Interview met Arco van der Ven

Hora, tempus, en de toegevoegde waarde van IT-audit

8 september 2017

Het is een zonnige vrijdagmiddag als we op de groene campus van Universiteit Tilburg aanschuiven bij Arco van de Ven, nu negen jaar hoogleraar Bestuurlijke Informatievoorziening aan TIAS. Arco spreekt met een zekere bedachtzaamheid, maar vooral begeesterd, over politiek, technologie, complexiteit en de rol van IT-auditors.

Kun je om te beginnen iets over jezelf vertellen?

'Ik heb lang geleden Bestuurlijke Informatiekunde gestudeerd aan de Erasmus Universiteit. Na mijn militaire diensttijd, waarin ik les gaf aan de Hogere Krijgsschool, heb ik een tijd als zelfstandig consultant gewerkt. Daarna heb ik financiële functies vervuld, interim opdrachten gedaan, en eigenlijk heb ik het lesgegeven ook nooit losgelaten. Tijdens een sabbatical ben ik gepromoveerd. Vervolgens kreeg ik mijn leerstoel hier in Tilburg, en parallel daaraan was ik vier jaar hoogleraar Controlling aan de Open Universiteit. Daarnaast ben ik voorzitter van het curatorium van IT-audit en operational audit-opleidingen aan Erasmus in Rotterdam.'

En waar houd je je in grote lijnen zoal mee bezig?

'In mijn onderzoek, dat vooral gericht is op de financiële functie, ben ik vanuit het perspectief van corporate governance geïnteresseerd in risicomanagement. De *Actor-Network Theory* vind ik een vruchtbare invalshoek om dat terrein te bestuderen. Een sociale omgeving beschrijf je dan als een verknoping van mensen, systemen, en technologie. Wat je ziet is dat in die verknoopte wereld geprobeerd wordt complexe concepten terug te brengen tot een behapbare norm of score, maar niet altijd met succes. Een goed voorbeeld is de FICO-score voor kredietwaardigheid. Daarmee werd het ingewikkelde begrip van kredietwaardigheid teruggebracht tot een score, een getal. Je zou denken dat je vervolgens in je onderzoek een verband vindt tussen bedrijven die in default raken en hun FICO-score. Dat verband was er ook, maar precies andersom dan verwacht: juist bedrijven met hoge FICO-scores gingen failliet. Leningverstrekkers bleken de minder kredietwaardige bedrijven toch een adequate FICO-score te kunnen bezorgen. Ze deden dat door te sturen op de attributen van die score om zo de score kunstmatig omhoog te trekken.'

'Wat mij bezighoudt als het gaat over vraagstukken van de klassieke administratieve organisatie, is dat we gericht zijn op de vraag hoe het zou *moeten*. Maar de praktijk laat keer op keer zien dat dat niet is zoals het daadwerkelijk *gaat*. In alle literatuur over wetenschappelijk onderzoek in top management journals gaat maar iets meer dan twee procent ook over IT. Dat staat haaks op de enorme invloed van IT op operationele processen en de versnelling van die processen door IT. Lees vooral ook het artikel van Wanda Orlikovski uit 2010, waarin ze duidelijkheid schept over betekenis en belang van technologie in organisaties.[1] Haar werk vind ik boeiend omdat ze je anders laat kijken. Als ik de discussies in de Tweede Kamer beluister, dan denk ik: jullie snappen echt niet wat de implicaties van IT kunnen zijn, en je hebt een verkeerde voorstelling van waar het om gaat bij, bijvoorbeeld, stabiliteit. We hebben niet alleen te maken met ingewikkeldheid, maar ook met complexiteit. Om met complexiteit om te gaan heb je veel meer aan aanpasbaarheid en flexibiliteit dan aan de traditionele continuïteit (dus ook stabiliteit) en vertrouwelijkheid. Wat je dan nodig hebt zijn *loosely coupled systems* in plaats van geïntegreerde systemen. Dit staat haaks op de gangbare gedachte dat integratie goed is, omdat het tot efficiencyvoordelen leidt. Dat gaat lang niet altijd op. Ik denk dat we juist wat meer naar loosely coupled systems toe moeten, waarbij je in het ontwerp natuurlijk wel weer die samenhang moet inbouwen.

