
BESTUURDERSAANSPRAKELIJKHEID VOOR FALEND RISICOMANAGEMENT INZAKE ARTIFICIËLE INTELLIGENTIE

Kunnen bestuurders aansprakelijk zijn wanneer een toepassing vele kansen biedt, maar waarbij de risico's die daarmee gepaard gaan moeilijk identificeer- en beheersbaar zijn?

Masterthesis Tilburg University

Naam: Maura Sibens

Afstudeerrichting: Ondernemingsrecht

ANR: 558846

Studentnummer: 1244828

Scriptiebegeleider: prof. dr. C. van der Elst

Datum: 16 augustus 2019

VOORWOORD

Voor u ligt de scriptie 'Bestuurdersaansprakelijkheid voor falend risicomanagement inzake artificiële intelligentie', die ik ter afsluiting van de Master Ondernemingsrecht aan de Universiteit van Tilburg heb geschreven. De colleges van het vak Ondernemingsrecht en Risicomanagement hebben mijn interesse in risicomanagement en de juridische kant daarvan aangewakkerd, omdat het een vak is waarbij niet louter een juridisch perspectief aan bod komt. Ik raakte geïnspireerd door het onderwerp risicomanagement in het kader van behoorlijk bestuur, waardoor ik na overleg met prof. dr. van der Elst heb besloten mijn scriptie over dit onderwerp te schrijven en dit toe te spitsen op een heet hangijzer: artificiële intelligentie.

Een grote uitdaging schuilde in het onderzoek naar artificiële intelligentie, omdat een technisch onderwerp immers vaak lastig is voor de typische atechnische jurist. Ik heb dan ook geprobeerd dit onderwerp zo goed mogelijk te vertalen naar voor juristen en niet-techneuten begrijpelijke taal. Ik ben blij dat ik in dit onderzoek verbanden heb kunnen leggen tussen het recht en andere disciplines, hetgeen mij het meeste aanspreekt en inspireert in de Master Ondernemingsrecht.

Het schrijven van mijn scriptie was niet mogelijk geweest zonder de steun vanuit de universiteit, vrienden en familie. Graag wil ik daarom prof. dr. van der Elst bedanken voor de inspiratie, begeleiding, feedback en prettige samenwerking. Hij heeft mij geheel vrij gelaten op het gebied van deadlines en het inleveren van conceptstukken, maar was altijd op zeer korte termijn beschikbaar voor feedback, zelfs tijdens zijn vakantie. Tevens wil ik mijn vrienden en familie bedanken voor de support gedurende de Master Ondernemingsrecht en het schrijven van deze scriptie. Meer in het bijzonder wil ik mijn vriend Coen bedanken voor zijn peptalks, knuffels en de manier waarop hij al het mogelijke heeft gedaan om mij in deze periode te ontzien van andere verplichtingen. Tot slot wil ik mijn ouders bedanken voor hun motiverende woorden en meer in het bijzonder mijn vader, voor het stellen van kritische vragen en het sparren over deze scriptie.

Ik wens u veel leesplezier toe.

Maura Sibens

Eindhoven, 16 augustus 2019

INHOUDSOPGAVE

VOORWOORD	2
LIJST MET AFKORTINGEN	6
1. INLEIDING	7
1.1 MAATSCHAPPELIJK PROBLEEM	7
1.2 CENTRALE VRAAGSTELLING	8
1.3 ONDERZOEKSMETHODEN	9
1.4 AFBAKENING	9
2. DEFINITIE EN WERKING AI	11
2.1 INLEIDING	11
2.2 DEFINITIE	11
2.3 DE WERKING VAN AI	12
2.3.1 ALGEMEEN	12
2.3.2 KENNIS- EN DATA GEBASEERDE BENADERING	13
2.3.3 WEAK EN STRONG AI	13
2.4 CONCLUSIE	14
3. TOEPASSING, RISICO'S EN KANSEN AI	15
3.1 INLEIDING	15
3.2 TOEPASSING AI IN KAPITAALVENNOOTSCHAPPEN	15
3.2.1 SERVICE EN HOSPITALITY	16
3.2.2 FINANCIËLE DIENSTVERLENING	16
3.2.3 RETAIL	17
3.2.4 GEZONDHEIDSZORG	17
3.2.5 VERVOER EN TRANSPORT	18
3.2.6 JURIDISCHE DIENSTVERLENING	18
3.2.7 INTERNE TOEPASSINGEN	18
3.3 RISICO'S VAN HET GEBRUIK VAN AI	19
3.3.1 ONEIGENLIJK GEBRUIK	19
3.3.2 INTERNE ONBETROUWBAARHEID	19
3.3.3 EXTERNE ONBETROUWBAARHEID: CYBERRISICO'S	19
3.3.4 INTERPRETEERBAARHEID	20
3.3.5 TRANSPARANTIE	20
3.3.6 VERANTWOORDELIJKHEID	20
3.3.7 GRONDRECHTEN EN ETHISCHE PRINCIPES	21
3.3.8 WET- EN REGELGEVING	22
3.4 KANSEN AI	22
3.4.1 KOSTENBESPARING EN INNOVATIE	23
3.4.2 AI 'ZIET' MEER	23
3.5 CONCLUSIE	25

4. ADEQUATE CORPORATE GOVERNANCE.....	26
4.1 INLEIDING	26
4.2 DE TAAK VAN HET BESTUUR	26
4.3 NCGC	27
4.3.1 NALEIVING, TOEPASSELIJKHEID EN REFLEXWERKING	27
4.3.2 RISICOBEBEERSING IN DE NCGC	30
4.3.2.1 <i>Risicomanagement door het bestuur</i>	30
4.3.2.2 <i>Verantwoording over risicobebepaling</i>	32
4.4 WET- EN REGELGEVING.....	32
4.4.1 PRIVACY- EN GEGEVENSBESCHERMING	32
4.4.2 ETHISCHE RICHTLIJNEN	33
4.5 CONCLUSIE	34
5. AANSPRAKELIJKHEID VOOR FALEND RISICOMANAGEMENT.....	36
5.1 INLEIDING	36
5.2 INTERNE BESTUURDERSAANSPRAKELIJKHEID EX ART. 2:9 BW	36
5.2.1 (ON)BEHOORLIJK BESTUUR EN ERNSTIG VERWIJT	38
5.3 EXTERNE BESTUURDERSAANSPRAKELIJKHEID EX ART. 6:162 BW	40
5.4 (ON)BEHOORLIJK BESTUUR EN ERNSTIG VERWIJT MAATSTAF IN HET LICHT VAN RISICOMANAGEMENT	41
5.4.1 FALEND RISICOMANAGEMENT	41
5.4.2 RISICOBEBEERSINGSFOUTEN	42
5.4.2.1 <i>Afwezigheid van een systeem</i>	42
5.4.2.2 <i>Systeemfouten</i>	42
5.4.2.3 <i>Werkingsfouten</i>	43
5.4.2.4 <i>Beoordelingsfouten</i>	43
5.4.2.5 <i>Gebrek aan transparantie</i>	45
5.5 CONCLUSIE	45
6. INRICHTING RISICOBEBEERSINGS- EN CONTROLESYSTEEM	47
6.1 INLEIDING	47
6.2 DE VIJF COMPONENTEN VAN COSO 2017	48
6.2.1 GOVERNANCE EN CULTUUR.....	48
6.2.1.1 <i>Strategie</i>	48
6.2.1.2 <i>Operationele structuur</i>	48
6.2.1.3 <i>Risicocultuur</i>	49
6.2.1.4 <i>Commitment aan kernwaarden</i>	49
6.2.1.4 <i>Menselijk kapitaal</i>	50
6.2.2 STRATEGIE EN DOELSTELLINGEN.....	50
6.2.2.1 <i>Context</i>	50
6.2.2.2 <i>Risicobereidheid</i>	51
6.2.2.3 <i>Alternatieve strategieën</i>	52
6.2.2.4 <i>Bedrijfsdoelstellingen</i>	53
6.2.3 PRESTATIEMETING.....	53
6.2.3.1 <i>Risico-identificatie</i>	53
6.2.3.2 <i>Prioriteit</i>	57
6.2.3.3 <i>Risicobeoordeling</i>	58

6.2.3.4 Risicoreacties.....	59
6.2.3.5 Portfolio-weergave risico's	60
6.2.4 EVALUATIE EN BIJSTUREN	61
6.2.4.1 Identificatie en beoordeling veranderingen.....	61
6.2.4.2 Prestatiebeoordeling	61
6.2.4.3 Verbetering risicobeheersing.....	62
6.2.5 INFORMATIE, COMMUNICATIE EN RAPPORTAGE	62
6.3 SYSTEEM- WERKINGS- EN BEOORDELINGSFOUTEN	62
6.4 CONCLUSIE	64
7. CONCLUSIE.....	66
Definitie en werking AI.....	66
Toepassing, risico's en kansen AI	66
Adequate Corporate Governance.....	67
Aansprakelijkheid voor falend risicomanagement	68
Inrichting risicobeheersings- en controlesysteem	69
BIBLIOGRAFIE.....	71
BOEKEN	71
TIJDSCHRIFTEN	74
NIEUWSBERICHTEN	75
KAMERSTUKKEN	76
OVERIGE BRONNEN	76
JURISPRUDENTIE	78

LIJST MET AFKORTINGEN

AI	Artificiële Intelligentie / Kunstmatige Intelligentie
AVG	Algemene Verordening Gegevensbescherming
Bb	Bedrijfsjuridische berichten
BW	Burgerlijk Wetboek
COSO	Committee of Sponsoring Organizations of the Treadway Commission
EC	Europese Commissie
ERMF	Enterprise Risk Management Framework
EU	Europese Unie
EVRM	Europees Verdrag voor de Rechten van de Mens
EY	Ernst & Young
GDPR	General Data Protection Regulation
Gw	Grondwet
Hof	Gerechtshof
HR	Hoge Raad
IVBPR	Internationaal verdrag inzake burgerrechten en politieke rechten
KYC	Know Your Customer
MAB	Maandblad voor Accountancy en Bedrijfseconomie
MvT	Memorie van Toelichting
MvV	Maandblad voor Vermogensrecht
NCGC	Nederlandse Corporate Governance Code
NJ	Nederlandse Jurisprudentie
NJB	Nederlands Juristenblad
OK	Ondernemingskamer
OR	Ondernemingsrecht
Rb	Rechtbank
RvC	Raad van Commissarissen
TGP	Tijdschrift voor Gezondheid en Politiek
Wft	Wet op het financieel toezicht
Wwft	Wet ter voorkoming van witwassen en financieren van terrorisme

1. INLEIDING

1.1 Maatschappelijk probleem

Artificiële- en kunstmatige intelligentie (hierna: AI) zijn termen die steeds vaker voorbij komen in het nieuws.¹ Voor ieder positief verhaal over de voordelen en mogelijkheden van deze vorm van intelligentie, bestaat er ook een die de negatieve gevolgen en potentiële risico's benadrukt. Zo wordt er enerzijds bericht over gigantische investeringen in AI door grote technologiebedrijven zoals Facebook en Google en wordt er anderzijds bijvoorbeeld door Stephen Hawking meerdere malen gewaarschuwd voor de risico's van 'super AI'. Hij meent dat de wereld en daarmee tevens de mensheid uiteindelijk overgenomen zal worden door robots en AI.²

Daartegenover staan stellingen die pleiten dat dat AI nog in de kinderschoenen staat, waarbij wel significante ontwikkelingen plaatsvinden, maar niet van dusdanige aard dat we binnen nu en een aantal jaar van bovenstaande verregaande gevolgen kunnen spreken. Veel van deze 'verkeerde' voorspellingen leiden ertoe dat de mensheid, voorlopig onnodig, angst kan creëren voor AI. Wel wordt benadrukt dat AI ook niet onderschat mag worden, omdat in de verdere toekomst ongetwijfeld grote ontwikkelingen plaats kunnen vinden.³ Een ding dat vaststaat, is dat AI heden ten dage al van (grote) invloed is op bedrijven en de algehele economie.⁴

Gezien het feit dat AI in de kleinste dingen schuilt, kan er gesteld worden dat AI reeds in vele ondernemingen gebruikt wordt. De vraag is echter in hoeverre bestuurders van vennootschappen bekend zijn met de risico's die met het gebruik en de toepassing daarvan gepaard gaan. Voorts kan de vraag gesteld worden in hoeverre zij maatregelen nemen ter voorkoming van verwezenlijking van deze risico's, hetgeen van belang is omdat bestuurders ingevolge art. 2:129 lid 1 BW en art. 2:239 lid 1 BW een bestuursplicht hebben. Wat het besturen van de onderneming precies inhoudt, hangt af van de omstandigheden per onderneming, zoals de wet en statuten en de omstandigheden waarin de vennootschap op dat moment in verkeer is. In ieder geval wordt de verantwoordelijkheid voor de dagelijkse gang van zaken, de doelstellingen, de strategie, het financieel beleid en het risicomanagement daartoe gerekend.⁵ Wat hierbij van belang is, is dat de bestuurder op grond van art. 2:9 BW de verplichting heeft deze taak behoorlijk te vervullen. Omdat een bestuurder op naam van de vennootschap handelt, zal de bestuurder in bepaalde gevallen op zijn handelen aangesproken moeten

¹ Zie bijvoorbeeld: Bergen, van, *De Telegraaf* 8 april 2019, Rooij, van, *Algemeen Dagblad* 3 mei 2019, Middendorp, de *Volkskrant* 26 mei 2019.

² Zie bijvoorbeeld: Cellan-Jones, *BBC* 2 december 2014, Madeiros, *Wired* 28 november 2017.

³ Brooks, *MIT Technology review* 2017.

⁴ Dirican, *PSBS* 2015, vol. 195, p. 564-573.

⁵ Stolp & Nijs Bik, de 2015, p.43.

kunnen worden, wanneer hij deze taak onbehoorlijk vervult.⁶

Het feit dat risicomanagement onder de bestuurstaak valt en deze derhalve behoorlijk uitgevoerd dient te worden, geeft nog geen invulling aan het criterium behoorlijk bestuur. Wat vast staat is dat een bestuurder in zekere zin bestuursautonomie heeft, welke een vrijheid in het vervullen van zijn of haar taken met zich meebrengt. Dit is een voorwaarde om de rechtspersoon te kunnen leiden.⁷ Verder is in de jurisprudentie uitleg gegeven aan dit criterium, zoals bijvoorbeeld het vereiste dat een bestuurder een ernstig verwijt moet kunnen worden gemaakt, wil er sprake zijn van onbehoorlijke taakvervulling in de zin van art. 2:9 BW.⁸ Hierbij is niet alleen van belang of een bestuurder bekend was met deze risico's, maar ook of hij deze had behoren te kennen. Er wordt in dat geval gekeken of van een redelijke, bekwame bestuurder de vaardigheden en het inzicht op het gebied van risico-identificatie en –analyse verwacht mag worden.⁹

Dát bestuurders aansprakelijk gesteld kunnen worden voor falend risicomanagement staat inmiddels buiten kijf.¹⁰ De vraag is echter of dit ook mogelijk is wanneer het gebruik van AI juist vele positieve aspecten kent, maar waarbij de risico's moeilijk voorspel- en/of beheersbaar zijn, of waarbij de meningen betreffende de risico's ontzettend uiteen lopen. Daarnaast is AI aan voortdurende ontwikkeling onderhevig. Kan op dat moment van een bestuurder worden verwacht dat zij haar bestuurstaak ten aanzien van risicomanagement behoorlijk uitvoert?

1.2 Centrale vraagstelling

De vraag die in dit onderzoek centraal staat is:

Kan het bestuur van een kapitaalvennootschap aansprakelijk worden gesteld wegens onvoldoende risicomanagement inzake artificiële intelligentie?

Bovenstaande centrale vraagstelling wordt beantwoord aan de hand van de volgende deelvragen:

1. *Wat is AI en hoe werkt AI?*
2. *Hoe wordt AI toegepast binnen kapitaalvennootschappen en welke risico's en kansen gaan daarmee gepaard?*
3. *Op welke wijze kan invulling worden gegeven aan het begrip adequate Corporate Governance in het licht van risicomanagement betreffende AI?*
4. *Op welke wijze(n) kan het bestuur van een kapitaalvennootschap aansprakelijk worden gesteld voor falend risicomanagement inzake AI?*
5. *Kan een risicobeheersingssysteem zoals COSO 2017 bestuurdersaansprakelijkheid voor falend risicomanagement inzake AI voorkomen?*

⁶ Strikwerda, MAB 2002/76(1/2), p. 54-64.

⁷ Asser/Maeijer & Kroeze 2-I* 2015/189.

⁸ HR 10 januari 1997, ECLI:NL:HR:1997:ZC2243 (Staleman/Van de Ven).

⁹ HR 10 januari 1997, ECLI:NL:HR:1997:ZC2243 (Staleman/Van de Ven); HR 8 april 2005, ECLI:NL:HR:2005:AS010 (Laurus); HR 8 juni 2001, ECLI:NL:HR:2001:AB2053 (Panmo).

¹⁰ Strik 2010, p. 241-327.

1.3 Onderzoeksmethoden

Om tot een antwoord te komen op de hierboven genoemde vragen is er gebruik gemaakt van literatuur- en jurisprudentieonderzoek. Allereerst is algemene literatuur betreffende AI en de risico's en kansen die daarmee verbonden zijn bestudeerd en geanalyseerd. Voorts is traditioneel juridisch onderzoek gedaan naar literatuur en jurisprudentie inzake bestuurdersaansprakelijkheid en de wijze waarop daar invulling aan wordt gegeven middels de NCGC en COSO 2017.

Ondanks het feit dat AI geen geheel nieuw fenomeen is, is het wel altijd aan ontwikkeling onderhevig waardoor literatuur die een verband legt tussen het recht en AI schaars is. Literatuur die betrekking heeft op het vorenstaande is vaak gericht op een juridisch vraagstuk dat niet specifiek toegespitst is op het verband tussen bestuurdersaansprakelijkheid en AI. Daarnaast zijn rechtelijke uitspraken die betrekking hebben op bestuurdersaansprakelijkheid op grond van onvoldoende risicomanagement relatief schaars, wat logischerwijs met zich meebrengt dat dit voor bestuurdersaansprakelijkheid op grond van onvoldoende risicomanagement inzake AI des te meer het geval is. Er is daarom vrijwel steeds teruggegrepen op juridische literatuur en jurisprudentie die betrekking hebben op bestuurdersaansprakelijkheid in algemene zin, alsmede literatuur en jurisprudentie die betrekking hebben op bestuurdersaansprakelijkheid voor onvoldoende risicomanagement. Dit brengt met zich mee dat er is gekeken naar relevante Nederlandse wet- en regelgeving, parlementaire stukken, jurisprudentie die invulling geeft aan de wet- en regelgeving en (wetenschappelijke) literatuur omtrent bovenstaande onderwerpen. Eveneens is in dit onderzoek gekeken naar rapporten betreffende de NCGC en COSO.

Op deze manier kunnen de deelvragen en uiteindelijk de hoofdvraag worden beantwoord, omdat de beantwoording van de deelvragen middels het uiteengezette traditioneel juridisch literatuur- en jurisprudentieonderzoek een kader met elementen zal geven, waaraan de risico's en kansen van AI getoetst kunnen worden. Dit zal het uiteindelijke antwoord vormen op de vraag of en in hoeverre bestuurders van kapitaalvennootschappen aansprakelijk kunnen zijn voor onvoldoende risicomanagement inzake AI.

1.4 Afbakening

In verband met de richtlijnen voor omvanggrootte van dit onderzoek is gekozen voor het uitwerken van bestuurdersaansprakelijkheid, omdat in het geval dat deze vraag positief beantwoord kan worden, voorzichtig geconcludeerd kan worden dat de vennootschap eveneens aansprakelijk gehouden kan worden. Dat volgt logischerwijs uit de maatstaf voor aansprakelijkheid, omdat deze zwaarder is in het geval van bestuurdersaansprakelijkheid.¹¹

De specifieke toespitsing op kapitaalvennootschappen is te verantwoorden doordat de

¹¹ Waals, van der 2017, 3.4.3.6; HR 20 juni 2008, ECLI:NL:HR:2008:BC4959 (*Willemsen/NOM*).

mogelijkheid om bestuurders aansprakelijk te stellen niet vanzelfsprekend is. Kapitaalvennootschappen hebben, anders dan personenvennootschappen rechtspersoonlijkheid en tevens genieten zij beperkte aansprakelijkheid. Dit houdt in dat een bestuurder de vennootschap weliswaar vertegenwoordigt, maar in beginsel niet hoofdelijk aansprakelijk kan zijn. Daarentegen is een 'bestuurder' van een personenvennootschap wél hoofdelijk aansprakelijk.¹² Op grond van het eerste argument, de zwaardere maatstaf voor bestuurdersaansprakelijkheid, zijn dan ook louter kapitaalvennootschappen van belang voor dit onderzoek.

De gronden voor bestuurdersaansprakelijkheid worden beperkt tot de gronden van art. 2:9 BW en art. 6:162 BW. Art. 2:248 BW zal buiten beschouwing worden gelaten, daar een claim ten aanzien van falend risicomanagement mogelijkserwijs tot faillissement kan leiden, maar dat in beginsel niet noodzakelijkerwijs het geval zal zijn.

De beantwoording van de vraag of het bestuur aansprakelijk gesteld kan worden voor falend risicomanagement inzake AI, is niet afhankelijk van de vraag in hoeverre een individuele bestuurder daarvoor verantwoordelijk kan zijn. Omwille van de complexiteit van het disculpatiebeginsel zal het bestuur ter degen louter als geheel worden behandeld.

¹² Pitlo/Raaijmakers 2017, p. 209.

2. DEFINITIE EN WERKING AI

2.1 Inleiding

In dit hoofdstuk zal een antwoord worden gegeven op de vraag: wat is AI en wat is de werking daarvan, om zo een beeld te schetsen van dit – voor juristen ingewikkeld – onderwerp. Deze beeldvorming is nodig om te kunnen begrijpen welke risico's en kansen met de toepassing van AI gepaard gaan en op welke wijze daar door bestuurders mee om dient te worden gegaan, teneinde bestuurdersaansprakelijkheid te voorkomen. Er wordt daarom eerst een definitie van het begrip AI gegeven, waarna de werking wordt uitgelegd middels een algemeen deel, geïllustreerd met een praktijkvoorbeeld. Voorts wordt afsluitend dieper ingegaan op het onderwerp, middels een uiteenzetting over de kennis- en datagebaseerde benadering en 'weak' versus 'strong' AI.

