitvindingen enorm toegenomen. In 1990 kostte de opslag van één gigabyte data nog ongeveer tienduizend dollar, in 2000 ongeveer tien dollar en tegenwoordig kost dat nog maar enkele centen[4]. Elke minuut wordt er nu meer dan honderd uur video aan YouTube toegevoegd. Vanaf 2014 werd er in appstores jaarlijks meer geld uitgegeven, dan Hollywood verdient aan films[5]. Vergeet niet dat er voor 2008 nog helemaal geen appstores waren.

Doordat de kosten van apparatuur en opslag zo snel zijn afgenomen, wordt het mogelijk om in allerlei processen en objecten sensoren toe te passen. Er zijn al sensoren die op de waterleiding in een huis geplaatst kunnen worden, om te meten of er plotselinge drukverlaging is, wat kan wijzen op een lek. Een signaaltje naar een klep kan er vervolgens voor zorgen dat het water naar de hoofdkraan afgesloten wordt. Dat scheelt veel geld. Dit is een voorbeeld van het Internet of Things (IoT) en dit zal de groei van data alleen nog maar vergroten: lampen die automatisch aangaan na een bepaald tijdstip, of als de eigenaar via een app een seintje geeft, garagedeuren die opengaan als de auto van de eigenaar de straat in rijdt, koelkasten die rottend voedsel bespeuren, noem maar op.

Door die toename spreekt men over ‘Big Data’[6]. Ook het vermogen om in die enorme berg data verbanden te vinden, neemt snel toe. Dit creëert nieuwe kansen voor mensen en bedrijven die zinvolle patronen kunnen ontdekken in die Big Data. Zo kan nu beter dan ooit creditcardfraude gedetecteerd worden, omdat creditcard-maatschappijen *real time* zien wat er gebeurt met een kaart en het systeem direct merkt wanneer een kaart op een afwijkende manier gebruikt wordt. Bij zo’n afwijking wordt contact opgenomen met de klant om te zien of er misschien een probleem is.

Dit soort voorbeelden zijn er op allerlei terreinen. Stormen en overstromingen kunnen beter voorspeld worden. De politie kan zien waar de kans op criminaliteit of ordeverstoring groot is, zodat politieagenten daar kunnen worden ingezet. Consumenten krijgen producten die beter aan hun wensen voldoen. Pieken in de vraag naar producten en diensten kunnen beter worden ingeschat, waardoor klanten beter bediend kunnen worden. Allemaal goed nieuws. Ook voor verzekeraars; die kunnen met Big Data namelijk beter risico’s

[3] http://www-01.ibm.com/software/data/bigdata/what-is-big-data.html
[4] http://www.mkomo.com/cost-per-gigabyte-update
[5] http://www.asymco.com/2015/01/22/bigger-than-hollywood/

[6] Er zijn diverse definities van Big Data. Een veelgebruikte gaat uit van drie V’s: volume (hoeveelheid), variety (diverse bronnen) en velocity (snelheid waarmee data gegenereerd en geanalyseerd wordt). Andere definities combineren twee assen: interne/externe data & gestructureerde/ongestructureerde data.

inschatten. Tegelijkertijd zijn er zorgen. Zorgen die zich vooral richten op grote thema's als privacy en solidariteit. Deze zorgen verdienen serieuze aandacht. Zonder een goed antwoord op deze zorgen zal er weinig maatschappelijk draagvlak zijn voor Big Data-toepassingen.

5 Big Data: de kansen

Met de combinatie van een grote hoeveelheid data én het vermogen daar zinvolle verbanden in te vinden, ontstaat er dus ook voor klanten en verzekeraars een hele nieuwe wereld. Inclusief kansen.

Big Data en autoverzekeringen
Auto's veranderen langzaam maar zeker in computers op wielen. Een moderne auto kan eenvoudig uitgerust worden met een extra chip die gegevens over het rijgedrag (zoals remmen, noodstops, optrekken en scherpe bochten) verzamelt en verstuurt naar een derde. Er zijn, onder andere in de VS en het VK, al enige jaren verzekeraars die hun klanten deze mogelijkheid bieden. Die gebruiken de gegevens over het rijgedrag om te bepalen hoe veilig het rijgedrag is. Per verzekerde leidt dit tot een veiligheidsscore die vertaald wordt naar een korting op de basispremie. De klant ziet dus in zijn of haar premie hoe veilig hij of zij rijdt in vergelijking met de andere verzekerden, eventueel aangevuld met een dashboard met aanvullende informatie over het rijgedrag. Het doel hiervan is dat alle verzekerden gestimuleerd worden om nog veiliger te rijden, zodat de premies omlaag kunnen. De klant krijgt een premie, die mede gebaseerd is op zijn of haar rijgedrag.

Hieronder sommen we een aantal kansen van Big Data voor klanten op. Dat iets *kan*, betekent niet dat het ook *moet*. Allereerst zullen verzekeraars in het concrete geval zorgvuldig kansen en zorgen moeten afwegen. Daarna is het aan de klant, die er al dan niet voor kiest gebruik te maken van producten of diensten waar aanvullende data voor nodig zijn.

1. **Snellere schadebehandeling.** Een auto die is uitgerust met een chip die het rijgedrag bijhoudt, kan bij een botsing gelijk een seintje geven naar de verzekeraar die vervolgens het schadebehandelingsproces snel kan opstarten. De klant hoeft dan op het moment van schade niet op zoek naar een schadeaangifteformulier, maar krijgt van de verzekeraar direct een telefoontje met de vraag of hulp welkom is.

2. **Dienstverlening die nóg klantgerichter is.** Met Big Data kunnen verzekeraars de wensen van hun klanten nóg beter begrijpen en klantgerichter meedenken. Stel dat een klant een reisverzekering met werelddekking heeft, maar uit data blijkt dat hij nooit buiten Europa op vakantie gaat, dan kan de verzekeraar de klant adviseren een beperktere dekking te overwegen. Op korte termijn is dat wellicht inkomstenderving vanuit het perspectief van de verzekeraar, maar op de langere termijn kan het resulteren in een hogere klanttevredenheid. Op grond van Big Data-analyses kunnen bedrijven hun online klanten ook beter begeleiden naar de informatie: voorwaarden, opzegmogelijkheden, een telefoonnummer.

3. **Meer veiligheid op straat.** Uit de verzamelde data van alle verzekerden, kunnen verzekeraars verbanden vinden die helpen bij het oplossen van maatschappelijke vraagstukken. Zo kan met data van alle verzekerden onderzoek worden gedaan naar de relatie tussen veiligheid en straatverlichting of tussen wateroverlast en de staat van de riolering. Zo wordt met behulp van data een veiligere buurt gecreëerd. Dat is winst voor de maatschappij, de klant en de verzekeraar.

4. **Voorkomen in plaats van genezen.** Op grond van klantdata, eventueel in combinatie met externe data, kunnen klanten geholpen worden om risico's te voorkomen. Voorkomen is beter dan genezen, niet alleen voor de klant, maar ook voor de verzekeraar (minder schade). In geval van een inbraak zal de verzekering de financiële schade afdekken, maar de

emotionele waarde van spullen wordt niet gecompenseerd. Met behulp van Big Data, inbraakpatronen of kenmerken van de woning, kan de verzekeraar gericht advies geven om de woning te beveiligen. Hoe specifieker zo'n advies, hoe beter een klant daarmee uit de voeten kan.

5. Premies afgestemd op de klant. Big Data-analyses kunnen ook gebruikt worden om van klanten een op maat gesneden premie te vragen. Veel klanten die veilig rijden willen liever niet betalen voor medeverzekerden die onveilig rijden. Als klanten de verzekeraar inzicht geven in hun gedrag, kan een verzekeraar daar ook rekening mee houden. Andersom kan dit principe een prikkel bieden om gezonder, veiliger en bewuster te leven. Want: leef je onveiliger of ongezonder, dan betaal je meer. Dat vereist ook heldere acceptatierichtlijnen en polisvoorwaarden.

6. Betere verzekerbaarheid. Data geeft inzicht. En biedt daardoor ook mogelijkheden. In het verleden was het voor verzekeraars bijvoorbeeld niet mogelijk om mensen die besmet waren met HIV een levensverzekering te bieden. Er was onvoldoende bekend over de levensverwachting van deze mensen om een zinnige risicoberekening te kunnen maken. Met het beschikbaar komen van meer data, werd het mogelijk om ook voor deze risico's een verzekeringsmogelijkheid te creëren. Met Big Data kan dat mogelijk voor meer groepen het geval zijn. Zonder data is verzekeren vaak heel moeilijk, meer data kan dus ook tot meer verzekerbaarheid leiden.

