Mine!

Over toezicht, vertrouwen en technologie

Roos Lindgreen, E.

Publication date
2019

Document Version
Final published version

Mine!

Mine!

Over toezicht, vertrouwen en technologie

Rede

uitgesproken ter gelegenheid van de aanvaarding van het ambt van
hoogleraar Data Science in Auditing
aan de Faculteit der Economie en Bedrijfskunde
van de Universiteit van Amsterdam
op vrijdag 30 november 2018

door

Edo Roos Lindgreen

Dit is oratie 602, verschenen in de oratiereeks van de Universiteit van Amsterdam.

Opmaak: JAPES, Amsterdam

Mevrouw de Rector Magnificus,
Mijnheer de Decaan,
Hoogleraren van de Universiteit van Amsterdam en zusteruniversiteiten,
Waarde collega's en studenten,
Familie, vrienden,
Allen die door uw aanwezigheid blijk geven van uw belangstelling,

Inleiding

Het oog van de meester maakt het paard vet. Kent u die uitdrukking? Ik moest eraan denken toen ik dit verhaal begon te schrijven. Ook Martin Luther kende deze uitdrukking. Hij maakte in 1542 een financieel overzicht bij zijn testament, die Hausrechnung.[1] In de kantlijn schreef hij: "Das Pferd wohl fein gefüttert wird, wo ihm sein Herr die Augen gibt". Het betekent zoveel als: als de baas toezicht houdt, gaat alles beter.

Luther had deze *meme* niet zelf bedacht. De oude Grieken gebruikten hem voor het eerst. Hij komt bijvoorbeeld voor in Oikonomika[2], toegeschreven aan leerlingen van de Griekse wijsgeer Aristoteles die het geschrift onder zijn naam publiceerden, en eerder in een discussie van Socrates in het boek Oikonomikos van de Griekse schrijver Xenofon.[3] Hierin zegt de landeigenaar Isomachos vrij vertaald tegen Socrates: "Als je wilt dat je werknemers zorgvuldig zijn, moet je toezicht houden op het werk dat ze doen; toetsen, onderzoeken, onder de loep nemen. Je moet goed werk belonen en nalatigheid bestraffen. Vergelijk het met dat verhaal van de koning en de Pers, je kent het denk ik wel. De koning had een goed paard en wilde het dier snel laten groeien, dus hij vroeg aan een ervaren paardenfokker uit Perzië: 'Hoe krijg ik zo snel mogelijk vlees aan dat paard?'. Waarop die antwoordde: 'Door het oog van de meester.' Als je verborgen kwaliteiten naar boven wilt halen en die tot iets moois en goeds wil laten uitgroeien, gaat er niets boven het oog van de meester." Dat beweerde die Isomachos.

Het oog van de meester maakt het paard vet. Een Middeleeuws cliché over toezicht, in de kantlijn van een huishoudboekje gekrabbeld door Luther, geleend van Aristoteles, die het weer van Xenofon had, die het vast ook niet zelf

bedacht had. Een *meme* die al duizenden jaren meegaat, daar moet wel een kern van waarheid inzitten, zou je denken.

Volgens een nog steeds veelgebruikte definitie van de Algemene Rekenkamer van twintig jaar geleden is toezicht "het verzamelen van de informatie over de vraag of een handeling of zaak voldoet aan de daaraan gestelde eisen, het zich daarna vormen van een oordeel daarover en het eventueel naar aanleiding daarvan interveniëren".[4]

Dat is een brede definitie. En inderdaad, toezicht is overal. Van de gemeente die het geluidsniveau meet van een nieuw café tot de accountant die een jaarrekening goedkeurt. Van ouders die in de gaten houden of hun kinderen wel naar school gaan tot de Raad van Commissarissen van een beursgenoteerde onderneming. Van de APK-keuring van een twintig jaar oude Volvo tot de ECB die banken controleert. Van de fietscoach voor het universiteitsgebouw tot de politiepost voor de synagoge. Toezicht is verweven met onze samenleving en is onmisbaar voor het functioneren ervan. Toezicht is ook een essentieel onderdeel van de cybernetische cyclus binnen organisaties. Toen de Amerikaanse consultant W. Edwards Deming na de Tweede Wereldoorlog de autofabrikant Toyota hielp bij de wederopbouw en groei en kwaliteitsverbetering, voerde hij de inmiddels beroemde cyclus Plan, Do, Check, Act in – kort samengevat: maak een plan, voer het uit, evalueer de resultaten, stuur bij, begin opnieuw. Deming had deze cyclus van zijn leermeester, de fysicus Walter Shewhart.[5] De derde stap, Check, wordt algemeen geïnterpreteerd als: houd toezicht, controleer, audit. Deming bedoelde het overigens breder: bestudeer, analyseer en leer van je bevindingen.

Laten we het eens over het paard hebben. Hoe is het om onder toezicht te staan? Los van het gevoel dat de meeste mensen hier bij hebben, en los van de wereldliteratuur die hierover geschreven is,[6] is er genoeg wetenschappelijk onderzoek waaruit blijkt dat mensen wel varen bij een relatief hoge mate van autonomie en vrijheid en vertrouwen, en dus bij een lage mate van toezicht.[7] Te veel toezicht maakt mensen ongelukkig; wie voortdurend onder toezicht staat, gaat zelfcensuur toepassen: het "chilling effect".[8] In de digitale samenleving zijn er voorbeelden genoeg. Werknemers, bespied door een baas die voortdurend hun aanwezigheid, productiviteit en performance aan het meten is.[9] Burgers die niet kunnen ontsnappen aan het wakend oog van een achterdochtige overheid. Ook organisaties kunnen verlamd raken door een teveel aan toezicht. Zij komen in een staat waarin mensen alleen nog maar bezig zijn met compliance, voldoen aan regels en richtlijnen, angstig op de gebaande paden blijven, en vervallen in geconditioneerde reflexen of zelfs totale apathie. Ook hiervan zijn er genoeg voorbeelden en er zijn vast mensen in deze kerk, die dit beeld herkennen.

Toezicht heeft dus twee gezichten. Als je er van uit gaat dat toezicht in één dimensie is uit te drukken, en het effect van toezicht ook, dan is er een optimum: te weinig toezicht is niet goed, maar teveel ook niet. Kennelijk ligt er ergens een optimum. In werkelijkheid is het natuurlijk niet zo eenvoudig. Toezicht is meerdimensionaal en dynamisch en de effecten ervan ook.