2.2 Definitie

AI is een veelomvattende term, welke niet staat voor een ingekaderd of tastbaar begrip. Het betreft een verzamelterm, voor 'een reeks methoden en softwaretechnieken (algoritmen en datastructuren) waarmee informatiesystemen worden gebouwd die mentale taken aankunnen.'¹³ In dit kader kunnen mentale taken worden omschreven als taken waarvoor in het algemeen kan worden aangenomen dat voor de uitvoering daarvan *enige vorm* van intelligentie vereist is. De vraag wanneer een systeem intelligent is, werd in de jaren 50 door middel van de Turingtest beantwoord.¹⁴ Deze test is in 1950 ontwikkeld door computerpionier Alan Turing, waarmee een einde kwam aan een lijst die eerder opgesteld was ter kwalificatie van AI, welke vol stond met elkaar tegensprekende kwalificaties. De onderliggende gedachte van deze Turingtest was dat computers of systemen intelligent zijn wanneer deze niet van een mens te onderscheiden zijn. Echter zijn systemen vaak gericht op een specifiek deel van de intelligentie, waar de mens juist een combinatie heeft tussen geest en brein, namelijk het gedrag en de fysiologie.¹⁵ Daarentegen wordt intelligentie in deze zin eveneens gedefinieerd als 'het vermogen om complexe doelstellingen te verwezenlijken', hetgeen erop duidt dat het verwezenlijken van complexe doelstellingen – dus ook op slechts één of meer specifieke gebieden – óók als intelligent wordt gekwalificeerd.¹⁶ Heden ten dage rijst daarom nog steeds de vraag of er reeds systemen ontwikkeld zijn die slagen voor deze Turingtest. In dat licht bezien zou het kwalificeren van AI een uitdaging zijn, waardoor in dit onderzoek zal worden uitgegaan van het vereiste van *enige vorm* van intelligentie.

¹³ Steels e.a. 2018, p. 10.

¹⁴ Duursma 2017, nr. 1.

¹⁵ Poggio 2016, p. 40.

¹⁶ Tegmark 2017, p. 35.

2.3 De werking van AI

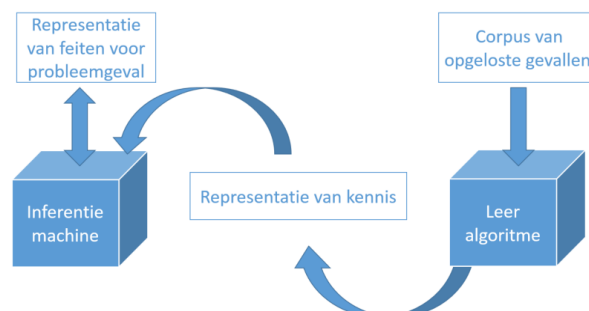
2.3.1 Algemeen

AI kent vele vormen en toepassingen, maar een eenvoudige weergave van de basis die aan bijna alle toepassingen ten grondslag ligt is het proces van informatieverwerking. Deze informatieverwerking is gericht op het vinden van een oplossing of antwoord en kan vergeleken worden met de informatieverwerking van een mens. Een mens verwerkt immers informatie alvorens tot een antwoord of reactie op een vraag of probleem te komen. Vanzelfsprekend moet het probleem duidelijk zijn om tot een passende reactie te komen.

Een typisch AI-systeem kent verschillende elementen, te weten de probleem- en kennisrepresentatie, de inferentiemachine en het leeralgoritme.¹⁷ De representatie is een weergave van het probleem, alsmede van de beschikbare kennis om dat probleem op te lossen. De beschikbare kennis wordt ook wel data genoemd, welke kan bestaan uit tal van elementen. Zo kan statistische data worden gebruikt, maar ook de input van experts en gebruikers van het systeem, eerdere ervaringen met betrekking tot het oplossen van een probleem, enzovoorts. De betreffende data loopt al snel op van duizenden tot honderdduizenden delen welke allen het AI systeem voeden. De kennis van de mens is immers gebaseerd op een immense omvang aan feiten en regels, waarvan we onszelf niet eens bewust zijn. Daarentegen gebruikt de inferentiemachine kennis (data) actief om het probleem op te lossen, door de regels op de feiten toe te passen en deze daarmee uit te breiden. Vervolgens kan middels een leer algoritme, dat feitelijk 'leert' van eerdere situaties en de uitkomsten daarvan, tot een concreet antwoord op een toekomstige vraag of probleem worden gekomen.

Ter illustratie van het bovenstaande wordt in figuur 1 de werking en architectuur van het typische AI-systeem weergegeven. Hierbij wordt onder corpus van opgeloste gevallen verstaan: zowel de data die ter input in het systeem zijn gestopt, alsook de data die het systeem zelf ontwikkelt, op basis van eigen ervaring die is opgedaan bij het oplossen van problemen. Uit figuur 1 kan worden afgeleid dat het systeem gevoed wordt door bestaande kennis en oplossingen in eerdere situaties. Het systeem is dus feitelijk grotendeels afhankelijk van de data waarmee de gebruikers en experts het systeem voeden.

Figuur 1: Architectuur
van een typisch
AI-systeem



¹⁷ Steels e.a. 2018, p.13.

2.3.2 Kennis- en data gebaseerde benadering

De input voor een typisch AI systeem, zoals deze is weergegeven in paragraaf 2.3.1 wordt vormgegeven middels de kennis- of data gebaseerde benadering. De kennis gebaseerde benadering is opgebouwd uit de reeds verworven kennis van bijvoorbeeld menselijke experts, welke in kaart wordt gebracht middels observaties en gesprekken.¹⁸ Het voordeel van een dergelijke benadering is dat uitkomsten en beslissingen van het systeem begrijpelijk blijven voor deze experts. Het nadeel is dat het weergeven van reeds verworven kennis extreem lang duurt en continu aan verandering onderhevig is. Een mens leert immers (bijna) iedere dag iets bij.

De data gebaseerde benadering, ook wel *machine learning* genoemd, wordt gevoed middels statistiek en is in staat tot het herkennen van patronen.¹⁹ De data die hiervoor gebruikt wordt is gebaseerd op het gedrag van mensen en de beslissingen die door de mens worden genomen. Daarnaast kunnen tevens verschijnselen die waargenomen worden via sensoren gebruikt worden voor deze data. Door middel van patroonherkenning en het toepassen van het gevonden patroon op nieuwe problemen, kan een oplossing voor dat probleem gevonden worden.

Heden ten dage bevat een AI systeem veelal een combinatie van verschillende benaderingen en kennisbronnen, omdat intelligentie niet louter door de ene of door de andere benadering verkregen kan worden. Zo zijn kennis gebaseerde technieken nodig om een oplossing rationeel te kunnen beredeneren of weer te kunnen geven op welke wijze zij tot een oplossing komen. Om de grote hoeveelheden data te verwerken en te analyseren zijn tevens data gebaseerde benaderingen nodig.

Deze systemen zijn onder andere gebaseerd op menselijke kennis, waardoor er nog niet gesproken kan worden van een systeem dat op zichzelf kan functioneren, welke daarmee de menselijke kennis en intelligentie overstijgt.²⁰ Op dit moment zijn er bij het ontwerp van het model, alsmede bij de data die voor de training van het model wordt gebruikt, altijd mensen betrokken. Daarnaast kunnen de AI systemen die reeds ontwikkeld zijn vaak hoofdzakelijk gecontroleerd en versterkend leren, waar mensen en dieren dat voornamelijk ongecontroleerd kunnen.²¹

2.3.3 Weak en strong AI

AI systemen kunnen op basis van capaciteiten in twee soorten worden onderscheiden, te weten het zogeheten *weak AI systeem* en *strong AI systeem*.²² Andere benamingen die hiervoor worden gebruikt zijn *narrow* en *deep*. In tegenstelling tot wat de termen doen vermoeden geven *weak* en *strong* niet per definitie de mate van intelligentie weer, maar hebben zij slechts betrekking op de totale capaciteit van een systeem. Zo is *weak AI* gericht op het oplossen van een specifiek probleem. Het systeem is gericht

¹⁸ Steels e.a. 2018, p.18.

¹⁹ Steels e.a. 2018, p. 18.

²⁰ Steels e.a. 2018, p. 20-21.

²¹ O'Reilly 2018, p. 135-136.

²² Duursma 2017, nr. 1.

op het functioneren binnen een vooraf ingestelde bandbreedte, vaak op basis van een kennis gebaseerd systeem. Het systeem wordt gevoed op basis van menselijke kennis, die voornamelijk bestaat uit feiten en regels. Het systeem past vervolgens deze regels toe op een specifieke situatie.

Daarentegen bevat *strong AI* kwalificaties die relateren aan de menselijke intelligentie, doordat zij goed, althans beter om kunnen gaan met onverwachte situaties dan een *weak AI systeem*. In dit kader wordt vaker de term *deep learning* gebruikt, welke staat voor een leermechanisme van meerdere lagen van zogeheten kunstmatige neurale netwerken. De inspiratie voor deze netwerken is afkomstig uit de hersencellen van levende wezens. Zo is de organisatie van onze hersenschors vergelijkbaar met *deep learning* netwerken, voor zowel zintuigelijke als motorische systemen.²³ *Deep learning* is een van de vier onderdelen van *machine learning*, hetgeen in paragraaf 2.3.2 is uitgelegd.²⁴ Niet louter op basis van bestaande kennis, maar op basis van patroonherkenning en big data-analyse komt een *deep learning* machine tot een gepast antwoord.²⁵ Tevens is een dergelijk systeem in staat complexe ideeën te begrijpen en kan het zichzelf snel nieuwe dingen leren, onder andere uit eerder opgedane ervaringen.²⁶ Het systeem wordt steeds slimmer doordat de lagen van deze neurale netwerken samenwerken.

2.4 Conclusie

Wat is AI en hoe werkt AI?

AI betreft een reeks methoden en softwaretechnieken (algoritmen en datastructuren) waarmee informatiesystemen kunnen worden gebouwd die mentale taken aan kunnen. Dit houdt in dat enige vorm van intelligentie daarvoor vereist is. Zo'n informatiesysteem is doorgaans opgebouwd uit een probleem- en kennisrepresentatie, een inferentiemachine en een leeralgoritme.

De input voor zo'n systeem komt voort uit de kennis- of data gebaseerde benadering, waarbij de kennis gebaseerde benadering stoelt op input vanuit experts en degene die het systeem gebouwd heeft en de data gebaseerde benadering stoelt op extreem grote hoeveelheden data. De systemen die momenteel gebruikt worden zijn vaak gebaseerd op zowel kennis als data, omdat intelligentie niet door het een óf het ander bereikt kan worden.

Tot slot valt het onderscheid te maken tussen *weak* en *strong AI*, ofwel *narrow* en *deep AI*. *Deep AI* is voor de toepassingen die momenteel gebruikt worden het meest relevant. Het staat ook wel bekend als *deep learning*, welke staat voor een leermechanisme van meerdere lagen van kunstmatige neurale netwerken. Middels patroonherkenning kan een algoritme zelf leren, en stukjes bruikbare kennis doorgeven aan de volgende laag in het neurale netwerk. Uiteindelijk zal dit leiden tot een oplossing voor een bepaald probleem.

²³ Sejnowski 2019, p. 32.

²⁴ Duursma 2017, nr. 1.

²⁵ Steels e.a. 2018, p. 19.

²⁶ Duursma 2017, nr. 1.

3. TOEPASSING, RISICO'S EN KANSEN AI

3.1 Inleiding

Recente ontwikkelingen wijzen erop dat het gebruik van AI alsmaar zal blijven toenemen, omdat het reeds op vele plekken succesvol wordt toegepast en deze toepassing grote besparingen en nieuwe mogelijkheden oplevert.²⁷ Om die redenen wordt AI door haar vele verschijnings- en toepassingsvormen reeds door tal van kapitaalvennootschappen uit verschillende werkgebieden en branches gebruikt.²⁸ Uit onderzoek blijkt dat de bedrijven in Nederland zelfs lichtelijk voorop lopen in het gebruik van AI, zo kopt RTL Z: 'Nederlandse bedrijven lopen voor in kunstmatige intelligentie'.²⁹

Met het gebruik van AI in kapitaalvennootschappen gaan risico's gepaard, welke afhankelijk zijn van de vorm van AI die gebruikt wordt. Zo zou het mogelijk kunnen zijn dat de meest verregaande vorm van AI, *deep learning*, zou kunnen ontwikkelen tot 'superintelligentie'. Belangrijke namen in de AI wereld; Stephen Hawking, Elon Musk, Peter Norvig en Nick Bostrom waarschuwen al langer voor deze vorm van AI, omdat het daarbij om een vorm van intelligentie gaat die voor de mens niet meer te bevatten zou zijn. De samenleving zou dermate veranderen dat deze voor mensen niet meer te volgen is.³⁰

Echter, van een dergelijke vorm van AI is tot op heden (nog) geen sprake. De benadrukking van deze risico's is daarom dikwijls overdreven. Tevens leidt het af van de daadwerkelijke risico's die het gebruik van AI in het algemeen met zich meebrengt. In dit kader worden oneigenlijk gebruik, onbetrouwbaarheid, gebrek aan transparantie en verantwoordelijkheid en de schending van grondrechten en ethische principes genoemd als voornaamste risico's.³¹

In dit hoofdstuk wordt een antwoord gegeven op de vraag hoe AI toegepast wordt binnen kapitaalvennootschappen en welke risico's en kansen daarmee gepaard gaan, om zo uiteindelijk in kaart te kunnen brengen welke maatregelen getroffen dienen te worden teneinde bestuurdersaansprakelijkheid te voorkomen. Hiertoe worden eerst de toepassingen van AI aan de hand van verschillende sectoren uiteengezet, waarna de risico's en kansen betreffende deze toepassingen worden toegelicht.

3.2 Toepassing AI in kapitaalvennootschappen

De RTL Z kop 'Nederlandse bedrijven lopen voor in kunstmatige intelligentie' schept hoge verwachtingen ten aanzien van het gebruik van AI in Nederlandse vennootschappen. De mate waarin

²⁷ Harbers 2018, p. 14.

²⁸ Duursma 2017, nr. 2.

²⁹ Teunis, *RTL Z*, 2 oktober 2018.

³⁰ Duursma 2017, nr. 5.

³¹ Steels e.a. 2018, p. 34.

gebruik wordt gemaakt van AI is zeer sectorafhankelijk. Niet alleen de vraag óf er gebruik wordt gemaakt van AI is daarbij van belang, maar eveneens in hoeverre dit gebruik gevorderd is. De mate waarin het gebruik als gevorderd valt aan te merken is afhankelijk van de vorm van AI (bijvoorbeeld *narrow* of *deep*) en in hoeverre deze vorm daadwerkelijk wordt gebruikt in het bedrijfsproces.

Uit onderzoek van EY in opdracht van Microsoft blijkt dat bedrijven in de sector *hospitality & services*, waar bijvoorbeeld klantenservice onder valt, het meeste gebruik maken van gevorderde AI. Daarentegen wordt in de sector infrastructuur op geen enkele wijze gebruik gemaakt van gevorderde AI. Wat in ieder geval vast staat, is dat het overgrote deel van Europese bedrijven bezig is met AI, bijvoorbeeld door middel van pilotprojecten of reeds door volledige implementatie van AI in de onderneming.³²

Concreet gezien wordt AI in ondernemingen toegepast om te anticiperen op gebeurtenissen en uitkomsten, om taken uit te voeren zonder menselijke tussenkomst, om patronen en trends te identificeren en te begrijpen, om te personaliseren en om oplossingen ten aanzien van problemen voor te stellen.³³ Een belangrijke kanttekening die hierbij gemaakt dient te worden is dat de implementatie van AI in Nederlandse vennootschappen er tot op heden met name op is gericht het werk van de mens gemakkelijker te maken. Het wordt in dat kader ingezet ter ondersteuning.³⁴

3.2.1 Service en Hospitality

De sector service en hospitality is de sector waarvan verwacht wordt dat deze de meeste impact van de toepassing van AI zal ondervinden.³⁵ Heden ten dage wordt veelal gebruik gemaakt van zogeheten 'chatbots' die de eerste antwoorden geven op vragen van klanten. Middels categorisering van een vraag, komt deze bij de juiste, gespecialiseerde medewerker terecht. Hierdoor kunnen vragen sneller en beter worden beantwoord en kunnen vele gesprekken naast elkaar worden gevoerd. Een chatbot wordt immers nooit moe. Een ontwikkeling die hierbij op de loer ligt, is dat de chatbots zélf antwoord zullen geven op de meest gestelde vragen van klanten. Daarnaast zullen in de zeer nabije toekomst door de chatbot suggesties worden gegeven over te geven antwoorden, oplossingen of nieuwe producten die kunnen worden aangeboden.³⁶

3.2.2 Financiële dienstverlening

In de financiële dienstverlening wordt op tal van verschillende wijzen gebruik gemaakt van AI. AI wordt gebruikt om zelfstandig op de beurs te handelen, door het doen van aan- en verkopen van aandelen en obligaties tegen een gunstige waarde. In dit licht bezien wordt het als middel ingezet om taken uit te voeren zonder menselijke tussenkomst, een van de meest verregaande vormen van AI. Ook wordt het

³² *Artificial Intelligence in Europe* 2018, p. 30.

³³ *Artificial Intelligence in Europe* 2018, p. 43.

³⁴ Teunis, RTL Z, 2 oktober 2018.

³⁵ *Artificial Intelligence in Europe* 2018, p. 39.

³⁶ Duursma 2017, nr. 2.

ingezet als hulp bij het nemen van financiële beslissingen, zoals bij het verstrekken van een lening. AI beoordeelt in dat geval of de aanvrager voldoende kredietwaardig is en in hoeverre deze een risico vormt op wanbetaling. Daarnaast wordt AI frequent toegepast voor KYC, waarbij klanten gescreend worden. Onder andere de Wft en de Wwft brengen deze verplichting met zich mee. Voorheen werd dit voornamelijk gedaan door middel van het invullen van vragenlijsten, maar heden ten dage wordt AI daarvoor ingezet, zodat het proces van analyseren veel sneller en preciezer verloopt. Op deze manier kan enerzijds vooraf worden bepaald of een klant een bepaald risico vormt, door middel van voorspelling, maar anderzijds ook of er bijvoorbeeld daadwerkelijk terrorismefinanciering, fraude of witwaspraktijken plaats vinden. Door middel van patroonherkenning kunnen bijvoorbeeld abnormale transacties worden gedetecteerd, waarmee bovenstaande gevallen aan het licht komen. Een ander voorbeeld van AI in de financiële sector is dat klanten een betere financiële planning kunnen maken op basis van hun eigen voorkeuren, waarbij het principe van personaliseren wordt gebruikt. AI kan in dat geval gezien worden als super persoonlijke bankmedewerker.³⁷

3.2.3 Retail

AI systemen zijn steeds beter in staat om data uit verschillende bronnen aan elkaar te koppelen, zodat er een uitgebreid en gedetailleerd profiel van de klant gemaakt kan worden. Het AI systeem kent de klant daardoor in sommige gevallen nog beter dan dat de klant zichzelf kent. Op deze manier kunnen automatisch producten en diensten aangeboden worden die passen bij de klant. Deze inzichten kunnen zelfs leiden tot nieuwe verdienmodellen en producten. Op basis van al deze informatie kan worden voorspeld wat voor beslissing de klant zal maken en kan deze beslissing zelfs worden beïnvloed.³⁸ Gesteld kan daarom worden dat in de retail, maar ook in andere sectoren waarin producten of diensten verkocht worden, zoals bijvoorbeeld het verzekeringswezen, reeds veelvuldig gebruik gemaakt wordt van AI. Dit begint al bij de zogeheten ‘cookies’ waar big datasets mee verzameld kunnen worden.

3.2.4 Gezondheidszorg

In de gezondheidszorg en meer specifiek in de geneeskunde, is de hoeveelheid kennis de laatste jaren enorm toegenomen. Deze kennis is geen entiteit op zichzelf, het betreft een samenhang tussen verschillende medische kennisgebieden, die vaak vele lacunes en tegenstrijdigheden kennen. Deze worden in de normale praktijk opgevangen door middel van praktijkervaring. Medische beslissingen worden daarom veelal op basis van gevoel genomen, in plaats van een op logische redenering gebaseerde probleemoplossing. Bovenstaande leidt ertoe dat de geneeskunde steeds moeilijker te overzien wordt voor de mens.³⁹ Om die reden wordt met name op het gebied van medische diagnose AI technologie toegepast. Op deze manier kan in grote hoeveelheden medische teksten gezocht worden

³⁷ Duursma 2017, nr. 2.

³⁸ Duursma 2017, nr. 2.

³⁹ Schreiber, *TGP* 1986/2, p. 28-31.

naar situaties die overeenkomen met de situatie van de patiënt. Op die wijze kan vastgesteld worden wat de patiënt mankeert en wat de beste behandelwijze in dat geval zal zijn.⁴⁰ Ook in beeldverwerking wordt AI op grote schaal toegepast. Grote sets MRI, röntgen en CT beelden met de daarbij behorende interpretaties worden gescreend op patronen.⁴¹ De ervaring en de superieure intelligentie van de arts wordt hierbij wel als cruciaal gezien, zodat enige vorm van controle gewaarborgd blijft.