7. Het voorkomen van fraude. Fraude met verzekeringen kost jaarlijks honderden miljoenen euro's. Fraude is niets anders dan diefstal van de medeverzekerden: een deel van de premies wordt niet gebruikt voor schade-uitkeringen, maar voor de frauduleuze claims. Big Data-analyses kunnen helpen deze claims op te sporen. Zo kunnen de analyses helpen een betere inschatting te maken welke claims mogelijk frauduleus zijn. Daar kan de verzekeraar dan een gericht onderzoek op zetten zodat meer fraude opgespoord kan worden. Hier hebben goedwillende verzekerden, gelukkig nog altijd de grootste groep, natuurlijk baat bij.

"Als er voor klanten waarde zit in Big Data-toepassingen, zal er meer bereidheid zijn om data te delen."

Nogmaals: dit zijn mogelijkheden. In Nederland worden Big Data-toepassingen nog maar beperkt gebruikt. Behalve in de eigen bedrijfsvoering van verzekeraars, zien we het anno 2016 eigenlijk alleen nog maar in praktijk gebracht worden in de vorm van *pay how you drive*-autoverzekeringen, ook wel *Usage Based Insurance*. Verzekeraars zijn redelijk terughoudend met het gebruik van Big Data. Misschien wel doordat klanten sceptisch aankijken tegen het gebruik van hun data voor commerciële doeleinden, tenzij er een duidelijk voordeel voor hen te halen valt. Er moet dus elke keer zorgvuldig afgewogen worden of er wel draagvlak voor is. Het vertrekpunt voor dat draagvlak is *shared value*: als er voor klanten waarde zit in de Big Data-toepassing, zal er meer bereidheid zijn om data te delen. Het is dus helder dat verzekeraars hier ook verschillend mee om zullen gaan.

6 Big Data: de zorgen

Deze grote kansen kennen helaas een schaduwzijde: er zijn ook zorgen. Een belangrijke zorg richt zich op de privacy van klanten, het recht op bescherming van de persoonlijke levenssfeer. Een andere zorg is de mogelijke spanning tussen Big Data en solidariteit. Een verbijzondering daarvan is de mogelijkheid dat Big Data-gebruik leidt tot indirecte discriminatie. Tot slot is er een zorg die niet zozeer voor klanten, maar wel voor

verzekeraars van belang is. Big Data brengt ook zorgen mee ten aanzien van het model van verzekeraars. Hebben klanten straks nog wel een verzekeraar nodig? En als alleen klanten die veel risico lopen zich verzekeren, wordt de premie dan niet veel te hoog? Overigens zijn dit soort zorgen denkbaar, maar is het ook goed om voor ogen te houden dat nieuwe technieken soms angsten oproepen die later helemaal niet blijken te kloppen of die verreweg overschaduwd worden door de voordelen. Het internet an sich brengt bijvoorbeeld allerlei zorgen omtrent privacy met zich mee, maar de voordelen wegen duidelijk op tegen de nadelen. Daarbij zijn er manieren denkbaar om de nadelen te beperken: cookiewetgeving, firewalls, et cetera. De recente switch van een grote berichtenservice naar encrypted berichten, laat zien dat er behoefte is aan privacyvriendelijke diensten.

6.1 Privacy

Big Data gaat over gegevens van klanten. En daarmee hebben we het direct over privacy. Veel zorgen die dat oplevert worden geaddresseerd in wetgeving. Daarbij is de Wet Bescherming Persoonsgegevens de basis. In een artikel van de voorzitter van het Cbp (tegenwoordig Autoriteit Persoonsgegevens) wordt uitgelegd wat de kern is bij privacy*: De wettelijke privacyprincipes zijn bedoeld om ongebreidelde verzameling en gebruik van persoonsgegevens tegen te gaan: wees transparant over de data die je verzamelt en gebruikt (transparantie); gebruik data niet voor een ander doel dan waarvoor je deze hebt verzameld (doelbinding); gebruik niet meer data dan noodzakelijk voor het doel (data-minimalisatie)*[7]. Het Verbond wil met dit paper tegemoetkomen aan deze voornaamste bezwaren.

Kernbegrippen uit de Wbp

Onder verwerking van persoonsgegevens worden alle handelingen begrepen die met persoonsgegevens worden verricht. Het betreft het verzamelen tot en met het vernietigen van de persoonsgegevens, inclusief alle tussenliggende handelingen De belangrijkste voorwaarden voor een rechtmatige verwerking van persoonsgegevens zijn: (i) het vaststellen van de doeleinden van de verwerking en ‘verenigbaar gebruik’; (ii) het vaststellen van een grondslag voor de verwerking; en (iii) de informatieplicht die op de verantwoordelijke (dat is degene die het doeleinde van de verwerking en de wijze van verwerking bepaalt) rust. Hieronder een toelichting op de hoofdlijnen uit de Wbp.

Uitgangspunt
Uitgangspunt is dat persoonsgegevens in overeenstemming met de wet, op behoorlijke en zorgvuldige wijze worden verwerkt.

Doeleinden
Persoonsgegevens mogen slechts voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld. Het doel waarvoor de persoonsgegevens worden verzameld geldt als toetsingscriterium voor tal van andere bepalingen, zoals het verenigbaar gebruik, de bewaartermijnen en de voorwaarde dat niet meer persoonsgegevens mogen worden verzameld dan voor het doel noodzakelijk is.

Rechtmatige grondslag
De verwerking van persoonsgegevens moet gebaseerd zijn op één van de in de Wbp (artikel 8) genoemde grondslagen. Zonder geldige grondslag is de verwerking van persoonsgegevens niet toegestaan. Verzekeraars baseren de verwerking van persoonsgegevens met name op de grond dat de verwerking noodzakelijk is voor het sluiten en uitvoeren van een overeenkomst met de betrokkene (dat is degene wiens persoonsgegevens worden verwerkt), om te voldoen aan wettelijke verplichtingen of omdat de verwerking noodzakelijk is voor het gerechtvaardigde belang van de financiële instelling. Naast deze drie grondslagen verwerken financiële instellingen ook gegevens op grond van ondubbelzinnige toestemming van de betrokkene.

[7] https://www.ictmagazine.nl/columns/big-data-en-het-voorkomen-van-digitale-predestinatie/

Verenigbaar gebruik
Onder strikte voorwaarden mogen de gegevens later ook verder gebruikt worden voor andere doeleinden. Die andere doeleinden mogen niet onverenigbaar zijn met de doeleinden waarvoor de gegevens origineel verzameld zijn. Of er sprake is van verenigbaar gebruik hangt onder andere af van de verwantschap tussen de twee doeleinden, de aard van de gegevens (gevoelig of niet), de gevolgen van de verwerking voor de betrokkene en de mate waarin ten aanzien van de betrokkene is voorzien in passende waarborgen. Van geval tot geval moeten dus alle omstandigheden worden beoordeeld en gewogen om te kunnen vaststellen of een verdere gegevensverwerking geoorloofd is. In geval de betrokkene toestemming heeft gegeven voor de verdere verwerking, wordt in ieder geval voldaan aan het vereiste van verenigbaar gebruik.

Kwaliteit van de persoonsgegevens
De kwaliteit van persoonsgegevens omvat twee aspecten. Allereerst mogen niet meer of andere persoonsgegevens worden verwerkt dan noodzakelijk voor het doel van de verwerking. Daarnaast moet de verantwoordelijke die maatregelen treffen die redelijkerwijs nodig zijn om er voor te zorgen dat de persoonsgegevens juist en nauwkeurig zijn.

Bewaartermijn
Artikel 10 lid 1 van de Wbp stelt: *Persoonsgegevens mogen niet langer bewaard worden dan noodzakelijk is voor de verwerkelijking van de doeleinden waarvoor de gegevens zijn verzameld of vervolgens verwerkt*. De verantwoordelijke dient zich dus af te vragen of er redenen zijn op grond waarvan de persoonsgegevens vastgelegd kunnen blijven.

Beveiliging
De verantwoordelijke moet de persoonsgegevens op passende wijze beveiligen tegen verlies en tegen onrechtmatige verwerking. Daarbij moet onder andere rekening worden gehouden met de aard van de gegevens en de technische mogelijkheden.

Informatieplicht
De verantwoordelijke moet de betrokkene informeren over de doeleinden van de verwerking waar hij de persoonsgegevens voor gebruikt (tenzij de betrokkene daarvan al op de hoogte is).