Herbert Simon gaf hiervan al in 1962 een goed voorbeeld in zijn parabel over Hora en Tempus, twee horlogemakers die beiden een even ingewikkeld horloge leveren, samengesteld uit duizend componentjes.[2] Iedere keer dat Tempus de telefoon moet opnemen om een klant te woord te staan, valt zijn horloge uit elkaar en moet hij helemaal van voren af aan beginnen. Hora, de andere horlogemaker, is veel slimmer. Hij maakt zijn horloges door tien onderdelen samen te voegen tot een module. Tien van die modules vormen samen weer een groter geheel, et cetera. Het resultaat is dat hij bij een onderbrekend telefoontje hoogstens de laatste tien componentjes opnieuw in elkaar moet zetten en dus veel minder tijd nodig heeft om het complete horloge te assembleren.'

'Maar hoe komen we nu tot zulke losjes gekoppelde systemen? De politiek begrijpt niet hoe dat moet. De kern is dat je omvangrijke systemen opknipt. En dat je keuzes maakt over de verbanden tussen die kleinere onderdelen: wat koppel je wel met elkaar en wat niet. Elk project dat langer dan twee jaar duurt moet je gewoon verbieden. Van zo'n project weet je van tevoren al dat het zijn dynamische omgeving niet zal bijhouden. Kaplan en Mikes bieden een aanknopingspunt met hun model met verschillende soorten risico's. Zo zijn er *preventable risks*, risico's die je tot op zekere hoogte rationeel kunt benaderen. Daar zijn traditionele risicoanalyses op gebaseerd, je kunt er maatregelen voor nemen en een auditor kan die maatregelen toetsen. Maar daarnaast onderscheiden ze *strategic risks* en *external risks*. Dat zijn risico's die zich niet zo gemakkelijk laten inschatten of bediscussiëren. Toch moet je ook met die risico's rekening houden. Dat zou je kunnen doen met prototyping of, in IT-termen, met Agile-processen. Als je dan ziet gebeuren wat de overheid doet, dat die per 1 januari drie decentralisaties gelijktijdig gaat uitvoeren, en wel in één keer

meteen landelijk. Dan snap je van tevoren al dat zoiets gewoon niet haalbaar is. Dat hele veranderproces vloeit voort uit het uitgangspunt dat wetgeving en uitvoering volgtijdelijke processen zijn. Een wet wordt op een bepaald moment vastgesteld en pas daarna wordt er bekeken of die wel uitvoerbaar is – vaak niet eerder dan wanneer het schip is gestrand. Met zo'n insteek vraag je om mislukking. Uitvoerbaarheid komt niet na het ontwerp, maar moet er *onderdeel* van zijn. Al in de ontwerpfase moeten deskundigen meedoen die uitvoerbaarheid ter discussie kunnen en durven stellen. Maar zo zit het politieke proces niet in elkaar.'

'Waar het uiteindelijk om moet gaan is dat een organisatie *public value* realiseert, dat wil zeggen dat de burger beter wordt van wat je doet. Dat bereik je niet als je blijft proberen volgens de standaard control-principes processen dicht te regelen. Het mooie van public value, een stroming met als voortrekker Michael Moore, is dat bij elke beslissing steeds de maatschappelijke waarde voorop staat. Dat is een buitengewoon krachtig richtinggevend principe. Ik ben momenteel betrokken bij een pilot voor de PO-Raad, de sectororganisatie voor het primair onderwijs. Toen we met ze gingen praten bleken ze voor hun risicoanalyses als vanzelfsprekend de standaard risicomanagementinstrumenten te hebben omarmd. Ik vroeg ze: gaan de kinderen hier beter door leren? Want dat is waar de sector voor staat, dat is hun publieke waarde! En die cruciale vraag konden ze nu net niet beantwoorden. Wat een organisatie moet doen is haar doelstelling en de bovenliggende public value uit elkaar halen. Door dat te doen ga je terug naar de basis: waar doen we het ook al weer voor? Daarmee krijgt de discussie een heel nieuwe dynamiek. En dat spreekt aan.'