3.2.5 Vervoer en transport

In de sectoren vervoer en transport is het meest gebruikte voorbeeld van AI van groot belang: de zelfrijdende auto. Hoewel het daadwerkelijke gebruik van de geheel zelfrijdende auto tot op heden beperkt is, kan dit binnen afzienbare tijd veranderen.⁴² De zelfrijdende auto is namelijk volop in ontwikkeling en wordt gezien als voorloper van andere autonome voertuigen, zoals schepen, vliegtuigen, vrachtwagens en bestelbusjes.⁴³ Vandaag de dag wordt in verschillende vervoersmiddelen reeds gebruik gemaakt van enige vorm van autopilot, zoals in de Volvo XC90(pilot assist), welke boordevol *deep learning* zit. Over slechts twee jaar wil Volvo zelfs geheel autonoom rijdende auto's aan kunnen bieden, wat illustreert dat deze ontwikkeling binnen kort tijdsbestek kan plaatsvinden.⁴⁴

3.2.6 Juridische dienstverlening

Deep learning wordt nog maar zelden toegepast in de advocatuur en de juridische advieswereld, echter is het zeer waarschijnlijk dat het routinewerk dat vaak door juridisch medewerkers wordt gedaan (deels) overgenomen zal worden door AI. Het onderzoeken van documenten en gegevens op mogelijk bewijs en ondersteuning van een zaak kan simpelweg uitgevoerd worden door het systeem, omdat deze gemakkelijk duizenden documenten kan doorzoeken. Daarnaast kunnen deze systemen helpen om juridisch advies beschikbaar te maken voor degenen die zich geen advocaat kunnen veroorloven.⁴⁵

3.2.7 Interne toepassingen

AI wordt niet louter te overstaan van externe partijen gebruikt, ook interne vraagstukken kunnen worden opgelost middels het gebruik van AI. Zo worden beslissingen door het bestuur ten aanzien van strategie niet zelden gemaakt op basis van AI, waarbij bijvoorbeeld gekeken wordt naar de uitkomst van een voorspelling, waarmee geanticipeerd kan worden op de toekomst van de onderneming. Ook kunnen oplossingen die door AI worden geboden ten aanzien van een bepaald probleem, door het bestuur worden overgenomen.⁴⁶ Daarnaast wordt het bijvoorbeeld ingezet voor werving en selectie van personeel. Op deze manier worden niet alleen de standaardcriteria zoals competenties, opleiding en

⁴⁰ Steels e.a. 2018, p. 12.

⁴¹ Sejnowski 2019, p. 9-11.

⁴² Sejnowski 2019, p. 5.

⁴³ Duursma 2017, nr. 2.

⁴⁴ Verheggen, *Duurzaam bedrijfsleven* 28 juni 2017.

⁴⁵ Sejnowski 2019, p.13.

⁴⁶ *Artificial Intelligence in Europe* 2018, p. 34-35.

dergelijke gescreend, maar kunnen ook andere patronen worden ontdekt, op basis waarvan een geschikte kandidaat wordt gevonden.⁴⁷

3.3 Risico's van het gebruik van AI

3.3.1 Oneigenlijk gebruik

Wanneer toepassingen van AI gebruikt worden in situaties waarvoor het systeem – gekeken naar de ontwikkeling daarvan – eigenlijk (nog) niet geschikt is, kan er worden gesproken van oneigenlijk gebruik. In dat geval kunnen resultaten en oplossingen afkomstig uit het systeem onbetrouwbaar en in sommige gevallen zelfs gevaarlijk zijn. Voorafgaand aan het implementeren van een dergelijk systeem moet dus voorzichtigheid worden betracht ten aanzien van het doel van het AI systeem.⁴⁸

3.3.2 Interne onbetrouwbaarheid

Naast het oneigenlijke gebruik van AI, vormt de onbetrouwbaarheid van een AI systeem een belangrijk risico. Daarin worden interne- en externe betrouwbaarheid onderscheiden, waarbij de interne onbetrouwbaarheid met name schuilt in de programmering en de voeding (data) van het systeem. De programmeur van een algoritme kan onbedoeld een algoritme programmeren dat bevooroordeeld is, doordat de programmeur zelf onbewust enige vorm van bevooroordeeldheid heeft. Een nog groter risico op vooroordelen schuilt in de datasets die gebruikt worden om het systeem te voeden. Immers, wanneer de gegevens die ingevoerd worden de geschiedenis weergeven, wordt het programma gevraagd om de vooroordelen van de mens aan te leren.⁴⁹ Dit leidt vervolgens tot beslissingen van het AI systeem die niet volledig zuiver zijn. Vorenstaande speelt een zeer grote rol bij kennis gebaseerde systemen, omdat deze louter op kennis van experts stoelt. Het lijkt in dat geval dan ook onoverkomelijk een systeem te produceren met minimaal enige vorm van bevooroordeeling.

3.3.3 Externe onbetrouwbaarheid: Cyberrisico's

Naast de interne onbetrouwbaarheid van AI-systemen, wordt de externe onbetrouwbaarheid eveneens als belangrijk risico gezien. De externe betrouwbaarheid wordt in twijfel getrokken omdat beslissingen mogelijk gebaseerd kunnen zijn op eventuele bedreigingen, zoals hacker- en cyberaanvallen van buitenaf. Cyberincidenten kunnen namelijk een systemische invloed hebben, bijvoorbeeld door het onderbreken van een bepaald proces of het manipuleren van gegevens die het systeem voeden.⁵⁰ In sommige gevallen wordt het bedrijf zelfs blootgesteld aan diefstal van intellectueel eigendom of privacygegevens.⁵¹

⁴⁷ Hiemstra & Nevels 2018, p. 1.

⁴⁸ Steels e.a. 2018, p. 35.

⁴⁹ Duursma 2017, nr. 5.

⁵⁰ *De transitie naar een digitale samenleving* 2017, p. 36.

⁵¹ Schatsky, Davenport & Loucks 2018.

3.3.4 Interpreteerbaarheid

Het gebrek aan mogelijke interpretatie van uitkomsten en oplossingen die AI kan bieden, vormt eveneens een gedegen risico. Zo bestaat er enerzijds het gevaar dat een *deep learning* systeem, zoals in paragraf 2.3.3 beschreven is, in staat is om complexe ideeën te begrijpen en zichzelf razendsnel nieuwe dingen te leren. Zo snel dat het voor de experts niet altijd mogelijk is om te achterhalen op welke wijze het systeem tot een beslissing is gekomen. Daarnaast is het – met name bij data gebaseerde systemen – voor degenen die de impact van zo’n beslissing ondergaan, moeilijk om deze te interpreteren en te begrijpen.⁵² Dit is bijvoorbeeld van belang bij de toepassing van AI in geval van bijvoorbeeld financiële beslissingen en verzekeringen. Een dergelijke beslissing moet immers verklaarbaar zijn om hem aan te kunnen vechten. Hiertoe is bijvoorbeeld in de Algemene Verordening Gegevensbescherming (hierna: AVG) expliciet het recht op uitleg opgenomen.

3.3.5 Transparantie

Het vijfde risico is gebaseerd op het gebrek aan transparantie van een AI systeem. Dit risico sluit aan bij het risico betreffende de interpreteerbaarheid, omdat door het gebrek aan transparantie een bepaalde beslissing moeilijk of zelfs onmogelijk te interpreteren is. Dit komt doordat een *deep learning* systeem als een soort ‘black box’ functioneert, waarbij aan de ene kant een vraag wordt gesteld en er aan de andere kant een antwoord uitkomt. De wijze waarop het systeem tot een antwoord is gekomen is niet zichtbaar, doordat dit zich in de zogeheten ‘black box’ bevindt.⁵³ Daarnaast is deze transparantie niet alleen belangrijk voor de verantwoording van bepaalde uitkomsten, maar eveneens voor het bepalen of er al dan niet sprake is van een ‘hack’ van het systeem. Doordat het in sommige gevallen niet geheel duidelijk is wat aan een uitkomst ten grondslag ligt, is een hack lastig op te sporen, met name in het geval van een slechts lichtelijk afwijkende beslissing. Door middel van duizenden tests zou het theoretisch mogelijk moeten zijn om te ontdekken wat een systeem aanmerkt als zijnde belangrijk voor het nemen van een bepaalde beslissing. Zo ver zijn de ontwikkelingen echter nog niet.

3.3.6 Verantwoordelijkheid

De vraag wie de verantwoordelijkheid draagt bij beslissingen genomen door een AI systeem, is een van de grootste onderwerpen van discussie. De capaciteit tot het nemen van beslissingen, zoals in de vorige alinea’s uiteen is gezet, is namelijk niet het enige waarvoor AI gebruikt wordt. Wanneer AI ingebed is in een fysiek systeem, zoals een zelfrijdende auto, heeft het de mogelijkheid om autonome beslissingen te nemen, die omgezet worden in acties in de ‘echte’ wereld. Dit kan grote gevolgen hebben wanneer zo’n auto een ongeluk veroorzaakt, omdat het – wegens het gebrek aan transparantie en interpreteerbaarheid – bijna onmogelijk is een verantwoordelijke aan te wijzen. De vraag wie er in dat

⁵² Steels e.a. 2018, p. 35.

⁵³ Duursma 2017, nr. 5.

geval aansprakelijk is, is nog altijd een onderwerp van discussie.⁵⁴ Deze vraag omtrent verantwoordelijkheid kan echter niet vergeleken worden met de vraag of bestuurders van kapitaalvennootschappen verantwoordelijk kunnen zijn voor falend risicomanagement inzake AI, omdat deze vraag zich richt op het beheersingssysteem waarvoor de bestuurder verantwoordelijk is en niet op het gebruik van AI op zichzelf.

3.3.7 Grondrechten en ethische principes

Twee van de belangrijkste risico's van het gebruik van AI in een kapitaalvennootschap zijn de potentiële schending van grondrechten en ethische principes. Het grondrecht op privacy is het recht ten aanzien waarvan de grootste risico's bestaan.⁵⁵ Een AI systeem moet immers met extreem grote hoeveelheden (privacygevoelige)data worden gevoed.⁵⁶ Met dit grondrecht gaan het recht op persoonlijke autonomie en menselijke waardigheid gepaard.⁵⁷ Het recht op privacy is in Nederland opgenomen in art. 10 – 13 Gw en daarbuiten in onder andere art. 8 EVRM, art. 7 EU-Grondrechtenhandvest en art. 17 IVBPR. Voor het verdere onderzoek worden de internationale rechten buiten beschouwing gelaten. Art. 10 Gw, het recht op eerbiediging van de persoonlijke levenssfeer, is het meeste van belang in het kader van het gebruik van AI. Het recht op bescherming van persoonsgegevens is daar onderdeel van.⁵⁸ Dit zal nader worden besproken bij het risico op schending van wet- en regelgeving in paragraaf 3.3.8 en 4.4.1.

Daarnaast bestaat met name in het geval dat AI wordt gebruikt voor het nemen van beslissingen, het risico op schending van het recht op gelijke behandeling en non-discriminatie.⁵⁹ Het gebrek aan interpretatie en transparantie van deze beslissingen alsmede de mogelijke interne onbetrouwbaarheid van een systeem, kan er toe leiden dat het recht op gelijke behandeling wordt geschonden. Wanneer een AI systeem bevooroordeeld is – hetgeen blijkt uit paragraaf 3.3.2 zonder meer mogelijk is – kan dit leiden tot ongerechtvaardigde ongelijke behandeling, waarbij mogelijk eveneens procedurele rechten worden geschonden.⁶⁰ Het vorenstaande grondrecht is algemeen vervat in art. 1 Gw, alsmede in art. 14 EVRM en art. 26 IVBPR. In lagere regelgeving zijn deze rechten meer specifiek vervat. Deze zullen in paragraaf 3.3.8 nader aan bod komen.

De risico's op schending van ethische principes kunnen zich verwezenlijken doordat een AI-systeem onvoorspelbaar kan zijn en in de meeste gevallen geprogrammeerd is tot het bereiken van een bepaald doel, zonder de ethische implicaties te gebruiken die een mens aan een beslissing ten grondslag legt. Het gebrek aan deze implicaties kan bijvoorbeeld leiden tot discriminatie, schending van privacy-

⁵⁴ Schatsky, Davenport & Loucks 2018.

⁵⁵ Vetzo, Gerards & Nehmelman 2018, p. 123.

⁵⁶ Schatsky, Davenport & Loucks 2018.

⁵⁷ Vetzo, Gerards & Nehmelman 2018, p. 53.

⁵⁸ Vetzo, Gerards & Nehmelman 2018, p. 54.

⁵⁹ Vetzo, Gerards & Nehmelman 2018, p. 79.

⁶⁰ Vetzo, Gerards & Nehmelman 2018, p. 188.

rechten en het creëren en verspreiden van valse informatie.⁶¹ Schending van ethische principes gaat derhalve vaak gepaard met grondrechtenschendingen. Het gebrek aan ethische implicaties bestaat doordat een AI systeem vaak door verschillende experts ontworpen wordt tot het dienen van een bepaald doel, zonder dat voldoende gekeken wordt naar de impact van de oplossingen op gebruikers, stakeholders en de samenleving.⁶² De zogeheten ‘ontwerpers’ van een AI systeem bestaan voornamelijk uit: programmeurs om software te ontwikkelen, ingenieurs om de eventuele hardware te bouwen en AI-wetenschappers en datawetenschappers om de toepassing intelligent te maken. Echter is ook kennis nodig over ethiek en ontwerp, om de AI toepassingen op verantwoorde wijze te kunnen ontwerpen.

3.3.8 Wet- en regelgeving

Zoals eerder uiteengezet in dit hoofdstuk, kunnen AI toepassingen onbetrouwbaar, moeilijk te interpreteren en weinig transparant zijn. Deze risico's brengen met zich mee dat er eveneens een gegrond risico op non-compliance met wet- en regelgeving bestaat. Met name de privacy en uitlegbaarheid spelen daarbij een grote rol, omdat AI toepassingen gevoed dienen te worden met extreem grote hoeveelheden gegevens.⁶³ Nadere regelgeving hieromtrent, is vastgelegd in de AVG. Dit is dan ook de enige regelgeving die specifiek op het daadwerkelijke gebruik van AI van toepassing is. Dit aspect zal daarom nader worden toegelicht in paragraaf 4.4.1. Daarnaast bestaat wetgeving die weliswaar niet specifiek gericht is op het gebruik van AI, maar die daarvoor wel relevant is. Zo bestaat er een risico op non-compliance met de Algemene wet gelijke behandeling, welke discriminatie op grond van bijvoorbeeld nationaliteit, geslacht en godsdienst verbiedt. Daarnaast bestaat meer specifieke wetgeving, waaronder de Wet gelijke behandeling op grond van leeftijd bij de arbeid en – van handicap en chronische ziekte. Ook valt te denken aan specifieke wetgeving voor bepaalde sectoren, bijvoorbeeld voor de gezondheidszorg en financiële dienstverlening. Een onbetrouwbaar AI systeem ten aanzien van KYC, kan bijvoorbeeld schending van de Wft en/of de Wwft opleveren.

3.4 Kansen AI

De CEO van Google, Sundar Pichai noemde AI in 2018 ‘de grootste kans die de mensheid heeft’.⁶⁴ Waar in paragraaf 4.3 uitsluitend wordt gesproken over de risico's die met het gebruik van AI in kapitaalvennootschappen gepaard gaan, zal deze paragraaf daarom de keerzijde daarvan belichten. Het gebruik gaat namelijk niet louter met risico's gepaard, maar kan in het algemeen, alsmede ten aanzien van risico's juist mogelijkheden en kansen bieden.

⁶¹ Schatsky, Davenport & Loucks 2018.

⁶² Harbers 2018, p.47-48.

⁶³ Schatsky, Davenport & Loucks 2018.

⁶⁴ Bremmer, *Algemeen Dagblad* 11 januari 2018.

3.4.1 Kostenbesparing en innovatie

Zoals eerder betoogd zijn er tal van AI toepassingen die vandaag de dag ingezet worden om bijvoorbeeld het werk van mensen uit handen te nemen. In dat licht bezien kan worden gesteld dat AI bepaalde specifieke taken van de mens over kan nemen, waardoor bijvoorbeeld de efficiëntie van die taak wordt verhoogd. Het voorgaande gaat doorgaans gepaard met kostenbesparingen, hetgeen ten gunste kan komen van het bedrijfsresultaat van de onderneming. Een specifiek voorbeeld daarvan is het potentiële voordeel dat AI oplevert in productieprocessen van fabrieken. Door middel van algoritmen kan het proces geoptimaliseerd worden, waardoor kostenbesparing voor de hand ligt. Daarnaast kan optimalisatie eveneens leiden tot een verbeterd eindproduct, dat mogelijk het bedrijfsresultaat ten goede komt en het risico op gebrekkige producten verkleint. Daarnaast kan een algoritme gebruikt worden om te voorspellen wanneer preventief onderhoud plaats dient te vinden aan de machines.⁶⁵ Een ander voorbeeld is de inzet van chatbots in de klantenservice. Door de beantwoording van eerstelijns vragen is minder personeel benodigd en kunnen moeilijkere vragen op efficiënte wijze gealloceerd worden naar de juiste medewerker. Ook dit levert een reductie van personeelskosten op. Daarnaast biedt AI grote kansen om te (blijven) innoveren binnen een onderneming, om zo te anticiperen op de toekomst, alsmede om te kunnen (blijven) concurreren met andere ondernemingen in dezelfde sector.

3.4.2 AI 'ziet' meer

AI biedt niet louter kansen ten aanzien van kostenbesparing en innovatie. Het biedt eveneens kansen ten aanzien van potentiële risico's, omdat AI meer 'ziet' dan dat de mens kan zien. Door middel van *deep learning* systemen en de patroonherkenning die daarmee gepaard gaat, kunnen voorspellingen worden gedaan en beslissingen worden genomen, die de menselijke capaciteit te boven gaan.

Naast de risico's betreffende de toepassing van AI in de onderneming, bestaan tal van andere risico's die gepaard gaan met de overige bedrijfsprocessen en -activiteiten. Hierbij valt te denken aan risico's ten aanzien van de bedrijfsdoelstellingen, maar ook ten aanzien van compliance met wet- en regelgeving.

Gekeken naar de risico's ten aanzien van de bedrijfsdoelstellingen, kan bijvoorbeeld worden gedacht aan inkooprisico's. Wanneer een onderneming een onjuist inkoopbeleid heeft, kan dat grote financiële gevolgen hebben. AI kan hier oplossing bieden, doordat het klantbehoeften kan voorspellen en mogelijk zelfs sturen, zodat een efficiënt inkoopbeleid kan worden gerealiseerd, waarmee de risico's worden gereduceerd.⁶⁶ Ook kunnen beleggingsrisico's van financiële instellingen worden beperkt, doordat een AI systeem autonoom kan beleggen binnen een vooraf bepaald kader. Minieme aanwijzingen voor koerswisseling kunnen worden gedetecteerd, waardoor het systeem te allen tijde

⁶⁵ Duursma 2017, nr. 2.

⁶⁶ Duursma 2017, nr. 2.

sneller en effectiever kan handelen dan de mens.⁶⁷ Het laatste voorbeeld betreft de mogelijkheid om AI in de vorm van een robot, deel uit te laten maken van het bestuur, of een adviserende rol aan te laten nemen ten aanzien van het bestuur. Zo worden in Hongkong en Finland reeds robots gebruikt om te adviseren over of zelfs mee te laten beslissen in investeringsbesluiten.⁶⁸ Op deze manier kunnen in deze besluiten door middel van grote hoeveelheden data betere afwegingen en voorspellingen worden gemaakt. Hiermee wordt het risico op het doen van verkeerde investeringen – die van grote invloed kunnen zijn op de bedrijfsdoelstellingen – ingeperkt.

Een andere kans van AI is bijvoorbeeld de mogelijkheid om het risico op een verkeerde diagnose in te perken door middel van *deep learning*, doordat een algoritme een betere en snellere diagnose kan stellen dan een arts. Dit is mogelijk omdat extreem grote hoeveelheden data kunnen worden geanalyseerd, op basis van de gegevens van de specifieke patiënt. Opvallende oneffenheden kunnen door middel van patroonherkenning sneller worden gesignaleerd.⁶⁹ Een voorbeeld daarvan is het *deep learning* algoritme van Zebra Medical, welke op basis van afbeeldingen sneller én accurater wervelfacturen kan vaststellen dan mensen.⁷⁰ Het stellen van een juiste diagnose is echter niet het enige voordeel. Een snellere diagnose zal tot tijdsbesparing bij de arts leiden, maar ook tot een besparing van de aan te wenden middelen om de diagnose te stellen. Het vorenstaande zou tot een kostenreductie in de zorgsector kunnen leiden, waardoor een deel van de publieke gelden elders besteed kunnen worden. Vanuit een ander perspectief bekeken zou de tijdsbesparing artsen in staat kunnen stellen om zich meer bezig te houden met de menselijke aspecten zoals empathie, ethische vraagstukken en emotionele ondersteuning van de patiënten.⁷¹ Daarnaast biedt AI mogelijkheid tot het verbeteren van de kwaliteit en toegankelijkheid van de zorg.⁷²

Ten aanzien van compliance met wet- en regelgeving kan een voorbeeld gevonden worden in het gebruik van AI voor KYC. Zoals eerder uitgelegd zijn financiële instellingen verplicht te voldoen aan de Wft en Wwft. AI biedt in dit opzicht tal van kansen, omdat de algoritmes veel sneller afwijkende patronen kunnen herkennen. Daarnaast herkent het patronen die, door de extreem grote hoeveelheden data, voor een mens niet grijpbaar zijn.

Middels bovenstaande voorbeelden kan dan ook zonder meer worden gesteld dat AI niet louter risico's met zich meebrengt, maar ook bijdraagt aan de reductie van risico's betreffende bijvoorbeeld bedrijfsdoelstellingen, het stellen van diagnoses en compliance met wet- en regelgeving.

⁶⁷ Duursma 2017, nr. 2.

⁶⁸ Hijink, *OR* 2019/3, afl. 1, p. 10-11.

⁶⁹ Duursma 2017, nr. 2.

⁷⁰ Duursma 2017, nr. 1.

⁷¹ Steels e.a. 2018, p. 23.

⁷² *Waarde(n)volle zorgtechnologie* 2019, p. 9.

3.5 Conclusie

Hoe wordt AI toegepast binnen kapitaalvennootschappen en welke risico's en kansen gaan daarmee gepaard?