Daardoor is de verantwoordelijke aanspreekbaar voor de betrokkene. Bij het aangaan van een relatie met een verzekeraar zal doorgaans uitdrukkelijk op het openings- c.q. aanvraagformulier worden aangegeven wat de doeleinden zijn waarvoor de persoonsgegevens worden verzameld.

Gedragscode
De hierboven beschreven uitgangspunten zijn, evenals de overige verplichtingen die voortvloeien uit de Wet Bescherming Persoonsgegevens, zijn voor verzekeraars nader uitgewerkt in de Gedragscode Verwerking Persoonsgegevens Financiële Instellingen (GVPFI). Deze gedragscode bevat tevens een uitgebreide toelichting. De leden van het Verbond van Verzekeraars zijn verplicht de GVPFI na te leven. Daar wordt op toegezien door de onafhankelijke Stichting Toetsing Verzekeraars.

In geval van Big Data is compliant zijn met wettelijke kaders echter niet genoeg. Dat komt omdat Big Data ook ethische vragen oproept, zoals de vraag in hoeverre verzekeraars moeten bepalen welk risicovol gedrag wel en niet tot een hogere premie leidt. Die zijn niet simpelweg te beantwoorden met een verwijzing naar de wet. Ook roept het gebruik van *observed data* extra zorgen op. Dat komt omdat klanten daar vaak weinig controle over hebben. Wellicht heeft een klant ooit een vinkje gezet, om gebruik te kunnen maken van een dienst, maar weet hij niet dat daarmee gegevens verzameld worden en wellicht zelfs worden gedeeld met derden. Dus bij *observed data* is het belangrijk om extra goed aan te geven wat er met die data gebeurt. Dat geeft klanten grip op data.

Dit wordt geregeld door cookiewetgeving als het gaat om observatie van online surfgedrag, maar waar het gaat om observatie van offline gedrag, moet dat even goed geregeld zijn.

In een brief van de minister van Economische Zaken aan de Tweede Kamer uit november 2014 wordt uiteengezet hoe de bestaande regels op Big Data-toepassingen slaan. Hoewel dit deels overlapt met de eerdere uitleg, halen we de brief van de minister hier toch wat uitvoeriger aan, omdat dit de eerste keer was dat er zo expliciet aandacht werd besteed aan het recht op gegevensbescherming en de Big Data-revolutie. In de brief staat dat de twee belangrijkste privacyprincipes voor Big Data *rechtmatigheid* van de verwerking en *informatieverstrekking* aan de klant zijn.

1. Rechtmatigheid. Persoonsgegevens mogen alleen in overeenstemming met de wet en op een behoorlijke en zorgvuldige manier worden verwerkt. Persoonsgegevens moeten voor welbepaalde, vooraf uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en vervolgens alleen verder worden verwerkt voor doeleinden die daarmee verenigbaar zijn. Dit is van belang bij de inzet van Big Data. Een verzekeraar mag data die verzameld worden voor bijvoorbeeld de autoverzekering dus niet zomaar gebruiken voor andere doeleinden. Stel dat uit die autodata blijkt dat een klant vaak naast de sportschool parkeert, dan mag een verzekeraar op grond daarvan niet zomaar een aanbieding voor een andere verzekering doen aan de klant. Dit geldt ook voor het delen van data: dat moet klanten vooraf verteld worden en zij moeten daarmee instemmen.

2. Informatieverstrekking. Degene van wie persoonsgegevens worden verwerkt (de betrokkene genoemd), moet ten minste op de hoogte zijn van de identiteit van de organisatie of persoon die deze persoonsgegevens verwerkt (de zogeheten verantwoordelijke). De betrokkene moet niet alleen geïnformeerd worden, maar heeft ook het recht op inzage in welke gegevens verwerkt worden, een recht op correctie of verwijdering als de gegevens onjuist zijn of niet ter zake doen en een recht van verzet (vooral tegen gebruik voor marketingdoeleinden). Dit is bestaande wetgeving die klanten grip op de data moet geven. De aanstaande Europese verordening zal aanvullend nieuwe en uitgebreidere rechten scheppen voor klanten, zoals het recht om niet te worden onderworpen aan automatische beslissingen.

De minister signaleert verder dat deze kaderstelling bescherming biedt tegen ongerechtvaardigde inbreuken op de privacy, maar stelt tegelijk dat er bij Big Data spanning is met deze principes: ‘spanning met het principe van rechtmatigheid, omdat het interessant en winstgevend is data voor een ander doel en context te gebruiken dan waarvoor ze zijn verzameld, ze langer vast te houden met oog op toekomstige analyses en zoveel mogelijk data te verwerken met oog op een betere analyse’. Toch ziet de minister wel mogelijkheden, mits bedrijven zorgvuldige afwegingen maken tussen hun gerechtvaardigde belang en het recht op privacy. Een *Privacy Impact Assessment* (PIA) kan hierbij helpen. Dat is een methode die organisaties dwingt om proactief na te denken over wat de impact is van het beoogde project voor de privacy van betrokkenen en wat de risico’s zijn voor betrokkenen en de eigen organisatie[8].

Het anonimiseren van klantdata kan hierbij ook behulpzaam zijn. Denk aan data die voor een bepaald contract verzameld zijn, maar waarvan het niet nodig is deze na afloop van het contract oneindig lang te bewaren. Die data moeten dan conform de wet vernietigd worden. Dat is jammer, omdat daarmee kennis verloren kan gaan. Anonimisering kan dan uitkomst bieden.

[8] Een veelgebruikt format voor een PIA is afkomstig van Norea, de organisatie voor IT-auditors: http://www.norea.nl/readfile.aspx?ContentID=82987&ObjectID=1265283&Type=1&File=0000042779_PIA%20versie%201.2%20def.pdf

"Tot nu toe worden verzekeraars vertrouwd. Het is belangrijk dat ze dit vertrouwen behouden."

Ook kan er spanning zijn met het principe van informatieverstrekking omdat het lastig is mensen te informeren over de vele ingewikkelde analyses en de hoeveelheid gegevens die daarbij gebruikt worden, zo stelt de minister in zijn brief. Dat is inderdaad lastig, interesse voor privacy is er vaak alleen als er iets misgaat. Recent onderzoek laat zien dat zelfs de best vormgegeven privacystatements niet gelezen worden en geen effect hebben op het gedrag van mensen[9]. Hier ligt dus een belangrijke uitdaging voor bedrijven om klanten te informeren en te interesseren voor die informatie. Ook het Verbond zal zich daar voor inzetten.

6.1.1 Privacy als betaalmiddel

Privacy is een grondrecht. En dus zou er geen verschil mogen zijn in premie of voorwaarden tussen mensen die wel of juist geen gegevens aan hun verzekeraar willen geven. Sommige mensen kijken daarom kritisch naar een *pay how you drive*-verzekering. Deze biedt verzekerden premiekorting in ruil voor gegevens over het rijgedrag. Criticasters zeggen dat privacy hier als betaalmiddel wordt gebruikt en beweren dat als deze ontwikkeling doorzet, privacy op termijn alleen nog betaalbaar is voor de rijken[10]. In dit geval is dat echter te weerleggen. Hier vindt namelijk niet direct een uitruil tussen privacy en premie plaats, maar tussen data en premie – iets wat verzekeraars al zeker honderd jaar doen. Er is altijd al een groot verschil geweest tussen mensen die wel en geen data willen delen met een verzekeraar. Zonder data was er geen verzekering mogelijk, met data wel. Enige verschil is dat de verzekeraar nu *meer* data tot zijn beschikking heeft, waardoor hij een betere risicoinschatting kan maken en een beter product kan leveren. Waar de grens ligt tussen de uitruil tussen data en premie en tussen privacy en premie, is een vraag die waarschijnlijk alleen in de praktijk beantwoord kan worden. Welke ruil vinden we maatschappelijk nog wel acceptabel en welke niet? Een rokerstarief bij een levensverzekering was veertig jaar geleden ondenkbaar, maar nu volkomen acceptabel. Zie ook paragraaf 7.2 over de Solidariteitsmonitor, waarin ook het wel of niet verstrekken van gedragsgegevens meegenomen wordt. Er is natuurlijk een verschil tussen soorten data en hoe privacygevoelig die is. Maar ook privacygevoelige informatie kan vertrouwelijk verwerkt worden, zonder dat daarmee andere of ongewenste doelen worden gediend. Vraag is waar mensen zich comfortabel bij voelen. Randvoorwaarde in elke situatie zal in ieder geval zijn dat verzekeraars betrouwbaar met gegevens omgaan.