Je had het daarnet over ingewikkeldheid en complexiteit. Is dat eigenlijk niet hetzelfde?

'Nee, complexiteit is wezenlijk anders dan ingewikkeldheid, en met het een moet je principieel anders omgaan dan met het ander. Met ingewikkeldheid bedoel ik dat iets uit een groot aantal entiteiten bestaat, die allemaal met elkaar samenhangen. Neem als voorbeeld een zwerm vogels. Zo'n zwerm kan bestaan uit een paar honderdduizend exemplaren. Het gedrag ervan kun je beschrijven met een verzameling vaste regels. Die regels gelden niet alleen op dit moment, ze gelden straks nog steeds en over een paar jaar ook nog. Bij complexiteit is dat fundamenteel anders. Complexiteit ontstaat wanneer entiteiten, actoren, op elkaar reageren. Een mooi voorbeeld vind ik de mobiele telefoon. In de jaren negentig waren er nog mensen die zeiden: hoezo een mobiele telefoon, dan stuur ik toch gewoon een brief? De vraag is: had je op dat moment de komst van de iPhone kunnen voorspellen? Misschien was wel te voorzien dat er ongeveer zo'n device zou komen. Maar hoe Facebook daarop zou inspelen, hoe de telefoonfabrikanten vervolgens weer rekening gingen houden met de functionaliteit die daarvoor nodig is en hoe op hun

beurt consumenten die ontwikkelingen omarmden, dat is een hele nieuwe dynamiek. Die dynamiek van hoe partijen precies op elkaar reageren – en dat is de kern van complexiteit – die is nu eenmaal veel lastiger te voorspellen.'

Wat betekent dit voor de IT-auditor?

'IT-auditors bevinden zich op vertrouwd terrein als het gaat om ingewikkelde systemen. Daar zijn ze goed in. Voor ingewikkelde systemen kunnen organisaties protocollen schrijven. IT-auditors kunnen daar dan normen uit halen en er vervolgens op toetsen. Dan kun je als IT-auditor prima in die toetsende rol blijven zitten. Vanuit de derde lijn, in termen van de three lines of defense, kun je dan zeggen: dít is goed geregeld en dát niet. Als organisatie loop je deze risico's, et cetera. Denk aan onderwerpen als toegangsbeveiliging, single sign-on, dat soort zaken. Nog steeds zijn er medewerkers die een zogenaamd verloren USB-stick op straat zien liggen, hem oppakken en vervolgens op kantoor in de computer steken. En ik ken een grote organisatie waar twee gebruikers, die hoge systeembevoegdheden hadden, waren vertrokken. Pas twee maanden later kwam de organisatie erachter dat hun accounts met alle bijbehorende toegangsrechten nog steeds actief waren. Al dat soort klassieke stompzinnigheden komt nog steeds voor. En het wordt steeds urgenter om ze te bestrijden naarmate cloud computing toeneemt en de kans dat iemand bij je data komt groter wordt dan als dat 'doosje' binnen de eigen organisatie staat. Een IT-auditor kan op dit soort terreinen nog steeds bijzonder nuttige bijdragen leveren. Je bezighouden met die dingen waar je vooraf over na kunt denken, waarvan we wéten dat het fout gaat, dat blijft dus belangrijk voor IT-auditors.'