AI wordt heden ten dage in tal van verschillende sectoren, op tal van verschillende wijzen toegepast. Vaak gaat het bij de toepassing om een vorm van zogeheten *deep learning*, de meest verregaande vorm van AI. Deze methode wordt gebruikt om te anticiperen op gebeurtenissen en uitkomsten, om taken uit te voeren zonder menselijke tussenkomst, om patronen en trends te identificeren en te begrijpen, om te personaliseren en om oplossingen ten aanzien van problemen voor te stellen. Veel van deze taken gebeuren – nu nog – onder het toezicht van de mens en dienen slechts ter vergemakkelijking, verbetering of versnelling van processen binnen een onderneming. In sommige gevallen wordt verregaande AI toegepast, waarbij tussenkomst of ondersteuning van de mens minder plaats vindt. Het is echter niet ondenkbaar, zelfs enigszins waarschijnlijk, dat AI in de nabije toekomst steeds meer het geval zal zijn.

De belangrijkste risico's van het gebruik van AI systemen en oplossingen in kapitaalvennootschappen zijn: oneigenlijk gebruik, de interne- en externe onbetrouwbaarheid, het gebrek aan transparantie en verantwoordelijkheid en het risico op de schending van wet- en regelgeving en ethische principes. De verwezenlijking van dergelijke risico's wordt waarschijnlijker naarmate een meer uitgebreide, diepgaande vorm van AI wordt gebruikt in de onderneming. Gezien het veelvuldige gebruik van *deep learning* is de kans op verwezenlijking van deze risico's zonder meer aanwezig. De mate waarin AI in de onderneming is geïncorporeerd en toegepast speelt hierbij echter een belangrijke rol, omdat het geval waarin AI louter gebruikt wordt ter aanvulling op de menselijke handeling of beslissing minder verregaande risico's met zich mee brengt dan wanneer een AI systeem op zichzelf functioneert. De menselijke factor zorgt immers voor enige controle of aanvulling door de aanwezigheid van menselijke intelligentie, die nog niet geëvenaard kan worden door AI. Naarmate de oplossingen van AI verregaander zijn en deze middels het zelflerende vermogen de menselijke kennis te boven gaan, vormen de genoemde risico's een reële dreiging. Daarnaast lopen de meningen ten aanzien van deze risico's ontzettend uiteen, waardoor de identificatie en beheersing daarvan bemoeilijkt wordt.

Desalniettemin gaat het gebruik van AI niet louter met risico's gepaard, maar biedt het ook grote kansen en mogelijkheden. Zo is het bevorderlijk voor de innovatie en daarmee de concurrentiepositie van ondernemingen. Daarnaast brengt het doorgaans grote kostenbesparingen met zich mee, doordat het (specifieke) taken van mensen over kan nemen en bijdraagt aan de efficiënte inrichting van bedrijfsprocessen en – activiteiten. Kostenbesparingen en betere efficiëntie kunnen immers ten gunste komen aan het bedrijfsresultaat. Echter, AI brengt niet louter kansen ten aanzien van het vorenstaande met zich mee. Het kan namelijk bijdragen aan de beheersing van risico's die met andere bedrijfsactiviteiten gepaard gaan, doordat AI meer 'ziet' dan de mens.

4. ADEQUATE CORPORATE GOVERNANCE

4.1 Inleiding

Corporate Governance is een veelomvattend begrip, waarvan in het algemeen wordt uitgegaan dat het gaat over het functioneren van de organen van de vennootschap, meer precies betreffende de onderlinge verhouding, de taken en bevoegdheden en de manier waarop zij hier invulling aan geven.⁷³ Daarnaast vloeit uit deze regels en principes voort op welke wijze over zeggenschapsverhoudingen verantwoording wordt afgelegd.⁷⁴ De termen die daar tevens vaak mee in verband worden gebracht zijn onafhankelijkheid, deskundigheid en integer handelen.⁷⁵

In Nederland zijn de regels voor Corporate Governance opgenomen in de NCGC, waarvan de herziene versie eind 2016 in werking is getreden. Verder valt onder Corporate Governance eveneens 'compliance' met wet- en regelgeving. Omdat risicomanagement een onderdeel van adequate Corporate Governance is en dit derhalve van belang is bij de beantwoording van de centrale vraag, zal in dit hoofdstuk worden ingegaan op de vraag op welke wijze invulling gegeven kan worden aan het begrip adequate Corporate Governance in het licht van risicomanagement inzake AI. Daartoe wordt allereerst ingegaan op de taak van het bestuur zoals deze is vastgelegd in boek 2 BW. Voorts wordt ingegaan op de uitvoering van deze taak ten aanzien van risicomanagement. Hiertoe wordt de NCGC besproken, waarbij dieper wordt ingegaan op de principes betreffende risicomanagement. Tenslotte zal relevante wet- en regelgeving in het licht van compliance worden besproken.

4.2 De taak van het bestuur

Zoals de naam bestuur reeds doet vermoeden, is het bestuur blijkens art. 2:129 lid 1 BW en art. 2:239 lid 1 BW belast met het besturen van de vennootschap. Dit wordt gezien als een bestuursplicht, welke met zich meebrengt dat het bestuur de leiding heeft over de gang van zaken binnen de vennootschap.⁷⁶ In dit kader wordt het bestuur als geheel gezien, maar bij de vraag welke taak specifiek aan welke bestuurder toebehoort wordt door art. 2:9 lid 1 BW gesteld dat alle taken die niet aan andere bestuurders zijn toebedeeld, binnen het takenpakket van die betreffende bestuurder vallen. Op deze manier zal geen enkele bestuurstaak tussen wal en schip kunnen vallen.⁷⁷

In de literatuur wordt over het algemeen aangenomen dat de eerder genoemde bestuursplicht met zich meebrengt dat het bestuur verantwoordelijk is voor de dagelijkse gang van zaken, de

⁷³ Honée, *OR* 2016/67, afl. 9, par. 2.

⁷⁴ Schilfgaarde, van 2013, nr. 10.

⁷⁵ Honée, *OR* 2016/67, afl. 9, par. 2.

⁷⁶ Asser/Maeijer/Van Solinge & Nieuwe Weme 2-II* 2009/390.

⁷⁷ Roest, in: *T&C Burgerlijk Wetboek*, art. 2:9 BW; *Kamerstukken II* 2008/09, 31763, 3, p.7, (MvT).

doelstellingen, de strategie, het financieel beleid en het risicomanagement van de vennootschap.⁷⁸ Risicomanagement kan in dat licht gezien tot de kerntaak van het bestuur worden gerekend.⁷⁹ Dat blijkt eveneens uit art. 2:141 lid 2 BW en art. 2:251 lid 2 BW, waarin is opgenomen dat het bestuur verantwoording aflegt over onder andere het beheers- en controlesysteem van de vennootschap. Als laatste blijkt uit art. 2:391 lid 1 BW dat het bestuur in het bestuursverslag een beschrijving moet geven van de voornaamste risico's en onzekerheden waarmee de vennootschap wordt geconfronteerd. Gezien het feit dat deze belangrijke taken door natuurlijke personen worden uitgevoerd, moeten de bestuurders op hun handelen kunnen worden aangesproken.⁸⁰ De bestuurstaak moet derhalve op grond van art. 2:9 lid 1 BW behoorlijk worden uitgevoerd.

De invulling van het criterium behoorlijk bestuur, is meer omvattend dan de verplichtingen die voortvloeien uit de wet. Het besturen en de bestuurstaak impliceren namelijk ook een niet nader door de wet omschreven algemene verplichting.⁸¹ Het bestuur heeft bij de invulling en uitvoering van deze algemene verplichting tot op zekere hoogte bestuursautonomie, welke een vrijheid in het vervullen van de taken met zich meebrengt. Dit is een voorwaarde om de rechtspersoon te kunnen leiden.⁸² Echter brengt dit niet met zich mee dat het bestuur daarin geheel vrij is, zo dient er in ieder geval sprake te zijn van verantwoord ondernemerschap.⁸³ Daartoe wordt bijvoorbeeld door de NCGC specifieke invulling gegeven aan deze taak. Daarnaast kunnen meer specifieke wet- en regelgeving verplichtingen scheppen voor bestuurders.

4.3 NCGC

4.3.1 Naleving, toepasselijkheid en reflexwerking

Uit de preambule van de NCGC blijkt dat de huidige Code, in tegenstelling tot eerdere Corporate Governance Codes, gericht is op de lange termijn waardecreatie van (beursgenoteerde) vennootschappen.⁸⁴ Korte termijn waardecreatie leidt namelijk in veel gevallen tot het nemen van uitzinnige risico's door bestuurders. De duurzame waardecreatie in de NCGC wordt derhalve onder andere in verband gebracht met risicobeheersing, de opzet van een risicobeheersingssysteem en de verantwoording daaromtrent.⁸⁵ De NCGC heeft de verantwoordelijkheid voor het risicomanagement binnen de onderneming bij de bestuurders neergelegd, wat met zich meebrengt dat de principes neergelegd in de NCGC van invloed zijn op bestuurdersaansprakelijkheid inzake falend

⁷⁸ Stolp & Nijs Bik, de 2015, p. 43.

⁷⁹ Strik 2010, p. 275.

⁸⁰ Strikwerda, MAB 2002/76(1/2), p. 54-64.

⁸¹ Westenbroek 2017, p. 73.

⁸² Asser/Maeijer & Kroeze 2-I* 2015/189.

⁸³ Zie: Schilfgaarde, van e.a. 2017, nr. 42.; Assink & Slagter 2013, p. 902 ev. en p. 1596 ev.

⁸⁴ *Herziene NCGC* 2016, preambule.

⁸⁵ Kleipool & Olffen, van, *OR* 2017/56, afl. 7, par. 2.

risicomanagement.⁸⁶

De plicht tot naleving van deze principes is wettelijk verankerd in art. 2:391 lid 5 BW, middels een pas-toe-of-leg-uit principe. Hierin is de verplichting opgenomen om intern en extern gemotiveerd verantwoording af te leggen over de wijze waarop de onderneming de principes en best practice bepalingen al dan niet toepassen, ook wanneer deze wél worden toegepast. Dientengevolge kan het meer gekwalificeerd worden als zijnde een pas-toe-én-leg-uit principe.⁸⁷ De vrijblijvendheid die met dit principe gepaard lijkt te gaan, is in de praktijk toch beperkt, gezien het feit dat vele bepalingen in de NCGC voortvloeien uit algemene vennootschappelijke normen waar vennootschappen in veel gevallen redelijkerwijs niet van af kunnen wijken.⁸⁸

Niet alleen middels de wettelijke verankering, maar ook in de rechtspraak wordt regelmatig verregaande juridische betekenis toegekend aan de bepalingen uit de NCGC. Zo is in de rechtspraak bepaald dat de NCGC invulling kan geven aan relatief open normen, zoals de redelijkheid en billijkheid van art. 2:8 BW en de onbehoorlijke taakvervulling van art. 2:9 BW.⁸⁹ De invulling van deze juridische open normen kan derhalve geschieden aan de hand van de principes en best practice bepalingen uit de NCGC. In algemene zin kan worden aangenomen dat de principes eerder invulling kunnen geven aan deze normen, dan de best practice bepalingen.⁹⁰ De mate waarin een bepaald onderdeel van de NCGC wordt nageleefd is hierbij bepalend.⁹¹

Het is echter niet vanzelfsprekend dat alle kapitaalvennootschappen onder de werking van de NCGC vallen, daar deze blijkens de preambule louter gericht is op Nederlandse beursgenoteerde kapitaalvennootschappen.⁹² De principes en best practice bepalingen kunnen echter wel relevant zijn voor niet beursvennootschappen.⁹³ Zo wordt de NCGC als een vorm van goede Corporate Governance gezien, die het verdient om ook door niet beursgenoteerde vennootschappen gevolgd te worden.⁹⁴ Tevens wordt in de literatuur algemeen aangenomen dat de NCGC een bepaalde reflexwerking kan hebben.⁹⁵ Dit betekent echter niet dat de NCGC in zijn geheel werking vindt ten aanzien van alle niet-beursvennootschappen.⁹⁶ Volgens Josephus Jitta moet namelijk ten aanzien van de reflexwerking onderscheid worden gemaakt tussen het geval dat de NCGC nieuwe beginselen dan wel regels toevoegt aan het bestaande rechtssysteem en het geval waarin het reeds geldende recht wordt weergegeven. Met name het laatste geval zou zich kunnen lenen voor de reflexwerking ten aanzien van niet

⁸⁶ *Herziene NCGC* 2016, principe 1.2.

⁸⁷ Koster, *OR* 2018/5, afl. 1.

⁸⁸ Raaijmakers 2016, p. 301.

⁸⁹ HR 13 juli 2007, ECLI:NL:HR:2007:BA7970 (*ABN AMRO*); HR 9 juli 2010, ECLI:NL:HR:2010:BM0976 (*ASMI*).

⁹⁰ Rietveld & Cremers, *OR* 2017/97, afl. 12, par. 3.2.

⁹¹ Honee, *OR* 2016/67, afl. 9, par. 3.2; Asser/Van Solinge & Nieuwe Weme 2-IIa 2013/39.

⁹² *Herziene NCGC* 2016, preambule.

⁹³ Vaessen, *MvV* 2017, afl. 12, par. 2.4.

⁹⁴ Kluiver, de, *NJB* 2017/839, afl. 15, par. 1.

⁹⁵ Asser/Van Solinge & Nieuwe Weme 2-IIa 2013/46; Huizink, in: *GS Rechtspersonen*, art. 2:64 BW, aant. 4.7.

⁹⁶ Josephus Jitta, *OR* 2007/135, afl. 12; Schilfgaarde, van 2013, p.381; Raaijmakers 2016, p. 309.

beursgenoteerde vennootschappen.⁹⁷ In het geval van risicomanagement inzake AI is dat echter tot op heden (nog) niet aan de orde, daar wettelijke regels betreffende inhoudelijk risicomanagement ontbreken. Voor ieder beginsel afzonderlijk zal daarom de afweging gemaakt moeten worden of het betreffende beginsel zich voor toepassing bij een niet onder de officiële werking van de NCGC vallende vennootschap leent. Deze afweging wordt ook wel gezien als een invulling van relatief open normen zoals de vennootschapsrechtelijke redelijkheid en billijkheid. Daarnaast leent de relatief open norm van de behoorlijke taakvervulling van art. 2:9 BW zich – afhankelijk van de omstandigheden van het geval – volgens de Kraker voor invulling door middel van de concrete gedragsnormen uit de NCGC.⁹⁸ De omstandigheden van het geval zien vaak toe op de vraag of toepassing van die gedragsnormen redelijkerwijs kan worden verwacht, gekeken naar de vennootschap. Zo zal in het geval van het midden- en kleinbedrijf de toepassing van de NCGC minder voor de hand liggen. Echter kan volgens Strik als uitgangspunt gelden dat ook voor die vennootschappen enige vorm van risicobeheersing – hetgeen voorschreven wordt in de NCGC – vereist is.⁹⁹ Aan welke vereisten in dat geval een risicobeheersings- en controlesysteem moet voldoen, hangt af van de aard, omvang, complexiteit en levensfase van de onderneming, de gebruiken binnen de branche en de aard van gelopen risico's.¹⁰⁰ Kleine ondernemingen hebben namelijk niet alle voorgeschreven controlesystemen nodig, bijvoorbeeld omdat het bestuur van deze ondernemingen vaak informatie uit eerste hand krijgt, waardoor ingewikkelde rapportagestructuren overbodig zijn. Van belang is wel dat door het bestuur een afweging wordt gemaakt op basis van de eerder genoemde omstandigheden. Voor niet beursgenoteerde vennootschappen met een grote tot zeer grote omvang, zal verregaande toepassing van de NCGC meer voor de hand liggen.¹⁰¹ Dit zal voornamelijk het geval zijn bij ondernemingen die grote investeringen doen in het gebruik en de ontwikkeling van AI.

In het geval van de reflexwerking moet wel in ogenschouw worden genomen dat afwijking van gedragsnormen niet per definitie leidt tot slechte Governance, wanbeleid of onbehoorlijke taakvervulling.¹⁰² Wél kan de niet-naleving van dergelijke gedragsnormen een extra argument vormen in het geval van onbehoorlijk bestuur of wanbeleid.¹⁰³ De vaststelling van een schending van de NCGC kan derhalve bijdragen aan het oordeel omtrent bestuurdersaansprakelijkheid, maar is op zichzelf bijna nooit dragend voor dat oordeel.¹⁰⁴ Er zijn dan ook slechts enkele gevallen bekend waarin

⁹⁷ Jospehus Jitta, *OR* 2007/135, afl. 12.

⁹⁸ Kraker, de, *Bb* 2017/44, afl. 11, par. 2.

⁹⁹ Strik 2010, p. 283.

¹⁰⁰ Strik 2010, p. 284.

¹⁰¹ Zie bijvoorbeeld de bedrijven die gebruik maken van AI in: *Artificial Intelligence in Europe* 2018.

¹⁰² Schilfgaarde, van 2013, p.381.

¹⁰³ Zie: Hof Amsterdam (OK) 16 november 2005, ECLI:NL:GHAMS:2005:AV0121 en Hof Amsterdam (OK) 9 oktober 2006, ECLI:NL:GHAMS:2006:AZ6791 (*UMI*); Hof Amsterdam (OK) 6 juli 2006, ECLI:NL:GHAMS:2006:AY0520 (*TCA*) ; HR 29 juni 2006, ECLI:NL:HR:2007:BA033; Hof Amsterdam (OK) 2 november 2015, ECLI:GHAMS:2015:4454 (*Maevita*).

¹⁰⁴ Soerjatin 2012, p. 133.

bestuurdersaansprakelijkheid op grond van het schenden van de NCGC werd aangenomen.¹⁰⁵ Op de gedragsnormen betreffende risicomanagement zal in paragraaf 4.3.2 verder worden ingegaan.

4.3.2 Risicobeheersing in de NCGC

De NCGC is gericht op lange termijn waardecreatie, wat blijkt uit het voorstel voor herziening met zich meebrengt dat een adequaat systeem voor de beheersing van risico's, waarbij risico's worden geïdentificeerd en beheerst, onmisbaar is.¹⁰⁶ Voor een adequaat systeem dienen 3 fasen te worden onderscheiden, te weten: de beoordeling van risico's, de implementatie van een beheersings- of controlesysteem en de monitoring daarvan. Hiertoe zijn in de NCGC principes en best practice bepalingen opgenomen, die betrekking hebben op de rol van het bestuur (principe 1.2), de interne auditor (principe 1.3), de verantwoording omtrent de wijze waarop de vennootschap inrichting heeft gegeven aan het beheersings- of controlesysteem (principe 1.4) en de auditcommissie (principe 1.5). Hoewel de interne auditor, de auditcommissie en de RvC een belangrijke rol innemen in het risicomanagementproces, worden deze voor dit onderzoek buiten beschouwing gelaten, omdat de vraag of bestuurders aansprakelijk kunnen worden gehouden voor falend risicomanagement inzake AI specifiek gericht is op de bestuurstaak. Hierdoor spelen met name de principes betreffende risicobeheersing een rol. Er zal dan voor het verdere onderzoek ook vanuit worden gegaan dat volgens de principes 1.3 en 1.5 wordt gehandeld.

4.3.2.1 Risicomanagement door het bestuur

Principe 1.2 schrijft voor dat de vennootschap dient te beschikken over adequate interne risicobeheersings- en controlesystemen, waarbij het bestuur verantwoordelijk is voor het identificeren en beheersen van de risico's verbonden aan de strategie en de activiteiten van de vennootschap.¹⁰⁷ Derhalve bepaalt het bestuur welke risico's het bereid is te nemen om de doelstellingen die in de strategie van de vennootschap zijn opgenomen te bewerkstelligen. Hiertoe dienen de risico's te worden geïnventariseerd en geanalyseerd, waarna de risicobereid dient te worden vastgesteld.¹⁰⁸ De mate waarin een vennootschap bereid is risico te nemen wordt ook wel de *risk appetite* genoemd en wordt vastgesteld op basis van verschillende overwegingen. Hier zal in paragraaf 6.2.2.2 nader op in worden gegaan. Op basis van deze *risk appetite* dient het bestuur adequate interne risicobeheersings- en controlesystemen te ontwerpen, implementeren en onderhouden.¹⁰⁹ Van belang hierbij is dat deze op die wijze in de werkprocessen van de onderneming worden geïmplementeerd, dat eenieder die werkzaamheden verricht ten aanzien waarvan deze systemen gelden, daarvan op de hoogte is. Als laatste dient het bestuur de werking van de systemen te monitoren middels jaarlijkse systematische

¹⁰⁵ Vaessen, MvV 2017, afl. 12, par. 4.

¹⁰⁶ MCCGC 2016, p.11.

¹⁰⁷ *Herziene NCGC* 2016, preambule.

¹⁰⁸ *Herziene NCGC*, best practice bepaling 1.2.1.

¹⁰⁹ *Herziene NCGC* 2016, best practice bepaling 1.2.2.

beoordeling van de opzet en de werking daarvan. Indien noodzakelijk worden verbeteringen doorgevoerd.¹¹⁰

De strategie die noopt tot het bewerkstelligen van de doelstellingen, dient blijkens principe 1.1 in ieder geval gericht te zijn op lange termijn waardecreatie. In dit licht kan worden gesteld dat de implementatie van AI in een onderneming zonder twijfel gericht is op lange termijn waardecreatie. Het is namelijk zeer waarschijnlijk dat het gebruik van AI met kostenbesparing gepaard gaat, hetgeen ten goede kan komen aan de bedrijfsdoelstellingen. Daarnaast kan AI worden gebruikt om te blijven innoveren en zo de concurrentiepositie van de onderneming te versterken. Het wordt daarom ook wel gezien als 'de toekomst'. Als laatste en meest belangrijke punt, 'ziet' AI meer dan de mens, waardoor risico's die gepaard gaan met andere bedrijfsactiviteiten kunnen worden ingeperkt. Hiermee wordt lange termijn waardecreatie in de hand gewerkt.