6.1.2 Proportionaliteit

Belangrijke eis uit de Wbp is dat niet meer gegevens worden verwerkt dan noodzakelijk. Dat wordt 'proportionaliteit' genoemd. De afweging of meer data verwerkt mag worden, moet steeds indiviueel gemaakt worden, maar ook in het algemeen kan volgens deze eis de vraag gesteld worden of verzekeraars Big Data wel nodig hebben. Met de wet van de grote getallen kunnen zij toch al heel goede risico-inschattingen maken?

Voor het berekenen van een premie voor een grote groep klanten, volstaat de beperkte set data inderdaad. Maar de samenleving individualiseert. En klanten verwachten ook een meer persoonlijke behandeling. Dat zien we bijvoorbeeld in de markt voor autoverzekeringen, waarin verzekerden met schadevrijejaren beloond worden voor hun goede rijgedrag. Ook verwachten klanten steeds meer service van hun verzekeraar. De verzekeraar die, binnen de wettelijke kaders, mee kan denken met de klant en er is op het moment dat een klant daar behoefte aan heeft, wint de concurrentiestrijd. Denk aan tips over veiliger of zuiniger rijgedrag. Of over inbraakpreventie. Voorkomen is beter dan genezen. Hoewel de afweging inzake

[9] *Simplification of Privacy Disclosures: An Experimental Test*. Paper uit 2015 door Omri Ben-Shahar & Adam Chilton.

[10] http://www.nrc.nl/handelsblad/2015/11/28/zo-behouden-alleen-de-rijken-hun-privacy-1561104

proportionaliteit dus door de individuele verzekeraar gemaakt moet worden, kan in het algemeen wel gezegd worden dat Big Data nodig kan zijn om klanten optimaal van dienst te zijn. Dan zal die toegevoegde waarde wel duidelijk moeten zijn voor klanten.

6.2 Solidariteit

Big Data kan ook gevolgen hebben voor de solidariteit. Big Data sluit solidariteit niet uit, maar Big Data kan bijvoorbeeld wel leiden tot meer segmentatie. Want hoe meer data over het risico en over de klant, hoe beter verzekeraars producten en premies op maat kunnen maken. Denk aan de *Usage Based*-autoverzekering, waarbij de verzekeraar de premie aanpast als de klant veiliger of minder veilig rijdt. Dan kan een verzekering geboden worden aan een beperkte groep klanten, die allemaal dezelfde scores hebben. Maar wat als de groepsgrootte steeds verder afneemt? Verdwijnt de solidariteit dan ook?

Een andere bedreiging voor de solidariteit zou kunnen liggen in het wegvallen van de informatiesymmetrie. Op het moment dat een klant een verzekering afsluit, moeten beide partijen over dezelfde risico-informatie beschikken. Weet een klant meer dan de verzekeraar, dan kan dat problematisch zijn. Het is goed dat klanten zelf beter begrijpen welke risico's zij lopen. Maar als zij zich vervolgens niet meer willen aansluiten bij een verzekering die ook mensen dekking biedt die een veel hoger risico lopen dan zijzelf, kan dat de verzekeraar in problemen brengen. Uit het voorbeeld: de veilige rijder wenst misschien niet langer te betalen voor zijn minder voorzichtige collega-bestuurder. Die zal dus geen verzekering meer afsluiten. Dat klinkt goed voor de klanten – die kunnen het heft immers gemakkelijker in eigen hand nemen. Maar de klanten die veel risico lopen zijn hiervan de dupe; als de verzekeraar alleen nog maar onveilige klanten heeft, zal de schadelast hoger worden dan gepland, waardoor de premie omhoog moet. Dreigt dan niet het einde van de solidariteit?

Het antwoord op deze vraag hangt mede af van wat er onder solidariteit verstaan wordt. Verstaan we onder solidariteit simpelweg de grootte van de groep die het risico deelt (een segment), dan kan Big Data inderdaad gevolgen hebben voor de solidariteit. Maar Van Dale definieert solidariteit als 'bewustzijn van saamhorigheid en bereidheid om de consequenties daarvan te dragen'. Het valt te betwijfelen of een individu, die anno 2016 een autoverzekering afsluit, een gevoel van saamhorigheid heeft richting de medeverzekerden. Zo is het moderne verzekeren wel ooit begonnen, toen mensen en bedrijven elkaar opzochten om het risico op een brand van hun woning of bedrijf te delen. Als er zich een buurtgenoot meldde bij zo'n groep verzekerden die zelf de veiligheid thuis of op het eigen bedrijf niet serieus nam, dan werd die daar zeker op aangesproken of mogelijk niet eens toegelaten tot de kring van verzekerden.

"Als je weet dat je tot een selecte groep veilige bestuurders behoort, dan wil je dat behouden. Zo bezien, maakt Big Data solidariteit weer mogelijk."

Het moderne verzekeren is echter volledig geanonimiseerd: mensen worden niet meer door hun medeverzekerden aangesproken op hun gedrag. Sterker nog: wie weet er of hij of zij bij dezelfde verzekeraar is aangesloten als de buren? Als een verzekeraar met Big Data beter weet welke verzekerden een even groot risico vormen, dan kan hij die samenbrengen in een groep en een op maat gesneden product aanbieden. De kans is dan aanwezig dat er juist meer solidariteit ontstaat. Als je weet dat je tot een selecte groep veilige bestuurders behoort, dan wil je dat behouden. Zo bezien, maakt Big Data solidariteit dus weer mogelijk. Maar voor die solidariteit maakt de groepsgrootte niet zoveel uit. Dat zien we anno 2016, nu er steeds meer kleine cooperaties opkomen. Broodfondsen zijn een aansprekend voorbeeld[11]. In zo'n fonds nemen maximaal vijftig zelfstandig ondernemers deel. Zij leggen maandelijks geld in en bij ziekte van één van

[11] http://www.broodfonds.nl/hoe_het_werkt

hen, keert het fonds uit. Het gevoel van saamhorigheid en de bereidheid daar de consequenties van te dragen, zijn in zo'n groep veel groter dan bij traditionele verzekeringen. Toch is de groepsgrootte zeer beperkt.

Tegelijk kan Big Data misbruik van solidariteit voorkomen. De anonimiteit van het moderne verzekeren zorgt er namelijk ook voor dat verzekeraars met veel fraude te maken hebben. Jaarlijks sporen verzekeraars voor honderd miljoen euro aan fraude op. Dit betreft vermoedelijk maar een deel van het probleem. Big Data-analyses kunnen ook op dit front hun waarde bewijzen doordat daarmee het detecteren, maar vooral ook het voorkomen van fraude beter mogelijk wordt.

Big Data en solidariteit sluiten elkaar dus zeker niet uit. Door Big Data gaan verzekeraars echter wel meer groepen creëren van mensen met een min of meer gelijk risicoprofiel en hen een op maat gesneden product en premie bieden. Dat betekent dat Big Data de solidariteit binnen die groepen kan vergroten, maar ervoor kan zorgen dat de verschillen tussen die groepen toenemen. Dat hoeft niet bezwaarlijk te zijn, mits iedereen tegen min of meer acceptabele condities een verzekering kan krijgen. De vraag is hoever deze trend zal doorzetten.

Er blijft altijd ruimte voor solidariteit

Met de komst van zelfrijdende auto's wordt weleens gezinspeeld op het einde van de behoefte aan autoverzekeringen. Hoewel de schadekans ongetwijfeld zal dalen, omdat deze auto's nog maar zelden zullen botsen, blijven er vermoedelijk voldoende risico's over. Een forse hagelbui kan nog altijd kostbare schade veroorzaken en auto's kunnen nog altijd gestolen worden (misschien zelfs op afstand). Ook kan een *softwarebug* voor flinke schade zorgen. Zo blijven er dus voldoende onvoorspelbare 'van buiten komende onheilen' die de behoefte aan verzekeringen voeden en die solidariteit tussen mensen creëert. De vraag is wie deze risico's zal dragen: een traditionele verzekeraar, een autofabrikant of een platform gebaseerd op de *blockchain* (over deze laatste optie, hieronder meer). Tot op zekere hoogte zullen er in ieder geval altijd groepen mensen zijn met een min of meer gelijk risicoprofiel, waardoor er altijd ruimte blijft voor solidariteit.

6.3 Uitsluiting en insluiting

Met Big Data weten verzekeraars nóg beter welk risico een klant vertegenwoordigt. Verzekeraars zouden gedreven door dit inzicht kunnen beslissen slechte risico's uit te sluiten of slechts tegen een hogere premie te verzekeren. Het is niet moeilijk om enkele doemscenario's te schetsen, maar er zijn tegelijk genoeg krachten in het spel om te voorkomen dat deze waarheid worden.