De filosoof Philip Pettit gaf vorige maand tijdens de Amsterdam Privacy Conference een lezing over vrijheid en privacy die diepe indruk maakte op het publiek. Volgens Pettit zijn er twee soorten vrijheid: laissez-faire, ofwel het afwezig zijn van inmenging (het neoliberale model) en het afwezig zijn van dominantie: je bent vrij als niemand macht over jou heeft (het neorepublikeinse model). Wetten geven vrijheid, aldus Pettit. Wetten zorgen ervoor dat iedereen gelijk is, dat niemand boven een ander staat. Maar zonder toezicht zijn wetten waardeloos. Dus toezicht geeft vrijheid. Tegelijkertijd geldt: wie toezicht houdt, heeft macht. En wie macht heeft over een ander, beperkt daarmee diens vrijheid. Dus toezicht geeft vrijheid, juist door vrijheid te beperken. Dat vond ik een mooie gedachte.

Toezicht is altijd sterk beïnvloed door technologische ontwikkelingen. Degenen die toezicht willen of moeten houden maken graag gebruik van de mogelijkheden die de technologie ze biedt. Omgekeerd wordt er ook technologie speciaal ontwikkeld om toezicht te kunnen houden: de ponskaart, de flitspaal, de enkelband, het leerlingvolgsysteem, de beveiligingscamera, de spionagesatelliet. Technologie om toezicht te houden.

De ontwikkeling van die technologie is de afgelopen tien jaar in een bizarre stroomversnelling geraakt. Natuurlijk, we kennen allemaal de Wet van Moore uit 1965, die zegt dat het aantal transistoren op een chip zich elke achttien maanden verdubbelt.[10, 11] We weten ook dat daarmee hetzelfde geldt voor de rekenkracht, bandbreedte en opslagcapaciteit van computersystemen en netwerken. En we weten inmiddels ook allemaal wel dat de Wet van Moore tegen zijn grenzen aanloopt, maar dat de industrie daar dan toch weer een list op bedenkt, zodat de volgende smartphone toch weer sneller is dan de vorige, en dat er de afgelopen twee jaar evenveel data is geproduceerd dan in alle jaren daarvoor, enz.

Het is niet makkelijk om je voor te stellen wat deze capaciteitsexplosie in de praktijk betekent. Wie weet er hoeveel bytes er door het internet vliegen tijdens dit uurtje? Niemand, maar Cisco denkt een triljoen, een miljard miljard, a million trillion (1.000.000.000.000.000.000).[12] Hoeveel bytes zijn er opgeslagen in de datacenters van Google? Niemand weet het en Google wil het niet zeggen, maar het zijn er superveel, bijvoorbeeld honderd triljoen (100.000.000.000.000.000.000). Hoeveel berekeningen worden er het komende half uur uitgevoerd door bitcoin miners over de hele wereld om de

volgende drie blokjes in de bitcoin blockchain te vinden? Honderdduizend triljoen (100.000.000.000.000.000.000.000).[13] Dit soort getallen gaat het menselijk voorstellingsvermogen ver te boven.

We drukken complexe technologische innovaties graag uit in pakkende Engelse termen: algorithms, analytics, artificial intelligence, big data, blockchain, internet of things, machine learning, quantum computing, robotics. Technologieleveranciers en consultants werken hier graag aan mee; als een buzzword aanslaat, dan kun je daar nog jaren commercieel plezier aan beleven. En als een term weer uit de mode raakt, dan wordt de bijbehorende technologie even makkelijk gerebrand, opnieuw verpakt en aan de man gebracht, als oude wijn in nieuwe zakken. Kijk je door het jargon heen, dan zie je een technologisch ecosysteem dat zelfs voor deskundigen nauwelijks meer te bevatten is, een wereldomspannende machine waarin honderden miljarden worden geïnvesteerd en waarmee enorme commerciële, maatschappelijke, militaire en politieke belangen zijn gemoeid.

Wat is de impact van deze technologische ontwikkelingen op toezicht? Wat betekent dit voor mensen, organisaties, samenlevingen? Kunnen we technologie gebruiken om het gewenste optimum te bereiken en vast te houden? Welke rol speelt vertrouwen daarbij? En hoe houden we eigenlijk toezicht op de technologie zelf?

Ofschoon mijn leeropdracht zich beperkt tot de rol van technologie en data in het vakgebied auditing, heb ik behoefte om het onderwerp vandaag in iets breder perspectief te plaatsen. Het komende half uur wil ik eerst met u kijken naar de impact van technologie op onderdelen van toezicht in brede zin. Daarna wil ik met u inzoomen op auditing als deelgebied van toezicht.

Toezicht

In de aanloop naar deze oratie heb ik aan veel mensen gevraagd: waar denk je aan bij het woord toezicht? De antwoorden vielen grofweg in drie categorieën: openbare orde en veiligheid, markttoezicht, en toezicht op ondernemingen.

Openbare orde en veiligheid

De meeste respondenten dachten bij het woordt toezicht aan openbare orde en veiligheid: surveillanten, bewakers, beveiligers. Of aan de camera's die nu overal hangen en waar we altijd fel op tegen waren maar waar uiteindelijk bijna niemand meer van wakker ligt. Misschien denkt u wel aan de politie. Misschien liep u wel tegen de lamp bij een trajectcontrole, en kreeg u vorige

week volledig geautomatiseerd een ouderwets papieren bekeuring in de bus, zoals ik.

Als er één categorie professionals is die technologie en data hebben ontdekt, zijn het de opsporings- en inlichtingendiensten. De AIVD hackte in 2017 de beveiligingscamera's van Russische spionnen die de systemen van de Democratische Partij in de Verenigde Staten hadden gehackt.[14] Ook de opsporingsdiensten zitten niet stil. In een recent artikel in het Financieel Dagblad vertelt de baas van de Fiscale Opsporings- en Inlichtingendienst (FIOD) hoe zijn dienst criminele digitale geldstromen in kaart brengt, om zo uit te komen bij partijen in de bovenwereld die criminaliteit mogelijk maken, de zogenaamde facilitators – notarissen, accountants, banken. Voor sommige diensten is digitaal rechercheren de normaalste zaak van de wereld. Voor andere diensten nog niet, blijkt uit een recent rapport van de Nederlandse Politiebond (NPB), getiteld NOODKREET RECHERCHE.[15]