Gekeken naar de situaties waarin AI reeds geïmplementeerd is in ondernemingen, blijkt dat de AI systemen vooralsnog voornamelijk ter ondersteuning van werkzaamheden dienen, waarbij uitsluitend een specifieke taak aan het systeem wordt toegekend. De daaraan verbonden risico's zijn reeds (grotendeels) in kaart gebracht, wat er mijns inziens toe zou moeten kunnen leiden dat deze door het bestuur adequaat geïdentificeerd worden. In het geval van verregaande AI toepassingen, welke tot op heden nauwelijks daadwerkelijk zijn geïmplementeerd, kan deze identificatie bemoeilijkt worden doordat de risico's daarvan lastig in kaart te brengen zijn. De mogelijke risico's daaromtrent lopen uiteen van de risico's genoemd in paragraaf 3.2, tot een overname van de algehele mensheid. De risicobereidheid die daar vervolgens aan wordt gekoppeld zou in lijn moeten liggen met de financiële gezondheid en doelstellingen van de vennootschap.

Het ontwerp, de implementatie en controle van risicobeheersings- en controlesystemen die dientengevolge plaats moeten vinden vormen een uitdaging, omdat vele van deze risico's nog aan onderzoek onderhevig zijn. Zo wordt onderzoek gedaan naar *explainable AI*, waarbij wordt gekeken naar de wijze waarop een AI systeem tot een beslissing komt, om op die manier het interpretatierisico in te perken. Daarentegen kan bijvoorbeeld wel het gebruik van AI in de onderneming ingekaderd worden binnen vooraf vastgestelde randvoorwaarden, zodat het risico op oneigenlijk gebruik kan worden tegengegaan.¹¹¹ Verdere mogelijke beheersingsmaatregelen zijn onderzocht door Deloitte en zullen in hoofdstuk 6 aan bod komen.¹¹² Desalniettemin kunnen dergelijke risico's ook op andere wijzen worden ingeperkt, bijvoorbeeld door de mate waarin AI toepassing vindt binnen de onderneming. Van belang bij de implementatie van een dergelijk beheersingssysteem is dat de werknemers die tijdens hun werkzaamheden betrokken zij bij enige toepassing van AI, op de hoogte zijn van de risico's en het

¹¹⁰ *Herziene NCGC 2016*, best practice bepaling 1.2.3.

¹¹¹ Steels e.a. 2018, p. 35-36.

¹¹² *Future of risk in the digital era* 2019, p. 7.

beheersingssysteem. AI schuilt in kleine toepassingen, waardoor de werknemers – zeker gezien de ingewikkelde technische achtergrond van AI – mogelijkwerijs niet beseffen met welke risico's het gebruik gepaard gaat.

De jaarlijkse systematische beoordeling is gezien de voortdurende ontwikkeling van AI, alsmede het vermogen van AI om zelflerend te zijn en derhalve zelfstandig tot oplossingen te komen, geen overbodige luxe. Mijns inziens vormt deze best practice bepaling dan ook een belangrijke schakel in het takenpakket van het bestuur.

4.3.2.2 Verantwoording over risicobeheersing

Principe 1.4 van de NCGC betreft de verantwoording over risicobeheersing, waarin is opgenomen dat het bestuur verantwoording dient af te leggen over de uitvoering zoals beschreven in paragraaf 4.3.2.1, waarbij de uitvoering, de opzet, de werking, eventuele tekortkomingen en de gevoeligheid van de resultaten van de vennootschap worden besproken.¹¹³ Hiertoe verklaart het bestuur in het bestuursverslag onder andere dat de risicobeheersings- en controlesystemen naar behoren hebben gewerkt en dat de verwachting is dat de continuïteit van de vennootschap het komende jaar gewaarborgd blijft.¹¹⁴

4.4 Wet- en regelgeving

Niet alleen de NCGC, maar ook wet- en regelgeving die specifiek van toepassing is op het gebruik van AI in vennootschappen is van belang voor de wijze waarop het bestuur dient om te gaan met het gebruik daarvan. Een kanttekening die hierbij gemaakt moet worden is dat wet- en regelgeving vaak achter loopt, wat in deze eveneens het geval blijkt te zijn. Desalniettemin kan het grotendeels ontbreken van deze specifieke wet- en regelgeving niet als vrijbrief voor ongelimiteerd gebruik van AI gezien worden, omdat de NCGC daar – indirect – eisen aan stelt middels de eerder genoemde principes en best practice bepalingen.

4.4.1 Privacy- en gegevensbescherming

Zoals eerder beschreven ontbreekt het grotendeels aan specifieke wet- en regelgeving omtrent het gebruik van AI. De Europese Unie is vandaag de dag wel bezig met de juridische inkadering daarvan, om op die manier te zorgen voor de inperking van risico's die met het gebruik gepaard gaan. Hetgeen wél reeds wettelijk is vastgelegd, is de beperking en regulering van datagebruik alsmede het recht op uitleg van geautomatiseerde besluitvorming.¹¹⁵ Hiertoe is de GDPR in werking getreden, waaraan in Nederland wordt gerefereerd als de AVG. Deze wet strekt tot bescherming van persoonsgegevens, waarbij onder persoonsgegevens op grond van art. 4 lid 1 AVG onder andere maar niet uitsluitend wordt verstaan: informatie over een natuurlijke persoon welke een (deel van) de fysieke, fysiologische,

¹¹³ *Herziene NCGC 2016*, best practice bepaling 1.4.1.

¹¹⁴ *Herziene NCGC 2016*, best practice bepaling 1.4.2.

¹¹⁵ Steels e.a. 2018, p. 34-35.

genetische, psychische, economische, culturele of sociale identiteit van een persoon bevat. Het is op grond van art. 6 AVG niet meer mogelijk om dergelijke gegevens te verwerken zonder dat daar een rechtmatige grond voor bestaat, zoals toestemming van de betrokkene of ter voldoening van een wettelijke plicht. Verder moet de verwerking blijkens art. 5 lid 1 AVG behoorlijk en transparant zijn. Tevens heeft een betrokkene conform art. 22 AVG het recht op uitleg en heeft deze het recht om niet onderworpen te worden aan geautomatiseerde besluitvorming.

Zoals eerder omschreven in hoofdstuk 2, is voor het gebruik van AI een grote hoeveelheid data nodig, waarmee het systeem gevoed kan worden. Op basis daarvan, in combinatie met een lerend algoritme, komt het AI systeem tot een oplossing. Data is dus van ongekend belang voor de toepassing van AI in een onderneming. De beperkingen die door de AVG worden gesteld zijn daarom van grote invloed op de wijze waarop AI in de onderneming gebruikt kan worden. De data moet immers rechtmatig gebruikt worden, de verwerking moet behoorlijk en transparant zijn en er moet uitleg gegeven kunnen worden omtrent de beslissingen. Blijkens paragraaf 3.3 vormen transparantie en interpreteerbaarheid echter gedegen risico's. Bestuurders van kapitaalvennootschappen zullen derhalve zorg moeten dragen voor adequate beheersing van deze risico's. Een overtreding van de AVG kan namelijk door de Autoriteit Persoonsgegevens worden bestraft met een boete die kan oplopen tot € 20.000.000,- of tot 4 procent van de totale wereldwijde jaaromzet van een vennootschap, indien dit hoger is dan het voornoemde bedrag.¹¹⁶ Daarnaast kan schending van de AVG, blijkens zeer recente jurisprudentie, leiden tot een schadevergoeding aan de betrokkene.¹¹⁷ Voor deze schadeposten zouden bestuurders – potentieel – aansprakelijk kunnen worden gehouden.

4.4.2 Ethische richtlijnen

De EC heeft zeer recentelijk richtsnoeren voor betrouwbare AI gepresenteerd, die momenteel middels een pilot getest worden, waarna de herziene versie in januari 2020 van kracht zal worden.¹¹⁸ Deze richtsnoeren zijn nog niet officieel van kracht en betreffen geen daadwerkelijke wet- en regelgeving. Echter kan hierbij wel worden aangesloten om een beeld te krijgen van hetgeen van een bestuurder verwacht zou mogen worden. Blijkens de richtsnoeren bestaat betrouwbare AI uit drie componenten. Zo moet het systeem wettig zijn, wat inhoudt dat het moet voldoen aan alle toepasselijke wet- en regelgeving. Daarnaast moet het systeem ethisch zijn, wat met zich meebrengt dat het zorg dient te dragen voor naleving van ethische beginselen en waarden. Als laatste moet het systeem robuust zijn, uit zowel technisch- als sociaal oogpunt, omdat systemen ongewild schade aan kunnen richten.¹¹⁹ Deze componenten zijn allen nodig, maar kunnen afzonderlijk van elkaar niet leiden tot voldoende

¹¹⁶ Art. 58 lid 1 onder i AVG jo. art. 83 lid 6 AVG.

¹¹⁷ Rb. Overijssel 28 mei 2019, ECLI:NL:RBOVE:2019:1827.

¹¹⁸ *Ethische richtsnoeren voor betrouwbare KI* 2019, voorwoord.

¹¹⁹ *Ethische richtsnoeren voor betrouwbare KI* 2019, p. 6.

betrouwbare AI. Concrete vereisten die hieruit voortvloeien zijn: menselijke controle, technische veiligheid, privacy- en data governance, transparantie, diversiteit, non-discriminatie en rechtvaardigheid, maatschappelijk en milieuwelzijn en verantwoording.¹²⁰ Deze vereisten sluiten aan bij de grootste risico's van AI, welke in paragraaf 3.3 uiteengezet zijn. De richtsnoeren vormen derhalve een uitstekende basis voor het risicobeheersings- en controlesysteem dat door het bestuur blijkens paragraaf 4.2 dient te worden opgezet. In hoofdstuk 6 zal daarom dieper worden ingegaan op deze richtsnoeren.

4.5 Conclusie

Op welke wijze kan invulling worden gegeven aan het begrip adequate Corporate Governance in het licht van risicomanagement betreffende AI?

Corporate Governance is een veelomvattend begrip, welke in ieder geval over het functioneren van de vennootschappelijke organen, waaronder het bestuur, ten aanzien van haar taken en bevoegdheden gaat. Ter toetsing van dit functioneren kan in het algemeen gekeken worden naar wet- en regelgeving betreffende de bestuurstaak en de regels van Corporate Governance, welke in de NCGC zijn opgenomen. Daarnaast betreft compliance met wet- en regelgeving eveneens een relevant element, daar bestuurders in beginsel gehouden zijn aan het opvolgen daarvan.

Het bestuur heeft op grond van art. 2:129 lid 1 BW en art. 2:239 lid 1 BW een bestuursplicht, waarbij het risicomanagement een van de kerntaken van het bestuur vormt, welke op grond van art. 2:9 behoorlijk dient worden uitgevoerd. Voor de invulling van het begrip 'behoorlijk' kan onder andere worden aangesloten bij de principes en best practice bepalingen van de NCGC. Deze is van toepassing op beursgenoteerde vennootschappen, maar kan middels een zogeheten reflexwerking eveneens van toepassing zijn op niet beursgenoteerde vennootschappen. Afhankelijk van de aard, omvang, complexiteit en levensfase van de onderneming alsmede de gebruiken binnen branche en de aard van de gelopen risico's, kan eveneens van kleinere ondernemingen worden verwacht dat deze enige vorm van risicobeheersing (al dan niet op grond van de principes van de NCGC) toepassen.

De vennootschap dient op grond van art. 2:391 lid 5 BW middels het pas-toe-of-leg-uit-principe verantwoording af te leggen over de wijze waarop de NCGC al dan niet wordt toegepast. Vorenstaande geldt echter louter voor vennootschappen ten aanzien waarvan volledige (reflex)werking geldt. Schending van de principes leidt niet per definitie tot slechte governance of onbehoorlijk bestuur, maar kan wel invulling geven aan deze begrippen.

Het bestuur dient op grond van de NCGC zorg te dragen voor adequate interne risicobeheersings- en controlesystemen, waarbij eerst de risicobereidheid van de vennootschap wordt

¹²⁰ *Ethische richtsnoeren voor betrouwbare KI* 2019, p. 16-17.

vastgesteld, alvorens het systeem te ontwerpen, implementeren, controleren en systematisch jaarlijks te monitoren. Daarnaast legt het bestuur in haar bestuursverslag verantwoording af omtrent de uitvoering, opzet, werking en eventuele tekortkomingen van het systeem.

Met name het ontwerpen en implementeren van een dergelijk beheersingssysteem kan in het geval van AI tot moeilijkheden leiden, omdat risico's moeilijk in te schatten kunnen zijn en er nog veel onderzoek plaats moet vinden naar de wijze waarop deze risico's ingeperkt kunnen worden. Wel kan de mate waarin AI in een onderneming is verweven hier een rol in spelen, omdat bijvoorbeeld verregaande AI toepassingen grotere risico's met zich meebrengen dan toepassingen die slechts ter ondersteuning worden gebruikt.

Tevens van groot belang voor adequate Corporate Governance is compliance met geldende wet- en regelgeving. In het geval van AI ontbreekt het daar grotendeels aan. Uiteraard zijn de grondrechten van belang, maar AI specifiek is er louter sprake van regelgeving met betrekking tot datagebruik en het recht op uitleg in de AVG. In het geval van AI toepassingen is overtreding, anders gezegd non-compliance zonder meer mogelijk, gezien het feit dat grote risico's zoals de transparantie en interpreteerbaarheid hierin vervat zijn. Bovenstaande geeft echter wel een kader waarbinnen het bestuur in het licht van adequate Corporate Governance in ieder geval moet opereren.

Als laatste zijn de ethische richtlijnen voor betrouwbare AI van belang voor bestuurders in het licht van adequate Corporate Governance, omdat hierbij aan kan worden gesloten bij de vraag op welke wijze bestuurders met de risico's om zouden moeten gaan. Deze richtlijn sluit namelijk naadloos aan op de risico's van AI.

Al met al kan gesteld worden dat het bestuur in het licht van adequate Corporate Governance zorg moet dragen voor een risicobeheersings- en controlesysteem dat aansluit bij de eisen in de NCGC, waarbij in ieder geval de risico's die betrekking hebben op grondrechten en de AVG dienen te worden beheerst. Daarnaast dienen de andere risico's te worden geïdentificeerd, geanalyseerd en eventueel beheerst, voor zover dat op dat moment mogelijk is. Hierbij kan wel worden aangesloten bij de ethische richtsnoeren van de EC.

5. AANSPRAKELIJKHEID VOOR FALEND RISICOMANAGEMENT

5.1 Inleiding

In hoofdstuk 4 is reeds beschreven welke taken bij het bestuur horen en waartoe het bestuur een bestuursplicht heeft. Risicomanagement is een van de kerntaken die valt onder de bestuursplicht, hetgeen met zich meebrengt dat deze taak behoorlijk vervuld dient te worden. Middels de NCGC en relevante wet- en regelgeving is daarom een begin gemaakt met de invulling van het begrip behoorlijk bestuur, in het licht van risicomanagement inzake AI.

In het geval dat het bestuur deze taak onbehoorlijk uitvoert, kan zij onder andere aansprakelijk worden gesteld op grond van art. 2:9 BW en art. 6:162 BW. Art. 2:9 BW ziet toe op de interne aansprakelijkheid, van de bestuurders jegens de vennootschap en art. 6:162 BW ziet toe op de externe aansprakelijkheid, van de bestuurders jegens derden.¹²¹

De vraag of bestuurders ook aansprakelijk kunnen zijn voor falend risicomanagement, is reeds door Strik positief beantwoord.¹²² De vraag is echter of dat ook het geval kan zijn wanneer het gebruik van AI vele kansen met zich meebrengt, maar waarbij de risico's bijvoorbeeld moeilijk voorspelbaar en/of beheersbaar zijn. Ondernemen betekent immers een bepaalde vorm van risico's nemen. Blijkens de kamerstukken betreffende art. 2:9 BW *'kan niet van bestuurders worden verwacht dat ze uitsluitend handelen in die situaties waarin de te nemen stap al op alle mogelijke manieren is onderzocht, doorgerekend, van accountantsverklaringen voorzien en in schema's gevat.'*¹²³ De grens ligt hierbij bij het nemen van onverantwoorde risico's.

In dit hoofdstuk zal worden ingegaan op de wijze waarop bestuurders van kapitaalvennootschappen aansprakelijk gesteld kunnen worden alsmede op welke wijze invulling gegeven wordt aan de (on)behoorlijke taakvervulling en ernstig verwijt. Op basis daarvan wordt getoetst in hoeverre het mogelijk is om bestuurders van kapitaalvennootschappen aansprakelijk te stellen voor falend risicomanagement inzake AI.

5.2 Interne bestuurdersaansprakelijkheid ex art. 2:9 BW

De vennootschap kan op grond van art. 2:9 lid 2 BW het bestuur intern jegens de vennootschap aansprakelijk stellen, indien het bestuur zijn taak onbehoorlijk heeft vervuld en hem daartoe een ernstig verwijt kan worden gemaakt. Een vordering ex art. 2:9 BW moet worden ingesteld door de vennootschap, bijvoorbeeld door de RvC, een opvolgend bestuur of de curator in faillissement.¹²⁴ Een

¹²¹ Kroeze, Timmerman & Wezeman 2007, p. 154-161.

¹²² Strik 2010.

¹²³ *Kamerstukken II* 2008/09, 31763, 3, p.9, (MvT).

¹²⁴ Assink e.a. 2011, p. 25.

aandeelhouder kan dus, ondanks het feit dat het bestuur haar taken in feitelijk jégens de aandeelhouders uitvoert, géén schade vorderen op grond van art. 2:9 BW.¹²⁵ Deze maatstaf geldt in beginsel voor het bestuur als geheel, maar art. 2:9 lid 2 BW biedt eveneens de mogelijkheid tot disculpatie van de individuele bestuurder. Het is daarvoor echter niet noodzakelijk om voor iedere bestuurder afzonderlijk te stellen en te bewijzen dat er sprake is van een ernstig verwijt.¹²⁶

Gekeken naar de criteria voor aansprakelijkheid – onbehoorlijke taakvervulling en ernstig verwijt – kan er gesproken worden van een gedragsnorm voor de wijze waarop een bestuurder zijn taak moet vervullen, alsmede een toetsingsnorm.¹²⁷ Uit de jurisprudentie van de Hoge Raad blijkt echter niet eenduidig hoe deze normen zich tot elkaar verhouden.¹²⁸ Volgens Assink e.a. bestaat er géén inhoudelijk verschil tussen situaties of gevallen die een ernstig verwijt opleveren en situaties of gevallen die tot onbehoorlijke taakvervulling leiden, waardoor de normschending reeds verpakt is in het criterium ernstig verwijt.¹²⁹ Volgens Strik kan uit de oneindige mogelijkheden wat betreft omstandigheden die van belang kunnen zijn bij de invulling van het criterium ernstig verwijt worden afgeleid dat er sprake zou zijn van een géintegreerde aanpak omdat het zowel de ernst van het gedrag als de verwijtbaarheid daarvan zou indiceren. Dit brengt met zich mee dat het kunnen maken van een ernstig verwijt met zich mee brengt dat er eveneens sprake is van onbehoorlijke taakvervulling.¹³⁰ Ook Borrius stelt dat de feitelijke omstandigheden de ernstig verwijt norm inkleuren, waarbij deze norm fungeert als sjabloon voor de beoordeling of er sprake is van (on)behoorlijk bestuur.¹³¹ Voor het verdere onderzoek zal daarom eveneens de géintegreerde aanpak van de normen behoorlijk bestuur en ernstig verwijt worden gebruikt.

De ernstig verwijt maatstaf vormt een hoge drempel voor bestuurdersaansprakelijkheid en wordt aangenomen om te voorkomen dat bestuurders hun handelen in onwenselijke mate door defensieve overwegingen laten bepalen.¹³² Het oordeel daaromtrent wordt namelijk altijd achteraf geveld. De rechter moet de beslissing van de bestuurder toetsen op het moment dat de risico's zich reeds hebben verwezenlijkt. Er is in dat geval mogelijk sprake van het zogeheten *hindsight bias*, wat inhoudt dat de gevolgen die zijn ingetreden ongewild meegewogen worden in de waarschijnlijkheid van het verwezenlijken daarvan.¹³³

¹²⁵ Kroeze 2004, p. 126.

¹²⁶ Asser/Maeijer/van Solinge & Nieuwe Weme 2-II* 2009/446.

¹²⁷ Asser/Maeijer/van Solinge & Nieuwe Weme 2-II* 2009/448.

¹²⁸ Zie in dat kader bijvoorbeeld de tegenstrijdigheden in: HR 11 juni 1999, ECLI:NL:HR:1999:ZC2925 (*Van Dooren qq/Hendriks*) waarin de twee normen afzonderlijk van elkaar worden gebruikt en HR 29 november 2002, ECLI:NL:HR2002:AE7011 (*Swandt/Berghuizer Papierfabriek*) waarin geneigd wordt naar een integrale benadering waarbij er zonder ernstig verwijt géén onbehoorlijke taakvervulling kan zijn.

¹²⁹ Assink 2007, p. 613-614.

¹³⁰ Strik 2010, p. 18-19.

¹³¹ Borrius 2003, p. 79-103.

¹³² Zie: Westenbroek 2017, p. 4-5 over HR 20 juni 2008, ECLI:NL:HR:2008:BC4959 (*Willemsen/NOM*).

¹³³ Kroeze, *OR* 2006/3, afl. 1, par. 8.2.

5.2.1 (On)behoorlijk bestuur en ernstig verwijt

Zoals eerder uiteengezet, zal bij een geïntegreerde aanpak van deze begrippen, een *ernstig verwijt* eveneens onbehoorlijke taakvervulling opleveren. In het Staleman/van de Ven arrest is door de Hoge Raad invulling gegeven aan het criterium ernstig verwijt. Er moet worden getoetst aan de zogeheten *maatman bestuurder* wat het volgende inhoudt: ‘(...) *het inzicht en de zorgvuldigheid die mogen worden verwacht van een bestuurder die voor zijn taak berekend is en deze nauwgezet vervult*’.¹³⁴ Hierbij wordt door Timmermans de nadruk gelegd op zorgvuldigheid en nauwgezet.¹³⁵ Het gaat er daarbij met name om wat de bestuurder redelijkerwijs had behoren te weten, afgaande op de informatie die tot zijn beschikking stond.¹³⁶ Deze norm werd vervolgens in het Laurus arrest als volgt ingevuld: ‘(...) *de wijze waarop een redelijk bekwame en redelijk handelende functionaris die taak in de gegeven omstandigheden had horen te vervullen*’.¹³⁷ In latere jurisprudentie wordt verder gegaan met het criterium van het Staleman/van de Ven arrest.