Laten we als voorbeeld eens kijken naar een standaard inboedelverzekering. Met de komst van allerlei apparaten en sensoren in de woning die aan het internet gekoppeld zijn (Internet of Things), weet de inboedelverzekeraar steeds meer over een verzekerde en diens woning (mits de verzekerde daar toestemming voor heeft gegeven). Dit zit op het snijvlak van *volunteered* en *observed data*. Dat kan er toe leiden dat een verzekeraar weet dat een bepaalde klant de batterij van zijn rookmelder niet tijdig vervangt. Diezelfde klant kan echter weer heel nauwgezet de woning afsluiten voor vertrek naar vakantie. De verzekeraar heeft nu veel meer data en kan daarmee de klant wellicht goed adviseren. Maar loopt deze klant nu veel of weinig risico? Dat is misschien helemaal niet zo duidelijk. Kunnen verzekeraars op grond van de toegenomen hoeveelheid data wel risico's of klanten uitsluiten, gegeven het feit dat menselijk gedrag niet altijd consistent is en niet in lijn is met de verzekerde risico's?

Verder is het niet waarschijnlijk dat verzekeraars grote groepen potentiele klanten links laten liggen. De Nederlandse verzekeringsmarkt is namelijk een verzadigde markt. Er is weinig groei mogelijk voor verzekeraars, anders dan ten koste van andere verzekeraars. Mocht er toch een groep worden uitgesloten dan zal er vermoedelijk al snel een

aanbieder zijn die daar een product voor ontwerpt. In het verleden zijn er ook onderlinge verzekeraars ontstaan uit groepen klanten die niet terecht konden bij bestaande verzekeraars. Overigens zijn er ook zonder Big Data al mensen die niet verzekerd zijn. Er is nu eenmaal armoede in Nederland. Sommige mensen kunnen daardoor ook hun basale verzekeringen niet meer betalen.

"Het is niet waarschijnlijk dat verzekeraars grote groepen klanten links laten liggen."

Toch is uitsluiting iets om scherp op te letten. Als er door toepassing van Big Data nieuwe groepen onverzekerden ontstaan, dan is het zaak om in te grijpen. Dat is de maatschappelijke taak van verzekeraars: het verzekeringsprincipe moet voor iedereen in Nederland mogelijk zijn. Dat is ook één van de waarden uit de Gedragscode Verzekeraars: mogelijk maken. Dat heeft de Nederlandse verzekeringsindustrie eerder gedaan met de komst van Rialto. Die maatschappij is in de jaren '60 opgericht om tegemoet te komen aan het feit dat een motorrijtuigenverzekering verplicht is, maar sommige klanten (bijvoorbeeld met een bijzonder slecht schadeverleden) door alle verzekeraars geweigerd werden. Mocht nu opnieuw een groep onverzekerden ontstaan, waar de markt geen oplossing voor heeft, dan zijn er dus altijd weer manieren denkbaar om tot een oplossing te komen.

6.3.1 Discriminatie

Overigens is het van belang om ook even stil te staan bij het fenomeen discriminatie. Als verzekeraars groepen klanten met een min of meer gelijk risicoprofiel bij elkaar brengen, dan bestaat het gevaar dat zij onbedoeld bepaalde mensen indirect discrimineren. We spreken van discriminatie wanneer er onderscheid gemaakt wordt op grond van ras (afkomst of huidskleur), geloof of levensovertuiging, handicap of chronische ziekte, seksuele voorkeur, geslacht, leeftijd, zaken als politieke overtuiging, nationaliteit of voltijd en deeltijdcontracten[12]. Een Big Data-analyse kan bijvoorbeeld aantonen dat mensen in een bepaalde straat minder kredietwaardig zijn of vaker met politie en justitie in aanraking komen. Als een bedrijf op grond daarvan beslissingen neemt over het productaanbod voor mensen met dit profiel, dan kan dat problematisch zijn. Stel dat veel mensen uit die straat een bepaald geloof aanhangen, dan leidt dit tot indirecte discriminatie van mensen met dat geloof. De Amerikaanse Federal Trade Commission (FTC) heeft in een recent rapport veel van dit soort onterechte en onjuiste verbanden aan de kaak gesteld, hoewel de FTC gelukkig ook veel goede voorbeelden aandraagt van de inzet van Big Data[13]. De FTC stelt dat het om deze reden van het grootste belang is om bij de inzet van Big Data, de gebruikte analyses bijzonder kritisch te bekijken: zitten daar elementen in, die voor discriminatie zorgen? Hoe accuraat is het model? Is de steekproef representatief? Er moet immers voorkomen worden dat Big Data leidt tot 'digitale predestinatie'. Deze term is afkomstig van de heer Kohnstamm van de Autoriteit Persoonsgegevens[14]. Hij betoogt dat mensen niet meer in staat zijn zelf hun leven in te richten als bedrijven allerlei keuzes maken op basis van zelf aangelegde profielen van (potentiële) klanten. Op grond van een bepaald profiel krijgen mensen uit de ene groep wel een aanbieding en mensen uit een andere groep niet, terwijl het best mogelijk is dat mensen uit die tweede groep baat kunnen hebben bij het aanbod of dat ze onterecht in die groep zijn ingedeeld. Zeker als dit gebeurt op grond van *observed data*, waar mensen weinig controle over hebben, kan dit verkeerd uitpakken. Dit stelt verzekeraars voor een uitdaging omdat verzekeraars van oudsher mensen in groepen indelen en die groepen vervolgens verschillend behandelen, afhankelijk van hun risicoprofiel. Verzekeraars zullen bij gebruik van *observed*

[12]https://www.rijksoverheid.nl/onderwerpen/discriminatie/inhoud/verbod-op-discriminatie
[13]https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf
[14] https://www.ictmagazine.nl/columns/big-data-en-het-voorkomen-van-digitale-predestinatie/

data, op grond waarvan klanten in groepen worden ingedeeld, dus extra voorzichig moeten zijn zodat klanten weten wat er gebeurt en eventueel bezwaar kunnen maken. Biedt de klant 'grip op de data'.

6.4 Zorgen omtrent het bedrijfsmodel

Big Data-analyses brengen risico's met zich mee voor klanten, maar ook voor verzekeraars. En uiteindelijk heeft dat ook weer gevolgen voor de klant. Big Data kan het bedrijfsmodel van verzekeraars bemoeilijken, anderzijds zorgt Big Data dat juist nieuwe concurrenten het makkelijker krijgen. Meer data kan verzekeraars meer inzicht opleveren, maar in de paragraaf over solidariteit, werd duidelijk dat ook klanten hiermee hun gedrag kunnen aanpassen. Als klanten zelf steeds beter weten welke risico's zij lopen, kan dit er toe leiden dat mensen die weinig risico lopen, zich niet of minder gaan verzekeren. Voor die klanten is dat misschien goed nieuws, maar daarmee stijgt de gemiddelde schade per klant, zodat de premie omhoog moet. Op die manier kan een neerwaartse spiraal ontstaan, waarbij uiteindelijk alleen de klanten overblijven met de hoogste risico's, die een hele hoge premie moeten betalen. Dan is er de facto sprake van onverzekerbaarheid. Niet onwaarschijnlijk, want met alle informatietechnologie, zelfrijdende auto's en sensoren weten klanten zelf steeds beter welke risico's zij lopen en waar zij zich wel voor willen verzekeren en waarvoor niet. Het is dus zaak deze ontwikkeling goed in de gaten te houden. Toch is de kans groot dat er altijd onzekerheid blijft. Denk aan een hagelbui of een storm. Ook kunnen er door de afhankelijkheid van IT weer nieuwe risico's ontstaan: risico's op identiteitsfraude, hacks of systeemfalen. In zoverre zal er altijd behoefte blijven bestaan om risico's te delen of over te dragen aan een partij, zoals een verzekeraar.