Misschien denkt u wel aan "predictive policing": systemen die een misdaad kunnen voorspellen voordat deze plaatsvindt, zoals in de klassieke science fiction-film Minority Report. Met zulke systemen wordt volop geëxperimenteerd.[16] De resultaten zijn op zijn zachtst gezegd weinig bemoedigend. De evaluatie van een experiment met predictive policing in de Amerikaanse stad Shreveport wees uit dat het systeem niet meetbaar bijdroeg aan het verlagen van criminaliteit en dat agenten het systeem na een paar maanden niet meer gebruikten.[17] Een mogelijke verklaring voor dit laatste is dat het systeem niets toevoegde aan de heat maps die het politiekorps toch al aan de muur had hangen: de slechte buurten waren al bekend. Een andere verklaring is het effect van false positives en false negatives. In de praktijk geven predictive policing-systemen nog te vaak het sein "all clear", waarna er alsnog een rel uitbreekt of een overval plaatsvindt. Ook worden agenten af en toe voor niets op pad gestuurd. De geloofwaardigheid van het systeem daalt dan snel en agenten gaan weer over tot de orde van de dag. Behalve hun onbetrouwbaarheid hebben predictive policing-systemen ook last van andere uitdagingen. Bijvoorbeeld de *bias* die kan ontstaan door het systeem te trainen op basis van vervuilde historische data, of bepaalde categorieën data wel of juist niet in de trainingssets op te nemen. Tenslotte is het effect van deze systemen moeilijk te meten. Stel dat de criminaliteit in een buurt daalt, komt dat dan door de invoering van zo'n systeem of zijn er andere oorzaken? Ondanks alle tekortkomingen zijn politiekorpsen over de hele wereld met deze systemen aan de slag gegaan. In een recent artikel in Nature wordt daarom opgeroepen tot meer transparantie en meer toezicht op deze vorm van toezicht.[18]

Markttoezicht

Misschien denkt u bij het woord toezicht wel aan toezicht op de financiële markten, zoals uitgeoefend door Europese Centrale Bank (ECB), De Nederlandsche Bank (DNB) of de Autoriteit Financiële Markten (AFM). Of andere markten, zoals de consumentenmarkt, bewaakt door de Autoriteit Consument en Markt (ACM), of de voedsel- en warenmarkt, gecontroleerd door de Nederlandse Voedsel- en Warenautoriteit (NVWA). Hoe gaan deze traditionele, bij wet ingestelde toezichthouders om met technologie? In hun jaarverslagen geven ze een redelijk consistent beeld van zichzelf: ze zijn goed op de hoogte van de manier waarop technologie binnen hun markten wordt ingezet, en houden daar ook toezicht op. Ze houden de vinger aan de pols, maken beleid, hebben specialisten in dienst, grijpen in. Zo investeerde de AFM in 2017 in technologieën en technieken om datagedreven toezicht te kunnen uitoefenen, voerde pilot-projecten uit, deelde databronnen met andere toezichthouders, en voerde 140 digitale onderzoeken uit.[19] De ACM deed onderzoek naar de betrouwbaarheid van online reviews en voerde een consumentencampagne over online verkopen op social media, en maakte gebruik van het recht om bestanden van de mobiele telefoons van medewerkers van onderzochte bedrijven te kopiëren.[20] Dus onze toezichthouders zijn goed bezig, vinden ze zelf. Maar het zou overdreven zijn om te zeggen dat ze even super high-tech en data-driven te werk gaan als de AIVD. Ondanks alle positieve berichten in de jaarverslagen schat ik zo in dat voor onze toezichthouders hetzelfde geldt als voor de Nationale Politie en elke andere organisatie: het adopteren van nieuwe technologie en het overschakelen op een nieuwe manier van werken kost tijd en moeite, kost geld, vergt het aanpassen van processen en systemen en stuit op weerstand bij de huidige generatie medewerkers, die het toch al enorm druk hebben; bovendien is het door de krapte op de arbeidsmarkt moeilijk om deskundige nieuwe medewerkers aan te trekken. Maar de belangrijkste reden is misschien wel dat toezicht niet gaat over data, maar over mensen. De tussentijdse conclusie? Toezicht op markten is vooral toezicht op mensen en door mensen, waarbij de mens af en toe een handje wordt geholpen door de technologie.

Toezicht op ondernemingen

Misschien denkt u bij toezicht wel aan corporate governance, een raad van commissarissen die toezicht houdt op de uitvoering van het beleid door de raad van bestuur. Over de relatie tussen technologie en deze overwegend mannelijke beroepsgroep met een gemiddelde leeftijd van 59 jaar is helaas

nog weinig te zeggen.[21] Er lijkt iets moois te ontstaan maar de relatie is nog altijd erg pril. Uit recent onderzoek door een bekend bureau voor executive search blijkt dat in 95% van de 300 onderzochte boards van beursgenoteerde ondernemingen geen aantoonbare digitale expertise aanwezig is, ook niet in Nederland.[22] De technologiesector scoort met een percentage van 43% aanzienlijk hoger. Die verhouding roept wel vragen op als je kijkt naar de ontwikkelingen in de economie en het tempo waarmee technologiebedrijven de markt en de macht overnemen. Immers, eén van de taken van een rvc is erop toe te zien dat het bestuur van de onderneming zorgt voor het creëren van waarde op de lange termijn en tegelijkertijd de risico's goed beheerst. De belangrijkste risico's die een onderneming loopt, blijken strategisch van aard, en een belangrijk deel van die strategische risico's heeft te maken met digitalisering. Je zou zeggen dat dit vraagt om digitale expertise, niet alleen in het bestuur, maar ook in de rvc. In 95% van de gevallen denkt de voorzitter van de rvc daar dus anders over. De vraag is hoe dit komt – digitalisering is immers niet iets van de afgelopen maanden. Daar geeft het rapport helaas geen antwoord op. Maar de conclusie is duidelijk: er moet meer digitale expertise komen in de raad van commissarissen.

Technologie

Nu komen drie aan technologie gerelateerde onderwerpen aan de orde die voor toezicht relevant zijn: big tech, AI en crypto.

Big tech

Een discussie over toezicht en technologie moet bijna wel beginnen met de rol van "big tech": Microsoft, Apple, Google, Facebook, Amazon, samen goed voor bijna 4 biljoen euro.[23] Zoals iedereen nu wel weet houden deze bedrijven ons doen en laten 24 uur per dag in de gaten. Bekijk even je timeline op Google Maps: je kan precies zien waar je de afgelopen jaren geweest bent. Google weet ook nog met wie, en waarom.

Volgens de twintig jaar oude definitie van de Algemene Rekenkamer zijn deze grote technologiebedrijven niets minder dan toezichthouders. Ze observeren, ze trekken conclusies en ze plegen interventies, onder meer door ons gedrag te beïnvloeden met advertenties, nieuwsberichten en suggesties.

Ons leven speelt zich af in het digitale domein. Cyberspace en meatspace zijn één geworden. Ik ben al een cyborg. Mijn smartphone is altijd bij me. De

sporen die ik achterlaat, zijn veel meer dan kruimeltjes data. Ze vertellen een verhaal: het verhaal van mijn leven, een dagboek, van seconde tot seconde. Waar ben ik? Met wie? Wat doe ik daar? Het dagboek is enorm waardevol, niet alleen voor mij, maar ook voor anderen.