De vraag die hierbij ten aanzien van AI rijst is wat als een *maatman bestuurder* gezien kan worden, nu AI van zulks technische aard is dat menig bestuurder daar geen kaas van gegeten zal hebben. Wist of behoorde het bestuur in dat geval te weten welke risico’s met het gebruik van AI gepaard gaan, zelfs wanneer dit als middel wordt ingezet om andere risico’s in te perken? Of kan van een bestuurder worden verwacht dat hij juist gebruik maakt van AI in de onderneming, om zo bijvoorbeeld andere risico’s in te perken, omdat AI meer ‘ziet’ dan de mens?

Mijns inziens is het aannemen van de onwaarschijnlijkheid dat bestuurders op voldoende verregaande wijze verstand hebben van AI – waarbij de risico’s overzien kunnen worden en op basis daarvan geïdentificeerd, geanalyseerd en een passend beheersingssysteem geïmplementeerd wordt – ondanks de bewuste hoge drempel van bestuurdersaansprakelijkheid, onwenselijk. Op die manier zou te pas en te onpas gebruik kunnen worden gemaakt van verregaande AI toepassingen, bijvoorbeeld zonder het toezien oog van de mens, waarbij achteraf gesteld zou kunnen worden dat er niet van het bestuur verwacht had kunnen worden dat zij bekend waren met de risico’s van het gebruik.

Daarentegen, wanneer het bestuur gebruik maakt van AI ter inperking van andere risico’s, illustreert dat de welwillendheid van het bestuur ten aanzien van adequaat risicomanagement. Het is in mijn ogen dan ook niet mogelijk om zwart op wit vast te stellen wat in het geval van het gebruik van AI gezien moet worden als *maatman bestuurder*. Dit komt doordat er een afweging plaats zal moeten vinden tussen verschillende omstandigheden die van invloed kunnen zijn op hetgeen van de bestuurder verwacht kan worden. Er dient daarom rekening te worden gehouden met de omstandigheden van het geval, waarbij in ieder geval gekeken dient te worden naar de aard en ernst van de normschending, de

¹³⁴ HR 10 januari 1997, ECLI:NL:HR:1997:ZC2243 (*Staleman/Van de Ven*).

¹³⁵ Timmerman, *OR* 2019/45, afl. 5.

¹³⁶ Olden, *OR* 2019/83, afl. 8, nr. 6.

¹³⁷ HR 8 april 2005, ECLI:NL:HR:2005:AS5010 (*Laurus*).

aard van de uitgeoefende activiteiten, de in het algemeen daaruit voortvloeiende risico's, de taakverdeling, eventueel geldende richtlijnen en de gegevens waarover de bestuurder beschikte of behoorde te beschikken.¹³⁸ Gezien het feit dat in de media ontzettend veel geschreven wordt over AI en de (basis)risico's enigszins toegankelijk zijn, zou mijns inziens van het bestuur mogen worden verwacht dat het bekend is met een (deel) van deze risico's en daaropvolgend uit hoofde van haar bestuursstaak nader onderzoek doet, zelfs wanneer AI ter inperking van andere risico's wordt gebruikt. Hierbij zou wel onderscheid gemaakt mogen worden in AI ter inperking van compliance risico's en risico's ten aanzien van financiële doelstellingen.

Echter, niet alleen de identificatie van risico's kan in het licht van het *maatman bestuurderscriterium* vragen oproepen, ook het gebrek aan beheersingsmaatregelen en de voortdurende ontwikkeling van AI kan de invulling daarvan bemoeilijken. Dit geldt zowel voor het gebruik van AI in de onderneming op zichzelf, maar ook voor het gebruik van AI als beheersingsmaatregel ten aanzien van andere risico's. In beide gevallen zal afgewogen moeten worden in hoeverre de risico's bedreiging vormen voor de doelstellingen van de onderneming. Deze afweging zal uiteraard van elkaar verschillen, doordat de toepassing van AI eveneens van elkaar verschilt. Wanneer de risico's ten aanzien waarvan AI als beheersingsmaatregel wordt gebruikt hogere beheersingsprioriteit hebben dan het gebruik van AI op zichzelf, zal bestuurdersaansprakelijkheid namelijk minder voor de hand liggen.

Opmerking verdient dat het potentiële gebrek aan identificatie- en beheersingsmogelijkheden vennootschappen die gebruik maken van AI niet ontslaan uit de verantwoordelijkheid om de publieke belangen die in het geding zijn te beschermen.¹³⁹ Daarbij dient in ogenschouw te worden genomen dat in (semi) publieke sectoren, zoals de gezondheidszorg, ten aanzien van de bestuurders een strengere norm in acht moet worden genomen, omdat er sprake is van een publiek belang. Dit publieke belang kan bestaan uit een maatschappelijk- en/of financieel belang. Hierbij valt te denken aan het feit dat in deze sectoren veelal gebruik wordt gemaakt van publieke gelden, waardoor rekening dient te worden gehouden met een grotere groep stakeholders. De belangen van deze stakeholders moeten dan ook altijd zorgvuldig worden afgewogen, hetgeen een verzwaarde zorgvuldigheidsnorm voor het bestuur met zich meebrengt.¹⁴⁰ Het vorenstaande impliceert dan ook dat de hoge drempel voor aansprakelijkheid – het ernstig verwijt – in het geval van een groot maatschappelijk of financieel publiekelijk belang sneller aanwezig is dan in andere gevallen.¹⁴¹ Het gebruik van AI in dergelijke ondernemingen kan in dat geval immers verregaande gevolgen hebben. Desalniettemin zal in dat geval

¹³⁸ HR 10 januari 1997, ECLI:NL:HR:1997:ZC2243 (*Staleman/Van de Ven*).

¹³⁹ *Waarde(n)volle zorgtechnologie* 2019, p. 21.

¹⁴⁰ Westenbroek 2017, p. 112.

¹⁴¹ *Kamerstukken II* 2008/09, 31763, 3, p. 9-11, (MvT).

eveneens de afweging moeten worden gemaakt of het beheersen van risico's door middel van AI juist van het bestuur verwacht mag worden, of dat het gebruik van AI meer risico's met zich meebrengt dan dat het beheerst. Hier zal in paragraaf 6.2.3.4 nog nader op in worden gegaan.

Tenslotte wordt over het algemeen in de literatuur aangenomen dat het handelen in strijd met wet- en regelgeving die gemaakt zijn ter bescherming van de rechtspersoon eveneens moet worden meegenomen als omstandigheid. Zo wordt de NCGC hiertoe gerekend, maar eveneens de bestuursplicht ter zake van risicomanagement, welke uiteen is gezet in paragraaf 4.2.¹⁴²

5.3 Externe bestuurdersaansprakelijkheid ex art. 6:162 BW

Op grond van art. 6:162 BW kunnen derden het bestuur aansprakelijk stellen wegens een onrechtmatige daad jegens hen, voor de door hun geleden schade.¹⁴³ Uit dit artikel blijkt dat er sprake moet zijn van een aantal elementen te weten: onrechtmatigheid, toerekenbaarheid, schade en causaal verband. Voorts blijkt uit art. 6:163 BW dat er eveneens sprake moet zijn van relativiteit. Ingevolge art. 6:162 lid 2 BW kan de onrechtmatigheid voortvloeien uit een inbreuk op een recht, een doen of nalaten in strijd met een wettelijke plicht of met hetgeen volgens ongeschreven recht in het maatschappelijk verkeer betaamt. In beginsel zal falend risicomanagement gezien worden als een doen of nalaten in strijd met een wettelijke plicht, gekeken naar de bestuursplicht zoals deze uiteen is gezet in paragraaf 4.2. Hierbij valt bijvoorbeeld eveneens te denken aan een (grove) schending van de AVG. Daarnaast kan een inbreuk op een recht zich voor doen, te weten de inbreuk op een van de grondrechten die uiteengezet zijn in paragraaf 3.3.7.

De Hoge Raad heeft in het *Onvanger/Roelofsen* arrest bepaald dat voor bestuurdersaansprakelijkheid ex art. 6:162 BW eveneens de maatstaf *ernstig verwijt* dient te worden gehandhaafd, zoals deze in paragraaf 5.2.1 uiteen is gezet. De bestuurstaak dient immers ten aanzien van derden ook behoorlijk te worden uitgevoerd.¹⁴⁴ Deze invulling is in latere jurisprudentie overeind gebleven.¹⁴⁵ Louter in gevallen waarin een zorgvuldigheidsnorm is geschonden die niet uit art. 2:9 BW voortvloeit kan deze invulling niet gebruikt worden. Dit is echter in het kader van bestuurdersaansprakelijkheid niet aan de orde.¹⁴⁶

Bij inkleuring van art. 6:162 BW met art. 2:9 en het daaruit voortvloeiende criterium ernstig verwijt, wordt eveneens een geïntegreerde aanpak gehanteerd, waarbij het ernstig verwijt zowel toeziet op de onrechtmatigheid van de gedraging, alsmede op de toerekenbaarheid daarvan aan de

¹⁴² Zie: Wezeman 1998, p. 69.; Asser/Maeijer & Kroeze 2-1* 2015/199.

¹⁴³ Pitlo/Raaijmakers 2017, p. 314-316.

¹⁴⁴ HR 8 december 2006, ECLI:NL:HR:2006:AZ0758 (*Ontvanger/Roelofsen*).

¹⁴⁵ Zie bijvoorbeeld: HR 2 maart 2007, ECLI:NL:HR:2007:AZ3535 (*Holding Nutsbedrijf Westland*); HR 20 juni 2008, ECLI:NL:HR:2008:BC4959 (*Willemsen/NOM*).

¹⁴⁶ Zie bijvoorbeeld: HR 23 november 2012, ECLI:NL:HR:2012:BX5881, NJ 2013/302 (*Spaanse Villa*), HR 5 september 2014, ECLI:NL:HR:2014:2628, NJ 2015/21 (*Tulip Air*).

bestuurder.¹⁴⁷ Voor de verdere beoordeling of bestuurders aansprakelijk kunnen zijn voor falend risicomanagement inzake AI, zal dan ook louter dit element betrokken worden.

Waar wel rekening mee dient te worden gehouden is dat het gebruik en de invulling van het criterium ernstig verwijt in procedures aangaande bestuurdersaansprakelijkheid op grond van art. 2:9 BW en art. 6:162 BW niet zonder meer met zich mee brengt dat wanneer een bestuurder succesvol op een der gronden aansprakelijk wordt gesteld, dit eveneens leidt tot aansprakelijkheid op grond van het andere artikel.¹⁴⁸ Immers, het gebruik van AI kan voor de onderneming voordelig en gunstig zijn, maar wel schade toebrengen aan derden. Het ernstig verwijt zal dus moeten worden bezien in het licht van degene die daardoor schade ondervindt.

5.4 (On)behoorlijk bestuur en ernstig verwijt maatstaf in het licht van risicomanagement

5.4.1 Falend risicomanagement

Volgens Strik moet in het kader van bestuurdersaansprakelijkheid voor falend risicomanagement onderscheid worden gemaakt tussen risico's die betrekking hebben op compliance en de financiële verslaggeving van een vennootschap en operationele- en strategische risico's.¹⁴⁹ In geval van risico's met betrekking tot wet- en regelgeving zou een bestuurder namelijk minder beleidsvrijheid toekomen dan het geval waarin het bestuur vrijwillig risico's aanvaard. Hierin kan ten aanzien van de risico's van AI een onderscheid worden gemaakt tussen de risico's betreffende compliance, zoals grondrechtenschendingen, schending van de AVG of andere relevante wet- en regelgeving en de overige risico's die uiteengezet zijn in paragraaf 3.3. Ook zal moeten worden gekeken naar het verschil tussen AI als beheersingsmaatregel en het gebruik van AI binnen de onderneming op zichzelf. Daarnaast dient ten aanzien van bestuurdersaansprakelijkheid rekening te worden gehouden met de mate waarin derden betrokken zijn bij de door de onderneming verkozen risico's. Crediteuren en aandeelhouders zijn vaak immers vrijwillig betrokken, terwijl andere derden niet voor deze risico's gekozen hebben. Dit kan bijvoorbeeld het geval zijn wanneer een zelfrijdende auto een ongeluk veroorzaakt, waarbij een aangereden persoon schade lijdt of zelfs komt te overlijden.

Het verwezenlijken van dergelijke risico's brengt echter niet noodzakelijkerwijs met zich mee dat er sprake is van een falend risicobeheersings- en controlesysteem.¹⁵⁰ De vraag of er sprake is van een falend systeem moet aan de hand van de door bestuurders gevolgde procedure en de logica die aan hun besluiten ten grondslag ligt worden beoordeeld. Het bestuur heeft immers de door Strik geformuleerde 'kritische faalfactoren' – welke bestaan uit psychologische-, externe- en interne factoren – niet altijd in de hand.¹⁵¹ Behoorlijke taakvervulling ten aanzien van risicomanagement brengt op grond

¹⁴⁷ Strik 2010, p. 35.

¹⁴⁸ Stolp, *NJB* 2013/1344, afl. 22, p. 1440-1447.

¹⁴⁹ Strik 2010, p. 244.

¹⁵⁰ Vgl. Stulz 2008, p. 2.

¹⁵¹ Strik 2010, p. 247.

van het bovenstaande dan ook geen resultaatverplichting, maar een inspanningsverbintenis met zich mee.¹⁵² In dat licht bezien, dient er voor het vestigen van bestuurdersaansprakelijkheid ten aanzien van falend risicomanagement onderscheid te worden gemaakt in vijf aan risicomanagement gerelateerde categorieën met fouten, welke door Strik als volgt uiteen zijn gezet: (i) de afwezigheid van een risicobeheersingssysteem, (ii) systeemfouten, (iii) werkingsfouten, (iv) beoordelingsfouten en (v) onvoldoende transparantie aan de markt over risico's en risicobeheersing.¹⁵³

5.4.2 Risicobeheersingsfouten

5.4.2.1 Afwezigheid van een systeem

Het geval waarin risicobeheersings- en controlesystemen in zijn geheel ontbreken komt niet vaak voor in grote vennootschappen, doch in het MKB ligt deze mogelijkheid meer voor de hand. Gezien de vele startups die gebruik maken van AI technologieën is deze kans dus reëel aanwezig. De waarschijnlijkheid dat in grotere vennootschappen waarin toepassingen van AI wordt gebruikt een systeem geheel ontbreekt is klein. Gelet op principe 1.2 van de NCGC en het toepassingsbereik van de Code, wordt van vennootschappen – afhankelijk van een aantal factoren – verwacht dat een dergelijk systeem in meer of mindere mate aanwezig is. In dat licht zijn Huizink¹⁵⁴, Strik¹⁵⁵ en Bier¹⁵⁶ van mening dat de afwezigheid van zo'n systeem dan ook zonder meer onbehoorlijke taakvervulling van het bestuur oplevert.

5.4.2.2 Systeemfouten

Van systeemfouten kan gesproken worden wanneer de systemen gebrekkig zijn, bijvoorbeeld wanneer in de onderneming een systeem aanwezig is, maar deze niet (voldoende) toeziet op een bepaald risico, alsmede de situatie waarin weliswaar ten aanzien van dat risico een systeem bestaat, maar waarbij dat risico onvoldoende wordt beheerst door dat systeem. In beginsel levert een dergelijke fout onbehoorlijke taakvervulling op, doch is dit afhankelijk van de mate waarin een risicobeheersings- en controlesysteem vereist is. Blijkens paragraaf 4.3.1 kan dit behoorlijk verschillen tussen bijvoorbeeld beursgenoteerde ondernemingen en startups. In dit kader valt te denken aan de mogelijkheden tot beheersing van de risico's betreffende AI, omdat deze veelal nog onderzocht moeten worden en een passende beheersing daaromtrent niet altijd voor handen is. Echter, gekeken naar de mate waarin AI reeds toegepast wordt in ondernemingen – veelal onder toezien oog van de mens en slechts ter aanvulling of vergemakkelijking van een specifieke taak – zijn mijns inziens reeds mogelijkheden om handen om deze risico's beheersbaar te maken. Het geheel ontbreken van beheersing daaromtrent zou in dat geval – mits deze toegepast worden binnen een voldoende grote vennootschap – een onbehoorlijke taakvervulling op kunnen leveren. Daarnaast valt in te denken dat in het geval waarin AI

¹⁵² Asser/Maeijer/Van Solinge & Nieuwe Weme 2-II* 2009/445.

¹⁵³ Strik 2010, p. 259.

¹⁵⁴ Huizink 2009, p. 84.

¹⁵⁵ Strik 2009, p. 261.

¹⁵⁶ Bier, *OR* 2005/188, afl. 16.

als beheersingsmaatregel wordt gebruikt, over het hoofd wordt gezien dat AI op zichzelf ook (grote) risico's met zich mee brengt. Dit kan een systeemfout tot gevolg hebben, ten aanzien waarvan de eerdere redenering eveneens geldt. De beheersbaarheid van de risico's van AI zal in hoofdstuk 6 nader toegelicht worden.

5.4.2.3 Werkingsfouten

Fouten in de werking van een systeem kunnen worden gekwalificeerd als werkingsfout. Dit is bijvoorbeeld het geval wanneer de systemen op een juiste wijze zijn opgezet – dat wil zeggen ten aanzien van de op correcte wijze in kaart gebrachte risico's – maar waarbij de procedures en maatregelen die daarvan deel uit maken niet (juist) zijn toegepast. Hierdoor heeft het bestuur niet de gelegenheid om alle belangrijke informatie betreffende de risico's te verkrijgen en alle belangrijke handelingen of verzuimen in strijd met het risicobeheersingssysteem te monitoren. Voor beantwoording van de vraag of een dergelijke fout onbehoorlijk bestuur oplevert dient te worden gekeken naar de aard van de fout, op welk niveau in de onderneming deze gemaakt is en in hoeverre het bestuur wist of behoorde te weten van deze fout.¹⁵⁷ Hierbij is ook de grootte van de onderneming van belang, omdat bij bijvoorbeeld grote ondernemingen de afstand tussen het bestuur en de laag waarop de fout gemaakt wordt ver uit elkaar kan liggen. In dat geval is het onwaarschijnlijker dat het bestuur van deze fout wist of behoorde te weten. In het geval van een grove fout zal dit sneller aangenomen worden dan in het geval van een kleine fout.

5.4.2.4 Beoordelingsfouten

Beoordelingsfouten zijn fouten die betrekking hebben op de beoordelingen die gemaakt worden door het bestuur. Daaronder vallen niet de beoordelingen van de risicomangers, zij zien immers alleen toe op het signaleren en beperken van risico's. Voorbeelden van beoordelingen die bestuurders dienen te maken zijn: het bepalen van de *risk appetite* van de onderneming, het bepalen van de strategische en operationele doelstellingen van de onderneming, het bepalen van de gewenste reactie op reeds geïdentificeerde risico's, het bepalen van de manier waarop in de praktijk gereageerd wordt wanneer een risico zich verwezenlijkt, alsmede tal van andere beoordelingen. Deze beoordelingsfouten dienen te worden getoetst aan het *ernstig verwijt* criterium van art. 2:9 BW, waarbij de *maatman bestuurder* uit het Staleman/van de Ven arrest een grote rol speelt.

Hier schuilt mijns inziens dan ook het grootste risico voor bestuurders ten aanzien van het gebruik van AI. Zoals in hoofdstuk 2 en 3 reeds beschreven is, is AI aan sterke ontwikkeling onderhevig, waardoor het in steeds meer vennootschappen kansen en oplossingen biedt, voor steeds gecompliceerdere vraagstukken. De kans is dan ook groot dat AI op korte termijn steeds meer toepassing vindt in vennootschappen. Zeker gezien de stellingen dat AI 'de toekomst' is en derhalve

¹⁵⁷ Strik 2010, p. 261.

noodzakelijk zal zijn voor het voortbestaan van de onderneming. De risico's die bij dergelijke vormen van AI komen kijken, zijn lastig in te schatten. Dit blijkt eveneens uit de meningen van 'experts', die uiteen lopen van de risico's die in hoofdstuk 3 zijn weergegeven, tot een overname van de algehele mensheid. Ten aanzien van de *risk appetite* zal de bestuurder dan ook een belangrijke afweging dienen te maken.

Enerzijds biedt AI grote kansen ten aanzien van innovatie, kostenbesparing en het beheersen van risico's. Anderzijds brengt het ook behoorlijke risico's met zich mee. Een bestuurder zal dan ook een afweging moeten maken tussen de baten en lasten van het gebruik van AI in de onderneming. Daarbij dient in ogenschouw te worden genomen dat de risico's ten aanzien van compliance in mindere mate mogen worden genomen dan risico's ten aanzien van operationele- en strategische doelstellingen. Dit geldt dus zowel voor het gebruik van AI als beheersingsmaatregel, als het gebruik van AI op zichzelf. In het eerste geval zal gekeken moeten worden of de risico's die met AI worden beheerst, van meer belangrijke aard zijn dan de risico's die de toepassing van AI met zich meebrengt. In het tweede geval zal dus voor een minder risicovol beleid dienen te worden gekozen ten aanzien van bijvoorbeeld cyberrisico's, omdat daardoor de AVG kan worden geschonden. Daarnaast kan worden gesteld dat toepassingen van AI in ondernemingen die publiekelijke invloed hebben, zoals het openbaar vervoer en de gezondheidszorg, een beperktere beleidsvrijheid hebben ten aanzien van het nemen van risico's. Hier dient het bestuur dan ook rekening mee te houden.