Dit punt maakt wel duidelijk dat verzekeraars de datarevolutie nauwgezet moeten volgen. Neem nu de data die een moderne *connected* auto verzamelt: autofabrikanten doen er alles aan om die data exclusief voor zichzelf te houden. In dit verband zijn er al consumentenorganisaties die er voor pleiten dat niet de fabrikant of een ander bedrijf 'eigenaar' van dergelijke data moet zijn, maar klanten zelf[15]. Dit fenomeen speelt momenteel bij auto's, maar als er met het Internet of Things straks steeds meer sensoren in bijvoorbeeld woningen geplaatst worden, zal dit punt breder gaan spelen. Los van toegang tot data is het belangrijk goede afspraken te maken over het eigenaarschap ervan – zeker omdat het goed denkbaar is dat derden met meer IT-kennis de data verwerken. Een IT-leverancier zou dan marktmacht kunnen krijgen als poortwachter tot de data. Die marktmacht kan een bedreiging vormen voor klanten die niet meer kunnen wisselen van aanbieders, maar ook voor de bedrijfsvoering van verzekeraars. Idealiter zou de klant zelf moeten kunnen bepalen wie toegang heeft tot de data, niet een IT-bedrijf, noch de verzekeraar. Dat brengt lastige discussies met zich mee, zeker voor data die in het verleden verzameld zijn. Maar het Verbond wil deze grip op de data voor de klant als uitgangspunt nemen bij toekomstige ontwikkelingen. Gelukkig voorziet de komende Europese privacyverordening al in een 'recht op dataportabiliteit' voor klanten. Dat is een recht van klanten om hun data, zoals die bij de ene aanbieder geregistreerd staan, over te dragen aan een andere aanbieder.

"Idealiter zou de klant zelf moeten kunnen bepalen wie toegang heeft tot de data, niet een IT-bedrijf, noch de verzekeraar."

Naast het feit dat Big Data dus zorgen oplevert ten aanzien van het bedrijfsmodel van verzekeraars, zorgt de Big Data-revolutie ook voor nieuwe concurrentie. Geen zorg voor verzekerden, maar wel voor verzekeraars. Het is nu mogelijk om met een gemiddelde computer en data uit de *cloud* berekeningen te maken, die vroeger alleen door grote bedrijven gedaan konden worden. Hierdoor kan de concurrentie nu plots uit heel onverwachtse hoek komen. En ook de transacties zelf kunnen gemakkelijk zelf geregeld worden. Banken zijn

[15] http://www.anwb.nl/auto/connected-car/my-car-my-data

al volop bezig de *blockchain*-technologie te onderzoeken. Dit is een openbaar register van transacties, waarmee deelnemers erop kunnen vertrouwen dat hun transactie zonder tussenkomst van *trusted third parties* conform de gemaakte afspraken uitgevoerd zal worden. Het is een register waarin elke paar minuten wordt vastgelegd wie aan wie welk bedrag schuldig is. Deutsche Bank verwacht de eerste commerciële *blockchain*-alternatieven voor eind 2017[16].

Het is niet ondenkbaar dat er ook *blockchain*-toepassingen komen voor de verzekeringsmarkt. Waarom zouden tienduizend individuen zich niet met zo'n register kunnen verbinden tot het doen van een betaling aan een ongelukkige enkeling als die door het noodlot getroffen wordt? Het is denkbaar dat zo'n platform de rol van een verzekeraar overbodig maakt. Overigens moet wel iemand dat platform ontwikkelen en beheren: dat zou ook een verzekeraar kunnen zijn. Er kleven vooralsnog echter allerlei moeilijkheden aan de inzet van zo'n *blockchain*-verzekering. Wie bepaalt bijvoorbeeld hoe hoog de schade is als de woning van een verzekerde afbrandt? Is zo'n *blockchain* niet te hacken? Wat als er ineens veel meer schades zijn dan vooraf gedacht? Wie bepaalt wie er mee mag doen? Lastige vragen, maar die hoeven een *blockchain*-verzekering niet in de weg te staan. Er zullen nog wat hobbels genomen moeten worden, maar de belofte is zo groot, dat dit de investering waarschijnlijk wel rechtvaardigt.

7 Checks and balances

De beschreven kansen en zorgen laten zien dat Big Data een krachtig instrument kan zijn. Tenminste: als er oog is voor de zorgen die leven en als nadelen zoveel mogelijk worden uitgesloten. Alleen dan hebben zowel verzekeraars als klanten baat bij Big Data. Let wel: het zijn *mogelijke* nadelen. Deze risico's hebben zich nog niet verwezenlijkt en dat gaat misschien ook helemaal niet gebeuren.

Allereerst is er natuurlijk wetgeving die dat moet voorkomen, met name de Wet bescherming persoonsgegevens (Wbp). Deze wet wordt voor verzekeraars nader uitgewerkt in de Gedragscode Verwerking Persoonsgegevens Financiële Instellingen (GVPFI)[17]. Tegelijk is er bij elke nieuwe ontwikkeling altijd even tijd nodig om uit te vinden hoe de wetgeving daarop van toepassing is. Nieuwe regels dan maar? Nee. Het Verbond pleit ervoor eerst eens beheerst te kijken naar de ontwikkelingen, zodat gericht ingegrepen kan worden waar nodig. Als niet bekend is welke problemen precies moeten worden voorkomen, hoe groot die zullen zijn en waar ze zich exact zullen voordoen, is de kans aanwezig dat de regels niet alleen de risico's, maar ook de kansen uitsluiten. Daarnaast is de kans groot dat de regels niet effectief zullen zijn. Volgens het Verbond heeft de verzekeringsbranche daarbij ook zelf een grote rol – mogelijk in samenwerking met andere partijen. Daarvoor doen we in dit hoofdstuk enkele aanbevelingen. Om hier goede invulling aan te geven, zal het Verbond allereerst een klankbordgroep Big Data oprichten die de ontwikkelingen volgt, maar ook geregeld met stakeholders overlegt om te zien of de hier voorgestelde 'checks and balances' doen wat ze moeten doen.

7.1 Privacychecks

Allereerst de zorgen over 'privacy'. Uitgangspunt is daarbij uiteraard dat verzekeraars zich aan de regels voor gegevensbescherming moeten houden. Het is daarvoor ook belangrijk dat verzekeraars het privacybewustzijn in hun organisaties en vooral bij de ontwikkeling van Big Data-toepassingen incorporeren. Privacy is niet iets van de Afdeling Compliance of van de Functionaris Gegevensbescherming, maar moet ook bij productontwikkelaars, marketeers en de

[16] http://www.coindesk.com/deutsche-bank-blockchain-tech-will-go-mainstream-next-decade/

[17] https://www.verzekeraars.nl/overhetverbond/zelfregulering/Paginas/Gedragscodes/Gedragscode-Verwerking-Persoonsgegevens.aspx

directie tussen de oren zitten. Het Verbond draagt hieraan bij met dit green paper, maar zal zich ook verder beraden op themadagen of andere middelen om leden hierbij te ondersteunen. Uiteraard kijkt het Verbond ook wat er buiten de muren gebeurt. Zo wordt *privacy by design,* een methode om vanaf het begin van een product de bescherming van persoonsgegevens in te bouwen[18], vanaf 2018 verplicht voor iedereen die onder de Algemene Verordening Gegevensbescherming valt. Vooruitlopend daarop wil het Verbond in het komende jaar onderzoeken hoe de principes van *privacy by design* op verzekeringen kunnen worden toegepast om daarmee zijn leden te inspireren.

De eisen ten aanzien van de bescherming van gegevens worden steeds strikter. Sinds 1 januari 2016 geldt in Nederland bijvoorbeeld de meldplicht datalekken. Het Verbond draagt bij aan gegevensbescherming doordat verzekeraars onderling en met het Nationaal Cyber Security Centrum, de Nationale Politie en de AIVD informatie uitwisselen over mogelijke beveiligingsproblemen. Dat doen zij in een zogeheten *Information Sharing and Analysis Center* (ISAC). Verder zal het Verbond in 2016 een CERT oprichten: een *Computer Emergency Response Team*. Dit is een operationeel samenwerkingsverband op het gebied van cybersecurity dat aangesloten deelnemers doorlopend informeert en adviseert. Bijvoorbeeld over dreigingen, kwetsbaarheden en incidenten, maar ook over preventiemogelijkheden en handelings-perspectieven. Daarnaast ontwikkelde het Verbond al in 2014 beleid voor de sector ten aanzien van *responsible disclosure*. Dit beleid helpt verzekeraars omgaan met goed-bedoelende hackers die gaten in de beveiliging van een verzekeraar aantonen. Het is van belang dat verzekeraars ook individueel werk maken van hun gegevensbescherming.

Belangrijk bij het beschermen van privacy is de informatieplicht: verzekerden moeten weten wat er met hun data gebeurt. Verzekeraars maken dat zo inzichtelijk mogelijk via het privacystatement. Dat verzekeraars de verantwoordelijkheid nemen klanten zo goed mogelijk te informeren over wat zij doen met data, is ook vastgelegd in de Gedragscode Verwerking Persoonsgegevens, een gedragscode die de branche als een van de weinige branches heeft. Deze code wordt in 2016 geactualiseerd, waarbij ook extra aandacht geschonken wordt aan manieren om klanten te informeren over privacybeleid.