Van wie is dat dagboek? Van mij natuurlijk, en alleen van mij. Ik schrijf dat verhaal, elke dag, en alleen ik heb de rechten op dat verhaal. Niet Google of Apple of een of ander louche marketingbureau. Als ik een dagboek bijhoud met een schrijfmachine van Remington, dan is het verhaal toch ook niet opeens van Remington?

Op de Web Summit, een enorm technologiecongres in Lissabon deze maand, waren er – voor het eerst op grote schaal – zeer kritische geluiden te horen over het huidige internet en de rol van de grote technologiebedrijven. De heersende gedachte is: hun invloed is te groot geworden. Tim Berners-Lee, de bedenker van het web, noemde het internet "broken" en de manier waarop wij er mee omgaan "dystopisch".[24] Hij stelt een wereldwijde gedragscode voor. Zelfregulering dus. Facebook-oprichter Mark Zuckerberg schreef een paar weken geleden een wat warrige blog met een blauwdruk voor toezicht op content. De essentie: we gaan AI gebruiken om proactief onwenselijke content zoals clickbait en desinformatie te censureren.[25] Volgens velen gaat zelfregulering niet ver genoeg. De toonaangevende Amerikaanse hoogleraar Helen Nissenbaum zei het vorige maand op de Amsterdam Privacy Conference nog stelliger: technologiebedrijven hebben elk recht op zelfregulering verspeeld. Ze moeten en zullen gereguleerd en onder toezicht gesteld worden, en Canada en Europa zullen daarbij voorop lopen. Margrethe Vestager, Eurocommissaris Mededinging, is waarschijnlijk nog niet klaar met de Frightful Five.

Artificial Intelligence

Misschien denkt u bij technologie wel aan AI en machine learning. Als we de kranten mogen geloven koersen we in een noodtempo af op een samenleving waarin intelligente algoritmen de dienst uitmaken. AI is booming. Op arXiv.org – een e-print service voor wetenschappelijke artikelen, beheerd door Cornell University – zijn elke 18 maanden twee keer zoveel research papers over AI te vinden. Overal ter wereld schieten AI-onderzoekscentra als paddenstoelen uit de grond. De gemeente Amsterdam investeert 4 miljoen euro in zo'n centrum op het Science Park in de Watergraafsmeer.[26] Ook benoemt deze universiteit vier universiteitshoogleraren op het gebied van AI. In Cambridge, Massachusetts, deed MIT daar nog een klein schepje bovenop met een investering van 1 miljard dollar.[27] En dat is te begrijpen: AI en machi-

ne learning zijn fascinerende onderzoeksgebieden met een enorm scala aan toepassingen in vrijwel alle sectoren.

AI bestaat al meer dan 50 jaar en is daarmee veel ouder dan de meeste mensen denken. De eerste AI-onderzoekers waren vooral geïnteresseerd in het modelleren en structureren van gesprekken en mentale processen om die vervolgens in software te kunnen nabootsen. Die pogingen waren meer charmant dan succesvol, zoals met de online therapeut Eliza uit 1966. Maar het was de enige aanpak die op dat moment mogelijk was: rekenkracht was kostbaar en data was schaars. Door de beschikbaarheid van goedkope rekenkracht en de overvloed aan data werd een andere, ongestructureerde aanpak mogelijk: deep learning. Hierbij heeft het systeem geen kennis over de structuur van het proces. Het is een black box die je dingen kunt leren door het te voeden met enorme hoeveelheden data. Dat levert soms extreem goede resultaten op voor deelgebieden als spraakherkenning, beeldverwerking, classificatie of suggesties. Soms ook niet, zoals bij de robot Sophia. Het ziet er uit als een soort vrouw, heeft ook een vrouwennaam, maar een goed gesprek kun je er nog niet mee voeren.

AI en machine learning worden in veel sectoren toegepast voor specifieke toepassingen, soms in samenwerking met de wetenschap. Zo onderzoeken de Gemeente Amsterdam en de UvA manieren om meldingen van overlast in de openbare ruimte te classificeren met machine learning (er komen elk jaar zo'n 300.000 meldingen binnen). Geestig detail: de onderzoekers boeken hier de beste resultaten met een algoritme uit 1958.

Echte AI is vooral weggelegd voor de grote technologiebedrijven. Alleen zij beschikken over de enorme hoeveelheden data, rekenkracht en talent die nodig zijn om AI te laten werken. En zelfs dan heeft AI nog veel beperkingen.

Over de oneerlijkheid, de bias, van AI-algoritmen is al veel geschreven, onder meer door onderzoeker Cathy O'Neil.[28] Veel AI-systemen worden getraind met data waar ongelijke behandeling en discriminatie historisch zijn ingebouwd. Die systemen nemen dat gedrag dan gewoon over en versterken het zelfs. Zolang we dit probleem niet hebben opgelost, moeten we ook volgens O'Neil zeer terughoudend zijn met het inzetten van AI in kritische functies.

Andere beperkingen van AI zijn minder serieus. Als je aan je Androidtelefoon vraagt: OK Google, make me laugh, dan verstaat hij dat, wat knap is, maar vertelt vervolgens een grap die zo flauw is dat ze er alleen in bepaalde achtergebleven gebieden om moeten lachen. Wie met Google zoekt op "images without muffins" krijgt alleen maar plaatjes te zien met muffins. Het verschil tussen zo'n muffin en een chihuahua ziet een mens direct, maar zelfs de beste AI-systemen hebben hier flinke moeite mee.[29, 30]

Een centrale vraag in AI-onderzoek begint te worden: kan onze hardware de vraag nog wel aan? AI-onderzoekers van Google waarschuwen dat we tegen de grenzen van de rekenkracht aanlopen, omdat de vraag naar capaciteit de performance van de huidige generaties chips overstijgt.[31] De onderzoekers lijken te suggereren dat de huidige vorm van AI zijn rompsnelheid bereikt heeft.