Gekeken naar de toepassing die AI reeds vindt in ondernemingen, zullen de risico's beperkter zijn dan in de toekomst. Desalniettemin bestaan de grootste risico's van AI: het gebrek aan interpreteerbaarheid en transparantie van een toepassing en daarmee het risico op non-compliance met wet- en regelgeving en de potentiële schending van grondrechten, eveneens voor de mate waarin AI reeds toepassing vindt. Echter zijn vele toepassingen op dit moment slechts gericht op een enkele taak, waarbij een menselijke factor in de meeste gevallen nog aanwezig is. Daarentegen blijkt uit hoofdstuk 4 dat de beheersing van de risico's die hedendaagse toepassingen met zich mee brengen al lastig kan zijn. Dit komt doordat er bijvoorbeeld nog onvoldoende onderzoek is gedaan naar *explainable AI* om het risico van het gebrek aan interpreteerbaarheid te ondervangen. In dat licht bezien lijkt het onmogelijk een bestuurder aansprakelijk te stellen voor iets wat nog niet bekend is. De vraag die dan rijst is of de bestuurder deze implementatie van AI had mogen doen omdat het bijvoorbeeld grote kansen met zich mee bracht ten aanzien van kostenbesparing of beheersing van andere risico's, dat het juist een beoordelingsfout is, of dat het gebrek aan beheersingsmaatregelen er toe zou moeten leiden dat het bestuur de keuze maakt om AI nog geen toepassing te geven in de onderneming. Het uitgangspunt hierbij is de kennis die op het moment van de beoordeling bij de bestuurder aanwezig

is.¹⁵⁸ Hierbij wordt terug gegrepen op het criterium ernstig verwijt en de daaruit voortvloeiende *maatman bestuurder*. Hoewel de risico's betreffende AI potentieel enorm zijn zou het gebruik daarvan, bij gebrek aan voldoende identificatie- of beheersingsmogelijkheden mijns inziens niet zomaar aan banden gelegd moeten worden. Het gebruik van AI brengt immers ook enorme kansen voor de onderneming met zich mee. In dat licht zou zelfs voorzichtig kunnen worden gesteld dat een bestuurder een vorm van AI in sommige gevallen wordt geacht te gebruiken, ten aanzien van bijvoorbeeld het beperken van compliance risico's. Deze moeten immers zo veel mogelijk beheerst worden, AI biedt in dat geval veel meer mogelijkheden dan dat de mens kan bieden.

Het gebrek aan bepaalde identificatie- en beheersingsmogelijkheden zou mijns inziens echter niet met zich mee mogen brengen dat implementatie van een verregaande vorm van AI zomaar mogelijk is, louter omdat de kennis daaromtrent nu nog niet bestaat en de bestuurder dit dus feitelijk niet kon weten. Mogelijkerwijs kan bij dit vraagstuk dan ook aansluiting gevonden worden bij de ethische richtsnoeren van de EC, die zijn uitgewerkt in paragraaf 3.3.7. Hieruit kan door het bestuur worden afgeleid wat verwacht wordt ten aanzien van het gebruik van AI. Bovenstaande illustreert des te meer dat het voor de vraag of een bestuurder aansprakelijk gesteld kan worden voor falend risicomanagement altijd afhankelijk is van de omstandigheden van het geval.

5.4.2.5 Gebrek aan transparantie

Het gebrek aan transparantie aan de markt over risico's en risicobeheersing vormt de laatste risicobeheersingsfout. Te denken valt hierbij aan het doen van foutieve mededelingen en het verzuimen van het doen van belangrijke mededelingen (bijvoorbeeld ten aanzien van de beurskoers).¹⁵⁹ Deze categorie van fouten kunnen echter in ieder systeem worden gemaakt en zijn derhalve niet relevant voor het onderzoek specifiek naar AI.

5.5 Conclusie

Op welke wijze(n) kan het bestuur van een kapitaalvennootschap aansprakelijk worden gesteld voor falend risicomanagement inzake AI?

Bestuurders kunnen op grond van art. 2:9 BW intern jegens de vennootschap en op grond van art. 6:162 BW extern jegens derden aansprakelijk worden gesteld, indien zij onbehoorlijk hebben bestuurd en hen daartoe een ernstig verwijt kan worden gemaakt. In het Staleman/van de Ven arrest is bepaald dat het handelen van het bestuur ter beoordeling van het ernstig verwijt dient te worden getoetst aan de *maatman bestuurder*: 'het inzicht en de zorgvuldigheid die mogen worden verwacht van een bestuurder die voor zijn taak berekend is en deze nauwgezet vervult'. Hierbij zijn de omstandigheden van het geval van groot belang. In het Ontvanger/Roelofsen arrest is voorts bepaald dat dit criterium eveneens geldt

¹⁵⁸ Strik 2010, p. 265.

¹⁵⁹ Strik 2010, p. 265

in een onrechtmatige daad procedure op grond van art. 6:162 BW. In dit kader worden de normen onbehoorlijk bestuur en ernstig verwijt middels een geïntegreerde aanpak gebruikt.

Bestuurdersaansprakelijkheid mag niet te snel worden aangenomen, omdat het bestuur ten aanzien van de bestuursstaak een zekere beleidsvrijheid heeft en het gevaar van *hindsight bias* op de loer ligt. Echter, onwenselijk zou zijn dat bestuurders AI reeds op verregaande wijze implementeren, door te stellen dat het bestuur niet bekend was met de mogelijk verregaande gevolgen daarvan. Mijns inziens zou van een bestuurder mogen worden verwacht dat hij bekend is met een (deel) van de risico's betreffende AI, ook wanneer deze in zekere zin onvoorspelbaar zijn. Daarentegen zou het gebrek aan identificatie- en beheersingsmaatregelen, gezien de grote kansen die AI biedt, de eventuele implementatie niet zomaar aan de kant mogen schuiven. De vraag is waar de grens ligt bij de invulling van het begrip *maatman bestuurder*, wat wist of behoorde de bestuurder in dat geval te weten? Hierbij zou dan ook een onderscheid gemaakt moeten worden tussen het geval dat AI als beheersingsmaatregel ten aanzien van andere risico's wordt ingezet en het geval dat AI op zichzelf gebruikt wordt in de onderneming. Zaken die eveneens onder de omstandigheden van het geval meegenomen moeten worden zijn onder andere het handelen in strijd met wet- en regelgeving, waaronder de bestuursplicht ter zake van risicomanagement alsmede de regels in de NCGC.

Het verwezenlijken van risico's levert niet noodzakelijkerwijs een falend risicosysteem op. Daarvoor dient er sprake te zijn van een risicobeheersingsfout. Zo levert de afwezigheid van een risicobeheersings- en controlesysteem in grotere ondernemingen per definitie een onbehoorlijke taakvervulling op. Systeem- en werkingsfouten leveren – op basis van de omstandigheden van het geval – mogelijk een onbehoorlijke taakvervulling op. Datzelfde geldt voor het gebrek aan transparantie aan de markt over risico's en risicobeheersing.

Beoordelingsfouten zijn in het kader van AI het meest waarschijnlijk, gekeken naar de risico's die met het gebruik gepaard gaan. De bestuurder zal een goede afweging moeten maken tussen innovatie en kostenbesparing binnen de onderneming middels het toepassen van AI enerzijds en de risico's die daarbij komen kijken anderzijds. Hierbij moet een onderscheid gemaakt worden tussen risico's betreffende compliance en risico's betreffende operationele- en strategische doelstellingen. In dat laatste geval komt de bestuurder meer beleidsvrijheid toe. Daarnaast moet onderscheid gemaakt worden tussen het geval dat AI gebruikt wordt als beheersingsmaatregel en het geval dat AI bijvoorbeeld louter ter kostenbesparing wordt gebruikt. Ook dient te worden gekeken naar de sector waarin de kapitaalvennootschap zich bevindt. Vervolgens dient ook te worden gekeken naar wat de bestuurder wist en behoorde te weten, gelet op het *maatman bestuurder* criterium.

Uit bovenstaande is af te leiden dat bestuurdersaansprakelijkheid voor falend risicomanagement inzake AI zeer zeker mogelijk is, maar dat daarbij dient te worden gekeken naar de soort risicobeheersingsfout en naar alle omstandigheden van het geval.

6. INRICHTING RISICOBEBEERSINGS- EN CONTROLESYSTEEM

6.1 Inleiding

Zoals eerder uiteengezet in hoofdstuk 4 en hoofdstuk 5, is het bestuur in veel gevallen verplicht tot het opzetten van een risicobeheersings- en controlesysteem ten aanzien van de risico's die de kapitaalvennootschap loopt. Vennootschappen kunnen ervoor kiezen om zelf een systeem op te zetten, maar veelal wordt gebruik gemaakt van een vooraf opgezet 'framework'.¹⁶⁰ Het Enterprise Risk Management Framework dat wereldwijd het breedst gedragen wordt, is dat van COSO. Dit staat ook wel bekend onder de naam: COSO 2017 Enterprise Risk Management – Integrating with Strategy and Performance. Hierin staat de integratie tussen risicomanagement en het strategie-ontwikkelingsproces en prestatie management centraal. Niet alleen worden risico's hiermee teruggebracht naar een acceptabel niveau, ook is het gericht op de lange termijn waardecreatie van de onderneming.¹⁶¹ De toespitsing op integratie is noodzakelijk omdat risicomanagement niet slechts gezien kan worden als een op zichzelf staand proces. Het is voor de juiste werking nodig dat een systeem volledig geïntegreerd is in een bedrijf. Effectief risicomanagement kan namelijk nooit ontstaan door middel van het 'afvinken' van alle elementen van een systeem. Het gaat juist om het samenspel tussen de instrumentele risicobenadering en gedrag en cultuur.¹⁶²

Blijkens paragraaf 5.4.1 en paragraaf 5.4.2 kunnen bestuurders aansprakelijk worden gesteld voor falend risicomanagement, indien er sprake is van een beheersingsfout. Gekeken naar de risico's die met het gebruik van AI gepaard gaan, zullen beoordelingsfouten waarschijnlijk het meeste voorkomen. Echter zouden systeem- en werkingsfouten ook voor kunnen komen. In dit hoofdstuk zal daarom gekeken worden naar de handvaten die COSO 2017 biedt om aansprakelijkheid te voorkomen. Hiertoe worden de vijf componenten van COSO 2017 uitgelegd, in verhouding tot het gebruik van AI en de kansen en risico's die daarmee gepaard gaan. Voorts zullen deze componenten, alsmede de principes die daarbij horen, in het licht worden gezien van risicobeheersingsfouten. Op die manier kan uiteindelijk een antwoord worden gegeven op de vraag of een risicomanagement systeem zoals COSO 2017 bestuurdersaansprakelijkheid voor falend risicomanagement inzake AI kan voorkomen.

¹⁶⁰ Strik 2010, p. 225.

¹⁶¹ COSO Enterprise Risk Management 2017.

¹⁶² Gorter, OR 2016/73, afl. 9, par. 11.

6.2 De vijf componenten van COSO 2017

6.2.1 Governance en cultuur

6.2.1.1 Strategie

Het eerste principe in de eerste component legt bij het bestuur de verantwoordelijkheid neer om overzicht te hebben over onder andere de strategie van de onderneming.¹⁶³ In deze strategie kan het gebruik van AI vervat zijn, omdat dat de strategie een middel kan zijn om (een van) de operationele doelstellingen van de onderneming te verwezenlijken. Het gebruik van AI brengt blijkens paragraaf 3.4 immers grote kansen met zich mee. De gekozen strategie moet een balans zijn tussen de gewenste externe resultaten en de bestaande interne mogelijkheden.¹⁶⁴ Met die strategie gaan risico's gepaard, welke dus eveneens onder het genoemde overzicht van het bestuur vallen. In dit kader zijn met name de concrete risico's van belang, die zich openbaren door het gebrek aan interpreteerbaarheid, transparantie en betrouwbaarheid. De concrete risico's zijn in dat kader non-compliance met wet- en regelgeving, cyberrisico's, reputatierisico's en op basis van het vorenstaande ook risico's met betrekking tot de operationele doelstellingen. Verwezenlijking van een der eerder genoemde risico's brengt namelijk eveneens het risico op bijvoorbeeld winstderving met zich mee.

De strategie, bijvoorbeeld de mate waarin AI toepassing zal vinden in de onderneming (een verregaande vorm of minder verregaande vorm) en ten aanzien van welke bedrijfsonderdelen, zal daarom afgestemd moeten zijn op de kansen en potentiële risico's die daarmee gepaard gaan, alsmede op de *risk appetite* van de onderneming. In paragraaf 6.2.2.2 zal op dat laatste dieper worden ingegaan.

6.2.1.2 Operationele structuur

Volgens principe 2 draagt het bestuur de verantwoordelijkheid voor het neerzetten van een operationele structuur, die de strategie en zakelijke doelstellingen van de onderneming nastreeft.¹⁶⁵ De operationele structuur betreft de organisatie van bedrijfsactiviteiten. Het geeft weer welke taken, bevoegdheden en verantwoordelijkheden de werknemers hebben.¹⁶⁶ Daarnaast is het een uiteenzetting van de functionele onderdelen van de onderneming, waarbij eveneens onderlinge verhoudingen worden weergegeven.¹⁶⁷ Een dergelijke structuur bestaat uit de verschillende lagen in de onderneming, waarin de taken, functies en verantwoordelijkheden worden onderverdeeld. Deze taken, functies en verantwoordelijkheden dienen helder te zijn voor iedere operationele laag. De structuur moet op die manier opgebouwd zijn, dat er zowel van bovenaf (het bestuur, de RvC, enzovoorts) naar beneden (lagere managementlagen en medewerkers) als van beneden naar boven helder kan worden gecommuniceerd. Op deze manier wordt door het bestuur de rest van de onderneming bewust gemaakt

¹⁶³ COSO *Enterprise Risk Management* 2017, principle 1.

¹⁶⁴ Nieuwenhuis 2003, p. 11.

¹⁶⁵ COSO *Enterprise Risk Management* 2017, principle 2.

¹⁶⁶ Nieuwenhuis 2003, p.11.

¹⁶⁷ Claes, Janicijvic & Lengkeek 2012, p. 82.

van bijvoorbeeld risico's en kan vanaf beneden naar het bestuur worden gecommuniceerd over potentiële risico's en de verwezenlijking daarvan.

6.2.1.3 Risicocultuur

Blijkens principe 3 dient zorg te worden gedragen voor de uiteenzetting van de gewenste (risico)cultuur binnen de onderneming, alsmede de gedragingen die daarbij gepast zijn.¹⁶⁸ Het is van belang dat de cultuur past bij de context (zie paragraaf 6.2.2.1) van de onderneming en dat deze onderling afgestemd wordt met de missie, kernwaarden en strategie van de onderneming.¹⁶⁹ De zogeheten *tone at the top* impliceert dat cultuur start bij het bestuur en vanuit daar doorsijpelt naar de rest van de onderneming.¹⁷⁰ Het bestuur bepaalt dus in feite het gedrag en de handelingen die nodig zijn om integriteit en ethische waarden uit te dragen, alsmede om op de gewenste manier de doelstellingen van de onderneming te behalen. Hiertoe kunnen bijvoorbeeld expliciete regels, gedragsstandaarden en processen voor besluitvorming worden opgesteld. Hierbij valt te denken aan expliciete regels omtrent het gebruik van AI, om bijvoorbeeld oneigenlijk gebruik daarvan te voorkomen. Daarentegen kunnen deze regelingen het gebruik van AI juist stimuleren, zeker wanneer AI als risicobeheersingsmaatregel wordt ingezet. Van belang hierbij is dat helder moet zijn dat een systeem niet geheel op zichzelf mag functioneren, maar dat de uiteindelijke beslissing vooralsnog bij de mens moet liggen.

Om de cultuur daadwerkelijk te waarborgen dienen de genoemde standaarden en regels tijdig geëvalueerd te worden, waarna indien nodig ingegrepen dient te worden. In de cultuur zal dus ook grotendeels de risicobereidheid (zie paragraaf 6.2.2.2) van de onderneming naar voren komen, omdat dat als rode draad door de besluitvormingsprocessen en het gedrag binnen de onderneming moet lopen. Het gaat hierbij met name om de bewustwording van de wijze waarop de onderneming in het algemeen met risico's wenst om te gaan. Deze cultuur geldt zowel intern, bijvoorbeeld ten aanzien van de besluitvorming, alsook extern, ten aanzien van klanten, leveranciers en andere stakeholders.¹⁷¹

6.2.1.4 Commitment aan kernwaarden

Het vierde principe schrijft voor dat er commitment getoond moet worden aan de kernwaarden van de onderneming.¹⁷² In dit kader is het van belang dat de risicocultuur niet slechts een keer genoemd wordt door het bestuur, maar dat er waarde wordt gehecht aan de bewustwording daarvan in de onderneming. Het bestuur bekleedt dan ook te allen tijde een voorbeeldfunctie, waarbij de risicobewuste cultuur omarmd moet worden. Daarnaast moet er frequent en open gecommuniceerd

¹⁶⁸ COSO Enterprise Risk Management 2017, principle 3.

¹⁶⁹ Culture as a Corporate Asset 2017, p.9.

¹⁷⁰ COSO Enterprise Risk Management 2013, p. 4.

¹⁷¹ Culture as a Corporate Asset 2017, p.9.

¹⁷² COSO Enterprise Risk Management 2017, principle 4.

worden over het bovenstaande, zodat het daadwerkelijk een cultuur zal zijn, die binnen de gehele onderneming leeft.

6.2.1.4 Menselijk kapitaal

Als laatste moet er gestreefd worden naar het opbouwen van ‘menselijk kapitaal’, in overeenstemming met de strategie en bedrijfsdoelstellingen.¹⁷³ Het gaat hierbij om het aantrekken en behoud van personeel. Hierbij kan gedacht worden aan de juiste mensen op de juiste plaats, het belonen van prestaties, de ontwikkeling van werknemers en een goede werkbalans. Gemotiveerde, goed opgeleide en weinig stressvolle werknemers zijn namelijk cruciaal voor goede besluitvorming. In het licht van AI valt te denken aan het aantrekken en/of behouden van werknemers die kennis hebben van AI systemen, zoals de programmeurs om software te ontwikkelen, ingenieurs om de eventuele hardware te bouwen en AI wetenschappers en datawetenschappers om de toepassing intelligent te maken. Mogelijkerwijs kunnen daar werknemers aan toegevoegd worden die kennis hebben van ethiek, omdat het daar blijkens paragraaf 3.3.7 vaak aan ontbreekt. Daarnaast is het verstandig om werknemers die tijdens hun werkzaamheden met toepassingen van AI te maken hebben, training te geven.¹⁷⁴ Op die manier kunnen zij leren hoe een systeem werkt, welke verantwoordelijkheden zij hebben en hoe zij dienen om te gaan met de risico's die met het gebruik van AI gepaard gaan.

6.2.2 Strategie en doelstellingen

6.2.2.1 Context

Volgens het eerste principe in de tweede component, strategie en doelstellingen, moet de onderneming in kaart brengen wat de potentiële effecten van de bedrijfscontext op het risicoprofiel zijn.¹⁷⁵ Hierbij moet gekeken worden naar de interne- en externe context. Zo moet er voor de externe context bijvoorbeeld gekeken worden naar de sector waarin de onderneming opereert, de wet- en regelgeving die op de onderneming van toepassing is, de stand van de politiek, de klantbehoeften, enzovoorts. De interne context kan bijvoorbeeld worden bepaald aan de hand van het kapitaal dat in de onderneming aanwezig is, de technologie die gebruikt wordt en de menselijke kennis die aanwezig is.

Toegespitst op het geval waarin AI gebruikt wordt binnen de onderneming zal dus allereerst gekeken moeten worden in welke sector de vennootschap zich bevindt. Blijkens paragraaf 5.2.1 mag van vennootschappen in de (semi) publieke sector alsmede vennootschappen waarmee publiekelijk maatschappelijk- of financieel belang gepaard gaat worden verwacht dat zij een zwaardere zorgvuldigheidsnorm in acht nemen.¹⁷⁶ Hieruit kan voorzichtig worden afgeleid dat zij ten aanzien van hun beslissingen waarmee het genoemde belang gepaard gaat, geacht worden minder risico's te

¹⁷³ COSO Enterprise Risk Management 2017, principle 5.

¹⁷⁴ Future of risk in the digital era 2019, p. 7.

¹⁷⁵ COSO Enterprise Risk Management 2017, principle 6.

¹⁷⁶ Westenbroek 2017, p. 112; Kamerstukken II 2008/09, 31763, 3, p. 9-11, (MvT).

nemen. Dit brengt echter niet met zich mee dat het gebruik van AI in zijn geheel niet toegelaten is binnen deze sectoren, louter omdat het gepaard gaat met risico's. Deze sectoren hebben vaak immers veel profijt van de grote kansen die AI biedt. Wel moet in ogenschouw worden gehouden dat de wet- en regelgeving voor deze sectoren uitgebreider zal zijn, waardoor het risico op non-compliance groter is. Voorts kan beargumenteerd worden dat niet alleen de sector van belang is, maar ook de wijze waarop AI toepassing vindt in de onderneming. Een interne toepassing zal vaak minder potentiële risico's met zich meebrengen dan een externe toepassing, omdat het onwaarschijnlijker is dat derden daardoor geraakt worden.

De interne context van de onderneming is gezien de complexiteit van AI van groot belang. Zo moet het AI systeem bij de techniek en kennis binnen de onderneming passen. Er is immers specialistische kennis en techniek nodig om een systeem op te zetten, te laten functioneren en te monitoren. Verder is voldoende kennis en techniek vereist om het risico op oneigenlijk gebruik van een toepassing in te perken. Blijkens paragraaf 3.3.1 moet namelijk voorkomen worden dat de AI toepassing gebruikt wordt wanneer het eigenlijk (nog) niet geschikt is voor het doel. In dit licht dient dus specifiek te worden gekeken of AI toepassing past binnen de onderneming, of dat dat mogelijkserwijs nog grotere risico's met zich mee brengt, doordat de benodigde kennis en techniek niet aanwezig zijn.

Eveneens van belang is het kijken naar de processen die in de onderneming aanwezig zijn. Goed georganiseerde operationele processen vergroten de kans op succesvolle risicobeheersing, doordat bijvoorbeeld de verwezenlijking risico's tijdig geïdentificeerd en gecommuniceerd worden. Deze structuur is daarom van groot belang voor de mate waarin een onderneming de kansen die AI met zich meebrengt benut en de mate waarin de onderneming risico's kan en mag nemen.