"Als de inzet van Big Data niet uitgelegd kan worden aan het publiek, dan moet je kunnen verklaren waarom je het toch doet, of je moet het niet doen."

Verzekeraars doen er verstandig aan om die actualisering niet af te wachten, maar zelf aan de slag te gaan met het vormgeven van waarborgen om Big Data-gebruik mogelijk te maken. Allereerst moeten zij open communiceren over de inzet van Big Data. Waarom zouden zij dat niet doen, als zij Big Data klantgericht inzetten? Als de inzet van Big Data niet uitgelegd kan worden aan het publiek, dan moet je kunnen verklaren waarom je het toch doet, of je moet het niet doen. Verzekeraars moeten klanten informeren over het gebruik van *observed data* en hen in de gelegenheid stellen om eventuele fouten te corrigeren zodat de klant 'grip op zijn data' heeft. Op internet gebeurt dat door middel van *cookie*-wetgeving. Offline maken verzekeraars gebruikt van *opt-in*, in combinatie met informatie over waar de informatie voor gebruikt wordt. Klanten vertrouwen verzekeraars met gegevens. Verzekeraars moeten er alles aan doen om dat vertrouwen te houden.

Iets verder weg liggen fenomenen als *data vaults* en mogelijk nog innovatievere oplossingen. Bij een *personal data vault* heeft de klant zijn persoonsgegevens in eigen beheer en mag een bedrijf daar eenmalig in kijken om daar een aanbod op te baseren. De verzekeraar heeft in zo'n model alleen nog maar wat contactgegevens in huis. Dit model vereist echter nogal wat ontwikkeling. De verwachting

[18]https://en.wikipedia.org/wiki/Privacy_by_design

is dat met de grote spanning tussen de Big Data-mogelijkheden enerzijds en de regelgeving anderzijds, dit soort innovaties in de komende jaren snel aan terrein zullen winnen. Het Verbond zal deze ontwikkelingen op de voet volgen en waar mogelijk verzekeraars stimuleren hier gebruik van te maken om de grip op de data door de klant te vergroten.

7.2 Solidariteitsmonitor

We zagen dat de solidariteit binnen groepen weleens kon toenemen, maar dat Big Data-toepassingen de zorg met zich meebrengen dat bepaalde categorieën mensen nergens meer een verzekering kunnen krijgen. Het is nog te vroeg om te zeggen dat dit zal gebeuren, maar we moeten hier wel alert op zijn.

Om daar handen en voeten aan te geven, wil het Verbond vanaf 2016 elk jaar een zogenaamde Solidariteitsmonitor organiseren. Doel is het vroegtijdig opsporen van mogelijke negatieve gevolgen van Big Data-toepassingen. Nederlanders zijn anno 2016 goed verzekerd. De penetratiegraad van aansprakelijkheidsverzekeringen voor particulieren ligt op 95 procent, de penetratiegraad voor inboedelverzekeringen ook. Van alle automobilisten is slechts een klein percentage aangewezen op het vangnet dat Rialto biedt. Het Verbond zal vanaf 2016 ieder jaar checken hoe dit zich ontwikkelt en daarover publiekelijk rapporteren. Dat moment vormt tevens de gelegenheid voor belangen-groeperingen om de verzekeringsbranche te wijzen op eventuele groepen onverzekerden. Als dit het geval is, zal het Verbond zich ervoor inzetten dat de toegang tot verzekeringen zo goed blijft, als die in 2016 was. Dit sluit aan op principe 21 uit de Gedragscode Verzekeraars, waarin verzekeraars beloven zo veel mogelijk klanten de mogelijkheid te bieden risico's financieel af te dekken en zich in te zullen spannen om onverzekerbaarheid te voorkomen[19].

Bij de Solidariteitsmonitor zal het Verbond monitoren hoe de bandbreedte tussen de laagste en de hoogste premie en de daarbij behorende dekking en voorwaarden zich ontwikkelt. De precieze vorm moet nog worden vastgesteld, maar de eerste gedachten gaan uit naar een toets met een aantal maatmensen en de ontwikkeling van hun premies en dekkingen. Door bijvoorbeeld na te gaan wat de hoogste en laagste premie is voor een specifieke maatman bij een bepaalde dekking en hoe de bandbreedte tussen die maatmannen zich ontwikkelt, ontstaat een beeld van de tendens. Bij dit onderzoek zullen we ook het aspect privacy meenemen: hiervoor zal een maatman opgenomen worden die niet bereid is gedragsgegevens te delen.

Belangrijke vraag is uiteraard, wat er gedaan wordt met de resultaten van de monitor: wanneer is er sprake van een probleem en wat gebeurt er dan? Dit is iets wat het Verbond in overleg met onder meer consumentenorganisaties nader zal bepalen. De monitor is derhalve geen oplossing, maar een manier om uit te vinden of er een probleem is, hoe groot het is en waar het zich voordoet.

In het hoofdstuk over solidariteit constateerden we ook dat Big Data onbedoeld kan zorgen voor indirecte discriminatie. Dit is een fenomeen waar verzekeraars individueel alert op moeten zijn. In Nederland is het College voor de Rechten van de Mens aangewezen om onderzoek te doen naar (vermeende) discriminatie. Het Verbond zal daarnaast zelf onderzoek stimuleren naar manieren om (indirecte) discriminatie te voorkomen: in samenwerking met universiteiten wordt onderzocht of het mogelijk is om richtlijnen op te stellen die voorkomen dat datamodellen onbedoeld indirecte discriminatie in de hand werken. Verzekeraars moeten verder zelf nadenken over mogelijkheden waardoor klanten zelf hun data kunnen corrigeren. Hierbij zal bijzondere aandacht zijn voor de anonieme data die verzekeraars inkopen en die hen helpen bij het aanleggen van profielen op

[19] https://www.verzekeraars.nl/overhetverbond/zelfregulering/Documents/Gedragscodes/Gedragscode_NL_2015.pdf

bepaalde generieke niveaus (bijvoorbeeld postcode, wijk of plaats). Dat zijn geen klantdata, maar klanten krijgen er wel mee te maken als deze data hun risicoprofiel deels bepalen. Hoewel dat profiel eerlijk is voor een groot deel van de mensen uit die wijk, zal een deel van de mensen zich hierdoor onterecht behandeld voelen. Klanten zouden dan een correctiemogelijkheid moeten kunnen krijgen. Ook hier gaat opnieuw de slogan op: biedt de klant 'grip op zijn data'. Desgevraagd zouden mensen bijvoorbeeld te horen kunnen krijgen, welk klantprofiel er over hen is samengesteld. Dat gaat verder dan hetgeen wettelijk vereist is, omdat de wet enkel toeziet op het informeren van klanten over hun persoonsgegevens.

"Verzekeraars moeten nadenken over mogelijkheden voor klanten om hun data te corrigeren."

Als klanten vragen hebben over een categorisering, is het belangrijk dat verzekeraars in staat zijn hun model uit te leggen. Hoe ingewikkeld Big Data-modellen ook mogen zijn, het is zaak dat verzekeraars ze zelf wel begrijpen zodat correctie altijd mogelijk is. Het Verbond raadt verzekeraars daarom aan een 'communicatietoets' te hanteren. Zo'n toets kan inhouden dat verzekeraars alleen die verbanden gebruiken in hun modellen, waar een logische, risicogerelateerde verklaring voor te geven is. Er is bijvoorbeeld een logische verklaring voor het gegeven dat het gewicht van een auto of de rijstijl van een bestuurder relevant is voor de hoogte van een premie. Ook het betaalgedrag van klanten is een logische factor: slecht betalende klanten nopen verzekeraars immers tot incassoprocedures. Factoren die niet uit te leggen zijn, zouden niet meegenomen moeten worden in datamodellen. Als verzekeraars Big Data-analyses niet kunnen uitgeleggen, kunnen zij ook niet verwachten dat klanten er begrip voor hebben en dat er duurzaam maatschappelijk draagvlak voor is. Dit sluit ook aan op belangrijke principes uit de Gedragscode Verzekeraars. Principe 5 zegt dat verzekeraars duidelijk zijn over de werking en kosten van producten. Principe 7 stelt dat het acceptatie- en schadebehandelingsproces inzichtelijk moeten zijn voor de klant. Hieraan zitten uiteraard wel grenzen. Verzekeraars zullen geen inzage kunnen geven in bedrijfsgeheime rekenmodellen. Ook is niet alles aan iedereen uit te leggen: het gaat hier vaak om complexe materie. Het streven zou echter wel moeten zijn dat verzekeraars hun modellen kunnen uitleggen.