Een "general AI", een systeem dat in de breedte intelligent gedrag vertoont, lijkt nog heel ver weg. Onderzoekers van Google, MIT en de Universiteit van Edinburgh pleitten daarom vorige maand voor het combineren van deep learning met de klassieke gestructureerde benadering.[32] Misschien dat dat helpt. Maar ook zulk AI-onderzoek is gebaseerd op een extreme vereenvoudiging van de processen die zich in onze hersenen afspelen als we "intelligentie" vertonen. Veel AI-onderzoek is gebaseerd op de impliciete aanname dat de menselijke hersenen elk probleem oplossen door het in losse brokjes op te delen, de samenhang tussen die brokjes te analyseren, en dan op basis van dat inzicht een conclusie te trekken. Dat beeld is te simpel. Intelligent gedrag is het product van een extreem complex samenspel van grotendeels onbegrepen biochemische en elektrochemische processen die zich niet alleen in onze hersenen, maar in ons hele lichaam afspelen, en in de interactie van dat lichaam met zijn omgeving. Het is vrij optimistisch, om niet te zeggen overmoedig om te denken dat je zo'n complex systeem in software kunt nabootsen. De ontwikkelaar van Eliza, Joseph Weizenbaum, vond het antropomorfische beeld van de computer een enorme onderschatting, zelfs ontkenning van wie wij zijn als mens.[33]

AI is nu vooral het domein van partijen die kunnen beschikken over enorme rekenkracht en enorme hoeveelheden data, en zelfs dan nog voor heel specifieke toepassingsgebieden, met heel veel beperkingen. Om de volgende stap te kunnen zetten, is nog heel veel onderzoek nodig.

Systemen die moeite hebben om een chihuahua van een muffin te onderscheiden, verdienen die een rol in toezicht? Die ethische vraag lijkt snel beantwoord. Maar stel dat er straks AI-systemen zijn die wel goed werken. Willen we die dan wel inzetten?

Crypto

Misschien denkt u bij technologie wel aan een systeem waar je geen toezicht meer op hoeft te houden, omdat er geen mensen meer achter de knoppen zitten. Een systeem waar de juiste werking is ingebouwd en waar niet van afgeweken kan worden. Zulke systemen bestaan, en de bekendste ervan is bitcoin.

Deze digitale munt werd tien jaar geleden gelanceerd door een onbekende persoon of groep onder de schuilnaam Satoshi Nakamoto, die niet alleen een inmiddels beroemd white paper publiceerde, maar daar ook meteen een werkende software-implementatie bij deed, en vervolgens in het niets verdween.[34] Informatici die het white paper lezen, krijgen steevast tranen in de ogen, zo ingenieus is het ontwerp.

Bitcoin is meer dan een digitale munt. Het is een protocol. Het is een systeem, een wereldwijd netwerk, waarvan de veel genoemde blockchain maar één onderdeeltje is. Bitcoin is volledig gedecentraliseerd: het is van iedereen en van niemand, er is geen centrale autoriteit. Het bitcoin-netwerk wordt in de lucht wordt gehouden door miljoenen gebruikers, meer dan honderdduizend nodes en miners die allemaal de regels van het protocol volgen. Ze moeten wel, want als je de regels niet volgt, mag je niet meedoen. Bij bitcoin zijn toezicht en controle volledig in het systeem ingebouwd. De juistheid, de volledigheid en vooral de onwijzigbaarheid van de transacties in het netwerk worden afgedwongen door beproefde en relatief simpele cryptografische operaties. Toezicht is niet meer nodig: er *kan* niet van de regels afgeweken worden. Het systeem zelf, het protocol en zijn gebruikers, dwingt naleving af.[35] Maar toezicht is ook niet meer mogelijk. Er is immers geen centrale partij, die ergens op aangesproken kan worden.

De afgelopen tien jaar zijn honderden alternatieve digitale munten bedacht, vaak afsplitsingen (*forks*) van bitcoin, en duizenden andere op "blockchain" gebaseerde systemen die ook gebruik maken van cryptografische biermuntjes, tegen betaling uitgegeven in Initial Coin Offerings (ICO's). Het idee is dat je zulke munten ooit kan gebruiken voor specifieke diensten, zoals de aankoop en registratie van vastgoed of het reserveren van tickets voor evenementen. Altcoins worden verhandeld op exchanges, waarbij de koers in bitcoin wordt genoteerd. Die handel leidde eind vorig jaar tot een golf van speculatie die de koers van bitcoin tot recordhoogte opstuwde, waarna uiteindelijk miljoenen mensen een godsvermogen kwijtraakten. Naast bitcoin en een handjevol andere cryptomunten is er niet één systeem in de wereld dat op enige schaal wordt gebruikt anders dan voor speculatie.

Het is interessant om te speculeren over de impact van bitcoin op toezicht, of over het toezicht op bitcoin, mocht de munt nog breder geaccepteerd worden. Bitcoin is geen betaalmiddel, eerder een ruilmiddel, net als edelmetalen. Op dit moment wordt bitcoin vooral gebruikt als een grensoverschrijdende "store of value". Je kunt er waarde in opslaan en deze waarde op elk gewenst moment tegen zeer lage kosten naar een andere partij waar dan ook ter wereld overhevelen. Voor kleine betalingen als een kop koffie is de bitcoin-blockchain ongeschikt, maar bovenop de bitcoin-infrastructuur ontstaat een

tweede laag die zulke kleine, snelle, goedkope transacties wel mogelijk maakt.[36]

Hoe toezichthouders met bitcoin en andere cryptomunten omgaan, verschilt van land tot land. Japan, Korea, de Verenigde Staten lopen voorop. De Amerikaanse Securities and Exchange Commission (SEC) ziet de tokens die bij ICO's worden uitgegeven inmiddels als securities die geregistreerd moeten worden, en vindt dat ook crypto-exchanges onder haar toezicht vallen, maar bitcoin niet.[37] Een paar landen met zowel een dictatoriaal regime als een extreem hoge inflatie vrezen een vlucht in bitcoin en komen met een eigen cryptomunt. Europese toezichthouders zijn wat knorrig over bitcoin; twee weken geleden nog noemde een topman van de ECB bitcoin "de boosaardige nakomeling van de financiële crisis".[38] In Nederland neemt de AFM een kritische positie in. De AFM waarschuwt consumenten wel, maar houdt geen toezicht, ook niet op gecentraliseerde munten en cryptobeurzen, onder verwijzing naar de Wet op het financieel toezicht (Wft).[39] Het is interessant om te zien of Europa de SEC zal navolgen.

Stel dat de invloed van gedecentraliseerde systemen als bitcoin op een gegeven moment zo groot wordt, dat overheden tot de conclusie komen dat zij onder toezicht gesteld zouden moeten worden. Wat dan? Niemand weet hoe je toezicht moet houden op iets waar je geen toezicht op kunt houden. We gaan interessante tijden tegemoet.