'Maar neem nu zoiets als de Diginotar-affaire. Had je die als IT-auditor ook kunnen zien aankomen? Kun je dit soort toestanden niet voorzien door vooraf goed te doordenken wat er allemaal kan geburen en daar (beveiligings)protocollen en normen voor opstellen? Waarschijnlijk niet. Dit zijn situaties waarin simpelweg geldt: zij vallen aan en wij moeten ons verdedigen. Daar kun je geen protocollen voor schrijven, geen normen voor opstellen. Het is een kat en muisspel tussen hackers en beveiligingsexperts. Die partijen spelen op elkaar in, waardoor een complex proces ontstaat dat door zijn aard onvoorspelbaar is. De IT-auditor staat in zo'n geval al bij voorbaat met lege handen, met alle protocollen en normen die hij ter beschikking heeft. Wat betekent dit voor de IT-auditor? Kan die zich dan niet met dit soort complexe vraagstukken bezighouden? De praktijk is inderdaad dat IT-auditors ervan weg blijven, maar dat is niet mijn conclusie. Het moet anders kunnen. Daarvoor is het nodig dat IT-auditors nadenken over hun rol bij complexe vraagstukken.'

En in welke richting denk jíj dan?

'Neem bijvoorbeeld die hackers, die kun je niet bestrijden met betere protocollen. Ik denk dat je dit soort complexe bedreigingen alleen kunt aanpakken in teams. Je moet samen met de eerste lijn meedraaien en er met zijn allen voor zorgen dat je er zo snel mogelijk achter komt dat een aanval gaande is. Vervolgens moet je, ook weer samen, kijken wat je kunt doen om de aanval in te dammen en de schade te minimaliseren. Met je voeten in de modder staan. Dat is dus een heel andere rol dan die van de klassieke afstandelijke, objectieve IT-auditor. Of je dit ook IT-audit wilt noemen, weet ik niet. Dat vind ik eigenlijk ook helemaal niet zo'n interessante vraag – mij gaat het er vooral om hoe een IT-auditor effectief kan zijn. Dit is een geheel andere benadering dan wat je tegenkomt in de klassieke IT-audithandboeken, in AO-boeken en in boeken over interne beheersing. Die zitten allemaal op de lijn van controles door toetsen aan een norm en op basis daarvan assurance afgeven. Het achterliggende idee is dat je risico kunt voorkomen door vooraf goed na te denken en dan maatregelen te treffen. En voor een deel blijft dat valide, maar als het gaat over snelheid, complexiteit, het onbekende, dan móet je naar een andere benadering toe. Vergelijk het maar met als je in een oorlogssituatie bent waar de eerste en de tweede lijn zijn uitgeschakeld. Wat doe je dan als de vijand eraan komt? Loop je naar de commandopost en zeg je: de vijand komt eraan, daar is-ie? Of ga je vechten? Dus, kijkend naar dat onafhankelijke oordeel of iets goed of niet goed is, moeten we dan niet juist de gecombineerde kennis van een IT-auditor en een echte IT-er in een team hebben zitten om dat te signaleren? Het is de IT-er die iets aan de situatie kan doen, maar die heeft wel het signaal van de IT-auditor nodig. Samen kun je er als team voor zorgen dat een aanval niet alleen gesignaleerd wordt maar ook wordt afgeslagen. Dit leidt niet tot minder nadruk op de onafhankelijkheid van de IT-auditor, wel tot meer doelgericht en in teamverband inzetten van diens oordeel.'

'En denk nu niet dat ik het alleen over beveiliging heb. Neem een compleet ander onderwerp, de algoritmes die allerlei organisaties gebruiken. Bijvoorbeeld algoritmes die zoekcriteria gebruiken om (potentiële) klanten aanbiedingen te doen. Dan is de vraag: hoe weet de organisatie dat die zoekcriteria werken? Dat die aanbiedingen goed staan? Het moet allemaal snel ontwikkeld worden en dat is riskant. En het zijn techneuten die aan de slag gaan: die beginnen, plat gezegd, gewoon code in te kloppen. Hoe kun je er als IT-auditor nu voor zorgen, samen met de eerste lijn, dat het een proces wordt met een bepaalde controleerbaarheid? Bijvoorbeeld in de vorm van een change managementprocedure, of dat in ieder geval een tweede ontwikkelaar zo'n algoritme test voordat het wordt vrijgegeven? Je wilt als organisatie immers zeker weten dat die korting alleen maar gegeven wordt aan wie die korting verdient.'