7.3 Bedrijfsmodel

Tot slot bleek dat Big Data ook zorgen kan opleveren over het bedrijfsmodel van verzekeraars. Als verzekerden meer inzicht krijgen in risico's dan verzekeraars, kan dat het model van verzekeraars bemoeilijken, met ook voor klanten allerlei gevolgen. Daarnaast zorgt het fenomeen Big Data voor nieuwe concurrentie, mogelijk uit totaal onverwachtse hoek. Dat is goed, omdat het bestaande aanbieders prikkelt. Tegelijk moeten de regels die voor verzekeraars gelden, ook op deze nieuwe bedrijven van toepassing zijn. In dit kader doen wij de volgende aanbevelingen:

1. Verzekeraars doen er verstandig aan om hun eigen data te organiseren. Sommige verzekeraars hebben te maken met zogenaamde *legacy*: systemen van rechtsvoorgangers die nog niet in lijn zijn gebracht met eigen of modernere systemen. Voordat verzekeraars Big Data gaan gebruiken, moeten ze hun eigen data op orde hebben.

2. Om een weloverwogen keuze te kunnen maken op basis van de voor- en nadelen van de inzet van Big Data, is het van belang dat verzekeraars beschikken over voldoende kennis. Het Verbond zal hier in zijn opleidingsaanbod aan verzekeraars op inspelen. Verzekeraars zelf doen er verstandig aan samen te werken met universiteiten, onder meer om talenten te interesseren voor hun bedrijf. Het Verbond is in 2016 voor het tweede jaar betrokken bij een vak aan de TU Delft waarin studenten proberen met bestaande data van verzekeraars nieuwe kennis te ontwikkelen.

3. Waar data anno 2016 al belangrijk zijn, zal dat de komende jaren alleen nog maar

toenemen. Het is dan ook belangrijk dat verzekeraars, wanneer gewenst, over data kunnen beschikken. Maar met de toenemende waarde van data proberen fabrikanten (van auto's, maar ook van allerlei huishoudelijke apparatuur) om hun data af te schermen. Dat is een risico. In eerste instantie zal een klant een mogelijk voordeel hebben van afgesloten systemen, maar op den duur kan een klant hierdoor ingekapseld raken en wordt het lastiger om te wisselen van aanbieder. Een verwarmingsketel van fabrikant x werkt alleen met radiatoren van fabrikant x, een thermostaat van fabrikant x en een monteur van fabrikant x. Dit fenomeen heeft zich de afgelopen jaren al voorgedaan in de markt voor softwarepakketten en mobiele telefoons, al biedt nieuwe regelgeving daar nu soms een oplossing voor. Het is daarom van belang om te voorkomen dat fabrikanten dit soort afgesloten systemen kunnen vormen zodat klanten altijd kunnen overstappen. Dit draagt bij aan het gebruik van data voor eigen dienstverlening van verzekeraars, maar biedt ook gezond tegenwicht aan de macht van fabrikanten. Het voorstel uit de aankomende Europese Verordening Gegevensbescherming over *dataportabiliteit* kan hier weleens heel belangrijk voor worden: dat geeft consumenten het recht om 'hun' data in een *machine readable format* op te vragen bij de ene dienstverlener om die vervolgens over te zetten naar een andere dienstverlener. Het Verbond zal er, samen met haar Europese zusterorganisaties, alert op zijn dat dit soort *checks and balances* ingebouwd wordt in regelgeving omtrent data.

4. De toepassingen van Big Data lijken oneindig: als verzekeraars die zelf niet benutten, zal een *fintech-startup* dat wel doen. Verzekeraars doen er dan ook goed aan hun eigen concurrentie te creëren. Er zijn al verzekeraars die stevig investeren in *startups*. Verzekeraars kunnen ook *blockchain*-verzekeringen ontwikkelen. Het Verbond stimuleert dit met zijn eigen insuranceLAB: een fysieke plek waar samengewerkt wordt met allerhande partijen van binnen en buiten de branche, op zoek naar innovaties.

5. Het Verbond beschikt met het Centrum voor Verzekeringsstatistiek (CVS) over veel (anonieme) data. Op grond hiervan krijgen verzekeraars allerlei vertrouwelijke rapporten over hun bedrijfseconomische positie. Het CVS gebruikt abstracten van deze data ook om trends in de samenleving te onderzoeken en werkt hiervoor al geregeld samen met wetenschappers. Deze rol moet echter uitgebreid worden: enerzijds door meer open data naar binnen te halen, op grond waarvan kennis voor verzekeraars ontwikkeld kan worden, anderzijds door meer data te ontsluiten voor wetenschappelijk onderzoek naar maatschappelijk relevante vraagstukken. Het Verbond roept wetenschappers dan ook op hun ideeën voor de toepassing van deze data in te dienen.

7.4 Wetgevers en toezichthouders

Alle bovenstaande aanbevelingen zijn gericht op verzekeraars of zullen door het Verbond worden ingevuld. Aan toezichthouders en wetgevers wil het Verbond aanraden om geen nieuwe regelgeving te ontwikkelen. Te snel handelen om mogelijke nadelige gevolgen te voorkomen kan ook de kansen de kop in drukken.

"Zolang er nog geen echte problemen zijn, moet er nog geen nieuwe regelgeving ontwikkeld worden."

Natuurlijk zijn er zorgen, deels terecht, maar we constateerden in deze visie al dat Nederlandse verzekeraars in hun producten nog amper Big Data gebruiken. Het is nu dan ook niet nodig om in de bekende 'risico-regelreflex' te trappen. Regelgeving moet niet gebaseerd zijn op zorgen, maar op feiten. Regels stellen enkel op grond van zorgen, kan innovatie belemmeren en de goede kansen de kop indrukken.

8 Tot slot

Een paper over Big Data zonder 'wiskundige' formule is natuurlijk ondenkbaar. Daarom

sluiten we dit betoog af met een formule voor de acceptatie van Big Data-toepassingen. Big Data brengt immers grote beloftes met zich mee, maar duidelijk is dat het lastig is om een goede Big Data-toepassing te implementeren die alle hobbels met vlag en wimpel wegneemt. Om zeker te weten dat een Big Data-toepassing 'kan', is dus zeker niet alleen een juridische beoordeling voldoende. Dit brengt ons tot een Big Data-acceptatie-formule:

Acceptatieformule
De acceptatiebereidheid voor een Big Data-toepassing = klantvoordeel x openheid x voorspelbaarheid x compliance x juistheid x begrijpelijkheid x correctiemogelijkheden.

Klantvoordeel slaat op het vertrekpunt van de data-analyse: op het moment dat een toepassing aantoonbaar voordelen oplevert voor klant en maatschappij, zal de acceptatiebereidheid groter zijn. Openheid gaat over de mate waarin klanten weet hebben van het gebruik van data. Voorspelbaarheid gaat over de mate waarin klanten kunnen inschatten hoe hun data gebruikt worden. Compliance gaat over de vraag of de toepassing binnen de bestaande wettelijke kaders valt. Juistheid gaat over de vraag of klanten in het gebruikte model op hun eigen karakteristieken beoordeeld worden. Begrijpelijkheid gaat over de vraag of de verzekeraar het model kan uitleggen. Dat is ook nodig in verband met de correctiemogelijkheden, die klanten moeten hebben als het model hen verkeerd beoordeelt. Kortom, deze formule impliceert dat er regie is bij de klant en de klant grip houdt op zijn data.

Deze formule maakt gelijk duidelijk waarom de acceptatiebereidheid verschilt tussen diverse soorten bedrijven. De regels zijn voor iedereen gelijk, maar de perceptie van klanten verschilt nogal. Het gaat niet alleen om compliance, maar ook om wat klanten verwachten van een bedrijf. Daarom is het belangrijk voor verzekeraars om open en voorspelbaar te zijn als het gaat om Big Data-toepassingen. Hoop is dat dit paper heeft bijgedragen aan die transparantie.

Vragen of opmerkingen?

Mail dan naar info@verzekeraars.nl

"Ik denk dat de maatregelen die het Verbond aankondigt, een Solidariteitsmonitor en communicatietoets, erg waardevol kunnen zijn. Ik denk dat je hier te maken hebt met ontwikkelingen waarvan de impact pas echt zichtbaar wordt op het moment dat ze in de praktijk komen. Dan is experimenteren terwijl je oog houdt op maatschappelijke waarden zoals solidariteit en begrijpelijkheid een goede stap."

Jelte Timmer MA, onderzoeker bij het Rathenau Instituut