Samenvatting

Het beeld dat ontstaat, is dat van een volledige gedigitaliseerde economie. Een economie waarin we onder permanent toezicht staan van een handjevol grote technologiebedrijven die hun observaties gebruiken om ons gedrag te beïnvloeden en die ons controleren in plaats van andersom. Een economie waarin werkgevers hun werknemers, overheden hun burgers permanent in de gaten houden en waarin we ook steeds meer toezicht houden op elkaar, via de camera's van onze smartphones en alle online kanalen die we tot onze beschikking hebben. Een economie waarin tegelijk langzaam maar zeker wereldwijde digitale ruilmiddelen opkomen die zich onttrekken aan elke vorm van toezicht. Een economie waarin traditionele toezichthouders wonderlijk genoeg nog maar beperkte aandacht hebben voor technologie, vaak onder het motto: we're too busy, the future has to wait.

Auditing

Laten we nu inzoomen op auditing. Auditing, voor de niet-auditors in deze kerk, is het vakgebied dat zich bezighoudt met het verschaffen van zekerheid door dingen te onderzoeken, te toetsen aan normen, en daarover te rapporteren. Auditors geven invulling aan de eerste twee onderdelen van de eerder genoemde definitie van toezicht: het verzamelen van informatie en het vormen van een oordeel. Het derde onderdeel, het plegen van interventies, hoort er niet bij. Dat doet degene die het oordeel gebruikt als input voor zijn of haar beslissing.

Je hebt externe en interne auditors. De externe auditor of accountant is de oudste van de twee. Accountant Theodore Limperg richtte in 1929 de eerste accountantsopleiding in Nederland op, hier aan de Universiteit van Amsterdam. De accountant controleert de jaarrekening van ondernemingen en instellingen en rapporteert aan het maatschappelijk verkeer. De interne auditor richt zich op de processen binnen de organisatie en is één van de belangrijkste instrumenten van de RvC om inzicht te krijgen in de manier waarop de organisatie de risico's beheerst. Het is niet voor niets, dat de interne auditor een prominente plaats heeft gekregen in de Nederlandse Corporate Governance Code.[40]

Met studenten heb ik altijd discussies over het "waarom" van auditing. Een auditor verschaft zekerheid. Maar aan wie? Aan het maatschappelijk verkeer. Aan stakeholders. Waarom hebben die behoefte aan zekerheid? Simpel: omdat ze onzeker zijn. Onzeker over een jaarrekening of een andere verantwoording. Onzeker over de beveiliging van hun informatiesystemen. Dus auditors geven in zekere zin zekerheid aan onzekere mensen.

De aanpak van de auditor is traditiegetrouw gebaseerd op twee sporen: het toetsen van de maatregelen die een organisatie heeft getroffen om ervoor te zorgen dat het getoetste object inderdaad aan de normen voldoet (*test of controls*), en het toetsen van de gegevens zelf (*substantive testing*).[41]

De ontwikkeling en adoptie van informatietechnologie hebben de laatste decennia op beide sporen een onomkeerbaar effect gehad.

De *test of controls* is ingrijpend van karakter veranderd. Hij is zowel makkelijker als moeilijker geworden. Makkelijker, omdat de technologie steeds krachtiger middelen biedt om hem geautomatiseerd uit te voeren. Maar vooral moeilijker, omdat het technologische landschap met alle maatregelen daarin is uitgegroeid tot een voortdurend veranderend doolhof waarin maar weinigen de weg kennen.

Een vergelijkbare ontwikkeling zien we bij *substantive testing*. De hoeveelheid beschikbare data is in figuurlijke zin geëxplodeerd; de auditor heeft veel

meer data tot zijn beschikking dan vroeger – niet langer alleen interne, gestructureerde data, zoals in een ERP-systeem, maar ook gestructureerde en ongestructureerde data uit externe bronnen die veelal openbaar toegankelijk zijn. Daarnaast leiden technologische ontwikkelingen ook tot steeds krachtiger tools en technieken om die gegevens te kunnen analyseren: van zeer gebruiksvriendelijke statistische analysetools tot geavanceerde algoritmen op basis van machine learning.

De combinatie van deze krachten lijkt te zorgen voor een paradigmaverschuiving in auditing, waarbij het analyseren van data steeds meer aan terrein wint.[42]

De uitdaging is, hoe de auditor met deze verschuiving omgaat. Onderzoek suggereert dat auditors, vergeleken met andere beroepsbeoefenaren, achterblijven bij het adopteren van data-analyse, geautomatiseerde audit tools en algoritmen.[43, 44, 45] Als redenen worden onder meer genoemd:

- Een gebrek aan kennis en vaardigheden
- Het ontbreken van infrastructuur en tools
- Niet weten waar de data te vinden is, en hoe deze te ontsluiten is
- Het ontbreken van prikkels om te innoveren
- De conservatieve aard van de beroepsgroep en haar beoefenaren

Ik ga nu kort op deze redenen in.

Kennis en vaardigheden

Het analyseren van data vereist specifieke kennis en vaardigheden die nu vaak nog ontbreken. Dit obstakel is relatief weg te nemen. Veel audit teams nemen op dit moment dataspecialisten aan: econometristen, biologen, zelfs psychologen, die in hun opleiding hebben geleerd om grote datasets te analyseren. Maar zonder auditvaardigheden heb je weinig aan die specialistische kennis. Om data scientists effectief in audits in te kunnen zetten, is het noodzakelijk dat de auditor zelf over enige kennis op het gebied van data science beschikt en ook de taal van de data scientist spreekt. Op de UvA hebben wij een maatwerkprogramma ontwikkeld, Data Science for Auditors (DSA), waarin wij auditors inwijden in de beginselen van data science. Een aantal voor de auditor relevante facetten van data science komt daarbij aan de orde: van het ontwikkelen van een data-driven auditplan tot het extraheren, transformeren en laden van data (ETL); van steekproeven, correlatie en regressie tot classificatie met machine learning; van fraudeonderzoek tot process mining en visualisatie. Het programma maakt gebruik van een Jupyter-programmeeromgeving, waarbij studenten in R en Python praktijkoefeningen uitvoeren. Inmiddels

hebben we een jaar ervaring opgedaan met dit programma, dat niet alleen deel uitmaakt van alle auditopleidingen, maar ook als vierdaagse Masterclass in de markt wordt aangeboden.

Infrastructuur en tools

Om data te kunnen analyseren, moet je investeren in infrastructuren en tools. Groot hoeft die investering niet te zijn. Met open source programmeeromgevingen voor R en Python kom je een heel eind. Deze omgevingen bieden een zeer krachtig en veelzijdig analyseplatform met uitgebreide packages voor analyse, machine learning en visualisatie. Ze zijn relatief gemakkelijk te leren via online learning omgevingen zoals Coursera of Datacamp. Als het budget het toelaat, kan je investeren in commerciële analysesoftware als SAS, SPSS, Cognos, Tableau of een van de vele andere opties die de markt te bieden heeft. Dat maakt de analyses waarschijnlijk net iets makkelijker en de visualisaties net iets mooier.