Is het niet zo dat we een wereld aan het creëren zijn die van schijnzekerheid aan elkaar hangt?

'In de wereld van *preventable risks* wel. Er gaat iets mis, daarom willen we meer transparantie hebben, daartoe verzinnen we regels, en de auditor moet controleren of die regels worden nageleefd. En die cyclus gaat maar door – grosso modo komt er meer regelgeving bij dan er verdwijnt. We patchen de onvolkomenheden die we hebben gecreëerd met aanvullende regels, want dat vinden we gemakkelijk. En zo raken we gevangen in een spiraal van steeds hogere, verlammende regeldichtheid. De drijvende kracht hierachter is legitimiteitsdruk. Om legitimiteit te behouden moeten bestuurders en toezichthouders iets doen. En als legitimiteitsbewijs wegen risicoanalyses en het nemen van acties om risico's te beperken nu eenmaal zwaarder dan het halen van een doelstelling.'

'Tot een keer de bom barst. Over de productiegroei is wereldwijd de voorspelling dat die de komende jaren kleiner zal zijn dan de groei van de consumptie. Met andere woorden, de productie zal de snelheid van de consumptiegroei niet meer kunnen bijhouden. Dat leidt hoe dan ook tot een nieuwe welvaartsverdeling. China en India krijgen meer, wij minder. Dat zie je nu al gebeuren, maar de echte consequenties zullen niet voor jou en mij zijn, maar voor onze kleinkinderen.'

'Dat is het plaatje op macroniveau. Op het microniveau waar we daarnet op zaten, dat van maatregelen voor risicobeheersing, denk ik dat het probleem niet zozeer is dat er in absolute zin *teveel* maatregelen worden getroffen. Het probleem is vooral dat teveel van de maatregelen *niet effectief* zijn. Die moeten eruit. Maar welke maatregelen zijn dat dan? Dat kan een IT-auditor niet in zijn eentje beslissen. Daar moet je via discussie met de eerste en tweede lijn zien uit te komen. Zo bezien heeft de IT-auditor meer een procesrol: zorg ervoor dat de juiste discussie wordt gevoerd.'

Tot slot: wat is in het kort je boodschap voor IT auditors? Wat moeten we anders of beter doen?

'Laat me even nadenken… Waar het op neerkomt is het volgende. Benader normen, standaarden en protocollen vooral kritisch. Vraag je af of, gegeven de problematiek, hun inhoud een organisatie kan helpen om haar doelen te bereiken. Stel jezelf bovendien de vraag of er in complexiteitsvraagstukken überhaupt wel van een norm sprake kan zijn.'

Vervolgens haast Arco zich naar een begeleidingsgesprek met een afstudeerder, ons enigszins contemplatief, met huiswerk, maar wel in het zomerzonnetje achterlatend.

Noten

[1] Wanda J. Orlikovski, 2010, The sociomateriality of organizational life: considering technology in management research. *Cambridge Journal of Economics*, Vol. 34, No. 1 (Jan. 2010), pp. 125-142.

[2] Herbert A. Simon, 2010, The Architecture of Complexity, *Proceedings of the American Philosophical Society*, Vol. 106, No. 6 (Dec. 12, 1962), pp. 467-482.

Drs. Th. (Thomas) Wijsman RE en Ed Ridderbeekx

Thomas Wijsman werkt zelfstandig als coach en strategisch adviseur/onderzoeker. Ed Ridderbeekx is werkzaam als zelfstandig IT-auditor en is lid van de redactie.