Data ontsluiten

Voor data-analyse is het stellen van de goede vraag essentieel. Pas daarna kun je de data ontsluiten waarmee je deze vraag kunt beantwoorden. Vaak kun je die data heel dichtbij vinden, in je eigen organisatie. Maar even vaak blijk je openbare databronnen te kunnen gebruiken, die je extra informatie en zekerheid in je audit kunnen geven. Het ontsluiten en prepareren van data is niet altijd een sinecure. In die gevallen is het inschakelen van een ETL-specialist de makkelijkste weg. Deze zorgt ervoor dat data uit verschillende bronnen en in verschillende formaten wordt samengevoegd tot één homogeen, analyseerbaar bestand.

Toegevoegde waarde

In disciplines als marketing of logistiek is de toegevoegde waarde van data-analyse direct duidelijk. Een goede analyse kan daar snel leiden tot een stijging van de omzet of een verlaging van de verwerkingssnelheid. Bij auditing is die business case vaak minder scherp. Data-analyse kost tijd en moeite, maar wat levert het op? Het effect op de effectiviteit van de audit is doorgaans positief. Door meer data te gebruiken, stijgt de kwaliteit van de audit. Maar het effect op efficiency is minder duidelijk. Data-analyse zelf is misschien efficiënter dan handmatig controleren, maar kan ook leiden tot meer bevindingen, waar dan weer opvolging aan gegeven moet worden. De belangrijkste kracht

van data-analyse in de audit is dat analyses nieuw inzichten kunnen geven in de kwaliteit van de bedrijfsvoering, inzichten waar de organisatie haar voordeel mee kan doen. Maak die toegevoegde waarde zoveel mogelijk zichtbaar en meetbaar om de inzet van data-analyse in toekomstige audits te stimuleren.

Conservatieve aard

Even generaliseren: in vergelijking met hun peers in andere disciplines zijn veel auditors voorzichtig of zelfs behoudend van karakter. Auditors gaan niet over één nacht ijs, houden niet van vervelende verrassingen, houden zich aan de regels, zijn dol op plannen en documenteren, en trekken geen conclusies zonder hard bewijsmateriaal. Deze karaktereigenschappen zijn niet verrassend; auditors hebben immers niet voor niets voor dit vak gekozen. Ook hebben veel auditors niet altijd een vanzelfsprekende affiniteit met technologie; logisch, anders waren ze waarschijnlijk wel een beta-vak gaan studeren. Desgevraagd geven auditors zelf aan: wij zijn niet de beroepsgroep met de hoogste *risk appetite* en *technology savviness*. Iets om rekening mee te houden bij het invoeren van nieuwe audittechnieken op basis van data science. Bij de UvA hebben we ervoor gekozen bij de basis te beginnen en gaan we uit van de algemeen geaccepteerde auditstandaarden en van de Concept-handreiking Data-analyse van de Nederlande Beroepsorganisatie van Accountants (NBA).[46] Zo leiden we de auditor via een bekend referentiekader de nieuwe wereld van data science binnen.

De paradigmaverschuiving binnen auditing is in volle gang; de toekomst van audit is data. Ik hoop daar vanuit deze universiteit een impuls aan te kunnen geven. Tenslotte zal de rol van toezichthouders en auditors de komende jaren naar mijn gevoel niet afnemen, maar juist toenemen – er is een toenemende behoefte aan zekerheid in onzekere wereld, en een toenemende behoefte aan zekerheid over technologie. Wordt deze dienst geleverd door de huidige auditors? Alleen als zij er in slagen het tempo van de technologische ontwikkelingen bij te houden.

Bijdrage

Graag sluit ik af met een belofte of verwachting over de bijdrage die ik de komende jaren aan deze universiteit zal lever bij het geven van invulling aan mijn leerstoel, Data Science in Auditing.

Dat is allereerst door onderwijs over digitalisering, data en technologie te organiseren en te geven aan auditors en zij die dat willen worden. Het eerder genoemde onderwijsprogramma, Data Science for Auditors, zullen wij de komende jaren verder ontwikkelen, in de auditopleidingen integreren en digitaal beschikbaar stellen.

In de tweede plaats doe ik samen met een aantal getalenteerde Ph.D.-studenten onderzoek naar manieren om technologie en data effectiever in te zetten in de auditprofessie, naar de adoptie van technologie door auditors, naar manieren om het succes van innovaties te kunnen voorspellen, en naar methoden en technieken om algoritmen te kunnen auditen.

Ten derde zal ik leiding geven aan het Institute for Executive Programmes aan de Amsterdam Business School. Dit instituut omvat 14 toonaangevende nationale en internationale master- en postmasteropleidingen, waaronder een MBA in Big Data, en een groeiend aantal kortlopende opleidingen en masterclasses over actuele onderwerpen op het snijvlak van finance, control, auditing en data.

Dankwoord

Het is onmogelijk om iedereen te bedanken die de afgelopen jaren op welke manier dan ook een bijdrage heeft geleverd aan mijn levensvreugde. Jullie zijn gewoon met teveel. In elk geval dank ik:

Het College van Bestuur van de Universiteit van Amsterdam en de decanen van de Faculteit Economie en Bedrijfskunde en de Amsterdam Business School, voor het in mij gestelde vertrouwen; het team van Executive Programmes, de collega's van de sectie Accounting & Control, het Amsterdam Platform for Privacy Research, en oud-collega's van KPMG voor de samenwerking.

De docenten en studenten van de opleidingen EMIA, EPDA en de PMA en het DSA-team.

HKC, Watermelon Men en de divisie Monnickendam voor de vriendschap en inspiratie.

De *famiglie* Roos Lindgreen, Van Dolen en Wildenburg, voor hun steun en belangstelling.

De druktemakers op de Middenweg, voor de gezelligheid en de dilemma's.

De Umbrella Gang Plus, voor de wokeness en de woordspelingen.

En tot slot Willemijn, voor al je liefde en voor wie je bent. Je verrast me elke dag.

Tot slot

Ik hoop dat ik u nieuwsgierig achterlaat, hongerig naar meer. Dit verhaal begon met Martin Luther. Ik zou graag afsluiten met de vaste wens van een geestelijke die in Nederland bekender is dan Luther zelf. Dus: ik wens u een fijne voortzetting en alvast een aangenaam etensmaal, met spekjes of wat dan ook erin.

Ik heb gezegd.

Noten

1. Seidemann, J.K. (1846). Luthers Hausrechnung, nebst zwei Briefen. *Zeitschrift für die historischen Theologie*. C.W. Riedner (ed). Vol. 16. No. 10. Pp. 418. Leipzig. J.W. Brodhaus.
2. Forster, E.S. (1920). *Aristoteles – Oeconomica (translation)*. Oxford at the Clarendon Press. Pp. 1343-1344.
3. Dakyns, H.G. (2008). Xenophon – The Economist (translation). *The Gutenberg Project*. EBook #1173.
4. Tweede Kamer (1998). *Kamerstuk 25 956: Toezicht op uitvoering publieke taken*. Tweede Kamer. Vergaderjaar 1997-1998. Nrs. 1-2. 31 maart 1998.
5. Best, M. and Neuhauser, D. (2006). Walter A Shewhart, 1924, and the Hawthorne factory. *Quality and Safety in Health Care*. Vol. 15. Pp. 142-143.
6. Orwell, G. (1949). *1984*. Secker and Warburg. London.
7. Ryan, R.M., and Deci, E.L. (2000). Self-Determination Theory and the Facilitation of Intrinsic Motivation, Social Development, and Well-Being. *American Psychologist*. Vol 55. No. 1. Pp. 68-78.
8. Goold, B.J. (2010). CCTV and Human Rights. *Citizens, Cities and Video Surveillance: Towards a Democratic and Responsible Use of CCTV*. Paris. European Forum for Urban Security.
9. Kuijpers, K., Muntz, T. en Staal, T. (2018). 'Privacy? Achterhaald'. *De Groene Amsterdammer*. 2 november 2018.
10. Moore, G.E. (1965). Cramming more components onto integrated circuits. *Electronics*. Vol. 38. No. 8. Pp. 114-117.
11. Oorspronkelijk noemde Moore een periode van één jaar; later, in 2005, stelde hij de periode bij tot twee jaar.
12. Cisco (2017). *Cisco Visual Networking Index:Forecast and Methodology, 2016-2021*. PDF. Retrieved 14 August 2017.
13. www.blockchain.com.
14. Versteegh, K. (2018). 'AIVD gaf VS cruciale informatie over Russische hacks'. NRC. 25 januari 2018.
15. NPB (2018). NOODKREET RECHERCHE – Waar blijft onze versterking? Rapport.
16. Saunders, J. et al. (2016). Predictions put into practice: a quasi-experimental evaluation of Chicago's predictive policing pilot. *Journal of Experimental Criminology*. Vol. 12. Pp. 347-371. doi: 10.1007/s11292-016-9272-0
17. Hunt, P. et al. (2014). Evaluation of the Shreveport Predictive Policing Experiment. RAND Corporation. https://www.rand.org/pubs/research_reports/RR531.html.
18. Shapiro, A. (2017). Reform Predictive Policing. *Nature*. Vol. 541. Pp. 458-460. doi:10.1038/541458a
19. AFM (2018). Jaarverslag 2017.
20. ACM (2018). Jaarverslag 2017.
21. Lückerath, M. en De Bos, A.G. (2017). Nationaal Commissarissenonderzoek 2016.
22. Amrop (2018). *Digitization on Boards Report | 2nd Edition*.

23. Manjoo, F. (2016). Tech's 'Frightful 5' Will Dominate Digital Life for Foreseeable Future. New York Times. 20 januari 2016.
24. https://www.theguardian.com/technology/2018/nov/05/tim-berners-lee-launches-campaign-to-save-the-web-from-abuse
25. Zuckerberg, M. (2018). A Blueprint for Content Governance and Enforcement. Blog post. https://www.facebook.com/notes/mark-zuckerberg/a-blueprint-for-content-governance-and-enforcement/10156443129621634/
26. Kukenheim, S. (2018). UvA en gemeente Amsterdam zetten zich in voor hotspot Artificial Intelligence op Science Park. Persbericht. https://www.amsterdam.nl/bestuur-organisatie/college/wethouder/simone-kukenheim/persberichten/uva-gemeente/
27. Mervis, J. (2018). MIT to use $350 million gift to bolster computer sciences. *Science*. 15 oktober 2018.
28. O'Neill, C. (2016). Weapons of math destruction.
29. Togootogtokh, E. and Amartuvshin, A. (2018). Deep Learning Approach for Very Similar Objects Recognition Application on Chihuahua and Muffin Problem. White paper. Mongolian University of Science and Technology.
30. Yao, M. (2017). Chihuahua or muffin? Searching for the best computer vision API. https://www.topbots.com/chihuahua-muffin-searching-best-computer-vision-api/
31. Ray, T. (2018). Google says 'exponential' growth of AI is changing nature of compute. *ZDnet*. 2 November 2018. https://www.zdnet.com/article/google-says-exponential-growth-of-ai-is-changing-nature-of-compute/
32. Battaglia, J.W. et al. (2018). Relational inductive biases, deep learning, and graph networks. arXiv:1806.01261v3 [cs.LG] 17 Oct 2018.
33. Weizenbaum, J. (1976). *Computer Power and Human Reason: From Judgment To Calculation*. San Francisco. W. H. Freeman. ISBN 0-7167-0463-3.
34. Nakamoto, S. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System.
35. Antonopoulos, A. (2017). Mastering Bitcoin: Programming the Open Blockchain. Wiley. ISBN-13: 978-1491954386.
36. Poon, J. and Dryja, T. (2016). The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. White paper. Draft version 0.5.9.2. 14 januari 2016.
37. https://www.sec.gov/news/press-release/2018-264
38. Jones, C. (2018). ECB official dubs bitcoin 'evil spawn of the financial crisis'. Financial Times. 15 november 2018.
39. https://www.afm.nl/nl-nl/consumenten/veelgestelde-vragen/ico-crypto/ico-toezicht
40. Monitoring Commissie Corporate Governance Code (2016). *Nederlandse Corporate Governance Code*. 8 December 2016.
41. De tekst in deze alinea is in gewijzigde vorm ook verschenen als een blog op LinkedIn.
42. Roos Lindgreen, E. (2016). From IT Auditor to Data Scientist. EDPACS. Vol. 53. No. 3. pp. 1-5.
43. Cao, M., Chychyla, R. and Stewart, T. (2015). Big Data Analytics in Financial Statement Audits. Accounting Horizons. Vol. 29. No. 2. pp. 423-429.

44. Wang, T. and Cuthbertson, R. (2014). Eight Issues on Audit Data Analytics We Would Like Researched. Journal of Information Systems. Vol. 29. No. 1. pp. 155-162.
45. Yoon, K., Hoogduin, L. and Zhang, Li. (2015). Big Data as Complementary Audit Evidence. Accounting Horizons. Vol. 29. No. 2. pp. 431-438.
46. NBA (2017). Concept-handreiking Data-analyse.