Als laatste is het van belang dat er inzicht is in de financiële gezondheid van de onderneming. Een gezond bedrijf kan meer risico's nemen dan een ongezond bedrijf, omdat de eventuele verwezenlijking van deze risico's in dat geval beter opgevangen kunnen worden. Op basis van het vorenstaande kan de *risk bearing capacity* worden bepaald. Dat is het beschikbare vermogen om risico's financieel op te vangen.¹⁷⁷

6.2.2.2 Risicobereidheid

Principe 7 schrijft voor dat de risicobereidheid gedefinieerd dient te worden in het kader van de lange termijn waardecreatie, hetgeen eveneens naar voren komt in de NCGC.¹⁷⁸ Hiertoe moet de onderneming de *risk appetite* vaststellen. De context die volgens principe 6 bepaald is, moet hieraan ten grondslag liggen. Verder speelt de houding ten aanzien van risico's een grote rol. Zo zal een risiconemende houding een andere *risk appetite* met zich meebrengen dan een risicomijdende

¹⁷⁷ Claes, Janicijvic & Lengkeek 2012, p. 59.

¹⁷⁸ COSO Enterprise Risk Management 2017, principle 7.

houding.¹⁷⁹ Die houding zou mijns inziens mede ontleend moeten worden aan de context. Ook zal de *risk appetite* aan moeten sluiten bij de missie, visie, waarden en strategie van de onderneming. Het is daarom in feite een weergave van de cultuur ten opzichte van het nemen van risico's.¹⁸⁰ Daarnaast zullen voor de bepaling daarvan eveneens de *risk tolerance* en de *desired level of risk* van belang zijn. De *risk tolerance* is 'de acceptabele variabele in resultaten rondom realisatie van specifieke doelstellingen' en de *desired level of risk* is 'de gewenste verhouding tussen de hoeveelheid risico en omzet'.¹⁸¹

Hoewel de *risk appetite* als een soort basisbeginsel van de cultuur van de onderneming fungeert, kan deze ten aanzien van verschillende investeringen en gebruiken anders zijn dan andere investeringen en gebruiken. Daarnaast kan het zo zijn dat deze voor afdelingen of businessunits onderling van elkaar verschilt, waarbij eveneens verschillende risicoaanpakken kunnen worden gehanteerd.¹⁸² Dit komt doordat de doelstellingen voor deze investeringen en afdelingen van elkaar kunnen verschillen. Het is dan ook van belang een *risk appetite* te definiëren die past bij het bedrijf als geheel, maar die ook toegespitst is op specifieke onderdelen. Het moet daarom gericht zijn op de doelstellingen, waarbij lange termijn waardecreatie in het achterhoofd moet worden gehouden.

In het geval van AI toepassingen in de onderneming is dan ook niet simpelweg vast te stellen wat de *risk appetite* zou moeten zijn. Gezien de vele mogelijkheden die AI biedt, kunnen doelstellingen mogelijk sneller en beter behaald worden mét het gebruik van daarvan. Op die manier zou lange termijn waardecreatie kunnen worden nagestreefd. Echter, de risico's die daarmee gepaard gaan kunnen – afhankelijk van de toepassing – juist afbreuk doen aan deze lange termijn waardecreatie. Van belang is dus dat de *risk appetite* past binnen de onderneming, zowel intern als extern. Het belang van een smetteloze reputatie, bijvoorbeeld op het gebied van compliance, zou daar met name in moeten worden meegewogen.¹⁸³ Het bestuur dient dit dan ook zorgvuldig te overwegen en in kaart te brengen, alvorens een beslissing daaromtrent te nemen. De uiteindelijke beslissing zal goed gecommuniceerd moeten worden, zodat het geïntegreerd kan worden in de besluitvormingsprocessen en derhalve als cultuur gaat leven binnen de onderneming.

6.2.2.3 Alternatieve strategieën

Principe 8 schrijft voor dat er alternatieve strategieën moeten worden vastgesteld, welke geëvalueerd moeten worden aan de hand van de impact op het risicoprofiel.¹⁸⁴ In dit licht is het noodzakelijk dat strategieën die afwijken van het voorgenomen gebruik van AI worden gedefinieerd, welke vervolgens

¹⁷⁹ Claes, Janicijvic & Lengkeek 2012, p. 60.

¹⁸⁰ *Culture as a Corporate Asset* 2017, p. 13-14.

¹⁸¹ Claes, Janicijvic & Lengkeek 2012, p. 61-62.

¹⁸² Strik 2010, p. 228.

¹⁸³ Claes, Janicijvic & Lengkeek 2012, p. 61.

¹⁸⁴ *COSO Enterprise Risk Management* 2017, principle 8.

getoetst moeten worden aan de *risk appetite* van de onderneming. Hierbij kan bijvoorbeeld gedacht worden aan het gebruik van AI in zijn geheel aan banden leggen, de keuze voor een minder verregaande vorm van AI of het gebruik van AI toepassingen slechts voor specifieke taken toestaan, waarbij de mens altijd als controlerende factor fungeert. Aan de hand daarvan kan de beste strategie worden bepaald, die uiteraard overeen moet komen met de *risk appetite*. Indien dat niet het geval is moet óf de strategie, óf de *risk appetite* worden aangepast. Gezien de potentiële kans op beoordelingsfouten ten aanzien van de *risk appetite*, moet aanpassing daarvan met grote zorgvuldigheid worden gedaan.

6.2.2.4 Bedrijfsdoelstellingen

Ingevolge principe 9 moet er rekening worden gehouden met risico's bij het vaststellen van de bedrijfsdoelstellingen. Deze doelstellingen moeten op verschillende niveaus worden vastgesteld en moeten de strategie ondersteunen.¹⁸⁵ Onrealistische verwachtingen of doelstellingen werken immers vaak risicovol gedrag in de hand. Om die reden is het noodzakelijk dat de bedrijfsdoelstellingen op die wijze worden opgesteld, dat redelijkerwijs verwacht kan worden dat deze haalbaar zijn, gekeken naar de kansen, de potentiële risico's en de *risk appetite* van de onderneming. Hiermee wordt voorkomen dat besluitvormingsprocessen louter op de doelstellingen leunen, terwijl deze in overeenstemming zouden moeten zijn met de mate waarin de onderneming bereid is risico's te nemen. Ook van belang is dat de doelstellingen voldoende concreet geformuleerd zijn, zodat hier daadwerkelijk aan kan worden getoetst.¹⁸⁶

Mijns inziens speelt hier niet alleen de *risk appetite*, maar ook de *risk tolerance* een rol. Zoals in paragraaf 6.2.2.2 reeds uiteen is gezet, gaat de *risk tolerance* over de acceptabele afwijking ten aanzien van de doelstellingen. Hieruit volgt des te meer dat de doelstellingen afgestemd moeten zijn op de mate waarin risico's worden genomen, om op die manier binnen de acceptabele afwijking te blijven.

6.2.3 Prestatiemeting

6.2.3.1 Risico-identificatie

Volgens principe 10 moet de onderneming risico's identificeren die van invloed zijn op de prestaties ten aanzien van de strategie en bedrijfsdoelstellingen.¹⁸⁷ Daartoe moeten methoden worden gebruikt die ervoor zorgen dat de risico's worden geïdentificeerd en op waarde worden geschat.¹⁸⁸ Niet alleen de risico's die in het hier en nu spelen zijn van belang, ook toekomstige risico's moeten geïdentificeerd worden.¹⁸⁹ Er bestaat echter geen eenduidige manier waarop dit moet gebeuren, omdat dit per onderneming en zelfs per afdeling kan verschillen.

Vooraf moet worden bepaald welke risico's geïdentificeerd moeten worden. Dit kan

¹⁸⁵ COSO Enterprise Risk Management 2017, principle 9.

¹⁸⁶ Claes, Janicijvic & Lengkeek 2012, p. 82.

¹⁸⁷ COSO Enterprise Risk Management 2017, principle 10.

¹⁸⁸ Strik 2010, p. 233.

¹⁸⁹ Claes, Janicijvic & Lengkeek 2012, p. 75.

uiteenlopen van alle risico's die van invloed kunnen zijn op strategische- en operationele doelstellingen, tot risico's die bijvoorbeeld gelden ten aanzien van aansprakelijkheid of continuïteit van de onderneming.¹⁹⁰ Volgens het COSO raamwerk moeten alle risico's ten aanzien van de bedrijfsdoelstellingen in kaart worden gebracht.¹⁹¹ Hierbij kan onderscheid worden gemaakt tussen interne risico's zoals strategische-, juridische-, materiële- en continuïteitsrisico's en externe risico's zoals maatschappelijke- en economische risico's.

Mijns inziens is het van groot belang dat alle risico's die gepaard gaan met het gebruik van AI in de onderneming in kaart worden gebracht. Deze zullen in het perspectief moeten worden geplaatst van de toepassing die AI vindt in de onderneming. Afhankelijk daarvan zullen deze namelijk groter of kleiner kunnen zijn.

De risico's oneigenlijk gebruik, onbetrouwbaarheid, het gebrek aan interpreteerbaarheid en transparantie kunnen ten aanzien van alle doelstellingen een risico vormen, zowel intern- als extern. De risico's die daar onder andere uit voortvloeien, non- compliance met wet- en regelgeving en het schenden van grondrechten verdienen extra aandacht. De potentiële grondrechtenschendingen, zoals uiteengezet in paragraaf 3.3.7 vormen een gedegen risico bij het gebruik van AI. Deze grondrechten beschermen in beginsel individuen tegen inmenging door de staat in hun privéleven. Echter, door de toenemende invloed van onder andere AI in privaatrechtelijke situaties – zoals dat bij de toepassing daarvan in kapitaalvennootschappen vaak aan de orde is – worden grondrechten steeds relevanter in horizontale verhoudingen.¹⁹² Grondrechten alsmede de handhaving daarvan, kunnen dan ook bijdragen in privaatrechtelijke verhoudingen.¹⁹³ Zo kunnen deze worden meegewogen bij de invulling van civielrechtelijke bepalingen, zoals art. 6:162 BW.¹⁹⁴ Meer concreet kan een privacy schending, bijvoorbeeld door strijd met de AVG, maar ook louter door schending van art. 10 Gw bijdragen aan het aansprakelijkheidsoordeel in een onrechtmatige daad procedure. Hieruit kunnen grote schadevergoedingen voortvloeien. Een schending van het grondrecht op gelijke behandeling kan eveneens bijdragen aan de invulling van art. 6:162 BW, maar brengt ernstige bewijstechnische complicaties met zich mee. Juist doordat beslissingen gemaakt door algoritmes weinig transparant en moeilijk te interpreteren zijn, is het moeilijk aan te tonen dat er ten aanzien van de beslissing daadwerkelijk sprake is van ongerechtvaardigde ongelijke behandeling. Echter, deze complicaties raken direct de effectiviteit van het recht op gelijke behandeling wanneer een beslissing niet voldoende transparant en te interpreteren is. De verzoekende partij moet immers haar rechten wel uit kunnen

¹⁹⁰ Claes, Janicijvic & Lengkeek 2012, p. 76.

¹⁹¹ Claes, Janicijvic & Lengkeek 2012, p. 79.

¹⁹² Vetzo, Gerards & Nehmelman 2018, p. 184.

¹⁹³ Emaus 2013, p. 357.

¹⁹⁴ Vetzo, Gerards & Nehmelman 2018, p. 62.

oefenen.¹⁹⁵ In beginsel zal een dergelijke procedure zich richten op de vennootschap als rechtspersoon, maar wanneer blijkt dat het bestuur ten aanzien van de schending een ernstig verwijt kan worden gemaakt – bijvoorbeeld door een falend risicobeheersings- en controlesysteem – kan dit eveneens tot bestuurdersaansprakelijkheid leiden.

Naast de mogelijke civielrechtelijke procedures op grond van art. 6:162 BW, vormt de potentiële regulering van de staat ten aanzien van grondrechtenschendingen een gedegen risico. De staat moet namelijk, op grond van positieve verplichtingen uit het EVRM, zo veel mogelijk voorkomen dat grondrechtenschendingen plaats vinden alsmede eventuele grondrechtenschendingen redresseren. Hiertoe moet de staat regulerend optreden jegens onder andere rechtspersonen, bijvoorbeeld door middel van adequate handhaving en toezicht.¹⁹⁶ Hierbij valt bijvoorbeeld te denken aan boetes die kunnen worden uitgedeeld door de Autoriteit Persoonsgegevens.

Naast het risico op grondrechtenschendingen, bestaat er eveneens het risico op non-compliance met andere wet en regelgeving. Allereerst bestaan er risico's ten aanzien van wetgeving die ontleed is uit de grondrechten, zoals de AVG en de Wet op de gelijke behandeling. Daarnaast is er veel specifieke wetgeving ten aanzien van producten, bijvoorbeeld in het kader van veiligheid, maar ook specifieke wetgeving ten aanzien van financiële instellingen en de gezondheidszorg. Niet alleen het risico op non-compliance op zichzelf is relevant, ook de risico's die daarmee gepaard gaan zijn van belang. Zo kan non-compliance met veiligheidsvoorschriften ertoe leiden dat er een (dure) terugroepactie plaats dient te vinden. Ook valt in het kader van deze risico's te denken aan boetes die uitgedeeld kunnen worden en strafrechtelijke vervolging door het Openbaar Ministerie, zoals dat bij ING het geval was door het overtreden van de Wwft.¹⁹⁷ In het laatst genoemde scenario was er echter wel bespaard op onder ander het personeel die dubieuze klanten en verdachte geldstromen dienden te controleren. In het geval dat AI wordt gebruikt, zal dit waarschijnlijk niet in deze extreme mate aan de orde zijn, daar vaak nog toezicht van de mens plaats vindt en AI door middel van patroonherkenning juist meer 'ziet' dan de mens. Echter zou wel voor kunnen komen dat middels een ongeïdentificeerde cyberaanval een systeem gemanipuleerd wordt en derhalve verkeerde uitkomsten zal genereren..

De hiervoor genoemde cyberaanvallen kunnen niet alleen ten aanzien van de uitkomsten van een AI systeem een risico vormen, maar ook op zichzelf. Een dergelijke aanval kan de financiële positie van de onderneming in grote mate verslechteren, doordat het oplossen daarvan gepaard gaat met hoge kosten. Er moet dan namelijk onderzocht worden wat de oorzaak van het incident is, hoe dit hersteld moet worden en op welke wijze dit in het vervolg voorkomen kan worden.

Niet alleen de directe gevolgen zoals mogelijke schadevergoeding, boetes en winstderving door

¹⁹⁵ Vetzo, Gerards & Nehmelman 2018, p. 186-187.

¹⁹⁶ Vetzo, Gerards & Nehmelman 2018, p. 185.

¹⁹⁷ Haegens, *de Volkskrant* 4 september 2018.

bijvoorbeeld een terugroepactie of cyberaanval zijn van belang. Schending van grondrechten en non-compliance met wet en regelgeving, leiden daarnaast in de regel vaak tot (grote) reputatieschade.¹⁹⁸ Hoewel er geen concrete en directe gevolgen zitten aan het louter schenden van ethische principes (waarbij niet gelijktijdig andere schendingen plaatsvinden), heeft dit vaak ook reputatieschade tot gevolg. Dergelijke schade zou zelfs de continuïteit van de onderneming in gevaar kunnen brengen.

Zoals vaker gesteld zijn niet álle risico's echter even gemakkelijk identificeerbaar. De voornoemde risico's zouden bekend moeten zijn bij een onderneming, maar de mate waarin dit daadwerkelijk een risico vormt voor de onderneming is lastig te toetsen. Niet ter discussie staat dat hoe verder de toepassing van AI reikt, hoe meer risico's daaraan verbonden zijn. De exacte omvang van een risico ten aanzien van het gebruik is echter – bij gebrek aan onderzoek – niet geheel vast te stellen. Naar mijn mening zal er wel gepoogd moeten worden hier op basis van de specifieke toepassing in de kapitaalvennootschap een concrete inschatting van te maken.

De potentiële risico's van AI in de toekomst staan onomstotelijk ter discussie. Moeilijk in te schatten is, in welke mate de risico's met betrekking tot verregaande toepassingen van AI zich ontwikkelen. In dit kader is het voorzorgsbeginsel interessant, daar deze toeziet op de vraag welke onbekende risico's op de samenleving afkomen door technologische ontwikkeling en vooruitgang.¹⁹⁹ Hierbij van belang is of voorzichtigheid geen rem op innovatie met zich meebrengt en wat de optimale balans is tussen innoveren en risico lopen. Dit is wat bij het gebruik van AI een grote rol speelt. Innoveren met AI brengt immers risico's met zich mee, maar de vraag is of een bestuurder deze risico's mag nemen nu nog maar weinig onderzoek is gedaan naar de beheersing daarvan.

Volgens de Wetenschappelijke Raad voor het Regeringsbeleid moet er een toekomstgerichte omgang met risico's plaatsvinden, die uit gaat van het voorzorgsbeginsel. In dat kader zal de vennootschap actief onderzoek moeten doen naar toekomstige risico's. Dit brengt eveneens met zich mee dat aansprakelijkheid kan worden vastgesteld indien toekomstige risico's zich verwezenlijken, zelfs als deze op het moment van identificeren nog niet duidelijk zijn.²⁰⁰ Om die reden zal bij het gebruik van AI nu rekening moeten worden gehouden met de potentiële risico's in de toekomst, ook al zijn deze moeilijk definieerbaar. Voorzichtigheid is dan ook betracht wanneer verregaande toepassingen van AI in de onderneming geïmplementeerd worden wanneer de risico's nog onvoldoende identificeerbaar zijn.

¹⁹⁸ Gorter, *OR* 2016/73, afl. 9, par. 10.

¹⁹⁹ Claes, Janicijvic & Lengkeek 2012, p. 80.

²⁰⁰ Claes, Janicijvic & Lengkeek 2012, p. 80-81.

6.2.3.2. Prioriteit

Blijkens principe 11 moeten de risico's gerangschikt worden op basis van prioriteit, zodat de risicoreacties daarop afgestemd kunnen worden.²⁰¹ Hierbij valt de denken aan de kans dat een risico zich verwezenlijkt, maar ook de potentiële impact van de risico's is van belang. Zo zouden risico's met een grote verwezenlijgingskans en/of een grote potentiële impact op de onderneming meer prioriteit moeten krijgen dan risico's met een kleine verwezenlijgingskans en/of kleinere potentiële impact.

In dit geval is de verwezenlijgingskans van risico's afhankelijk van de toepassing die AI vindt in de onderneming. Met de toepassing wordt in dit kader zowel het doel ten aanzien waarvan AI wordt gebruikt bedoeld (bijvoorbeeld het nemen van beslissingen of om een specifieke taak uit te voeren), alsmede de vorm van AI die wordt toegepast (bijvoorbeeld *deep* of *narrow*). Per onderneming zal dus specifiek gekeken moeten worden naar de toepassing van AI die gebruikt wordt. Zo zal de kans op bijvoorbeeld schending van het grondrecht op gelijke behandeling een grotere verwezenlijgingskans hebben wanneer de AI toepassing wordt gebruikt om te beslissen of een krediet al dan niet wordt verstrekt. Daarentegen zal de kans op een terugroepactie vanwege een gebrekkig product waarschijnlijker zijn bij bijvoorbeeld zelfrijdende auto's of producten waarin AI verwerkt is.

Zoals in paragraaf 6.2.3.1 uiteengezet gaan met de risico's potentiële gevolgen gepaard. Zo is het mogelijk dat de onderneming te maken krijgt met schadevergoedingen wegens onrechtmatige daad, bijvoorbeeld door grondrechtenschendingen. Daarnaast kunnen bijvoorbeeld boetes worden opgelegd, producten worden teruggeroepen en kunnen er kostenposten komen die betrekking hebben op een cyberaanval of het voldoen aan andere specifieke wet- en regelgeving. Als laatste bestaat het gevaar voor reputatieschade, dat niet alleen ten koste zal gaan van de omzet van de onderneming en op die manier tot winstderving zal leiden, maar ook voor een directe afwaardering van de goodwill in de onderneming kan zorgen. De impact van reputatieschade is daarom in bijna alle gevallen erg groot, zeker wanneer het om grondrechtenschendingen gaat, maar ook in geval van non-compliance met wet- en regelgeving. Het vorenstaande alsmede hoofdstuk 5 brengen daarom met zich mee dat risico's ten aanzien van grondrechten, wet- en regelgeving en financiële verslaggeving prioriteit dienen te hebben. Risico's met betrekking tot bedrijfsdoelstellingen kunnen lagere prioriteit krijgen. Uit dit onderzoek blijkt echter dat deze twee soorten risico's niet zomaar van elkaar te scheiden zijn. In bijna alle gevallen is er sprake van een overlap tussen beide.

Deze prioriteitsindeling heeft niet louter betrekking op de gehele onderneming op bestuursniveau, maar kan voor verschillende bedrijfsonderdelen apart worden vastgesteld. Wanneer de potentiële effecten van de risico's de bedrijfsonderdelen overstijgen of in meerdere

²⁰¹ COSO Enterprise Risk Management 2017, principe 11.

bedrijfsonderdelen voor komen, wordt het een prioriteit voor de gehele onderneming.²⁰² Dit zal in ieder geval aan de orde zijn bij de risico's met betrekking tot wet- en regelgeving en financiële verslaglegging.

6.2.3.3 Risicobeoordeling

Blijkens principe 12 moet de organisatie de ernst van de risico's beoordelen.²⁰³ Deze risicobeoordeling kan zowel kwalitatief als kwantitatief worden uitgevoerd en wordt in een getal of geldbedrag uitgedrukt. De beoordeling van de risico's die met het gebruik van AI gepaard gaan, kan echter enigszins problematisch zijn. Er zijn aan sommige risico's weliswaar bedragen te koppelen, zoals een boete van de Autoriteit Persoonsgegevens en een terugroepactie van een bepaald product. Andere risico's, zoals reputatieschade en schadevergoedingen zijn moeilijker te beoordelen. De hoogte daarvan is immers vooraf niet altijd duidelijk. Daarnaast kan dit ook afhankelijk zijn van grootte van de groep derden die getroffen is.

Na de kwalitatieve en kwantitatieve beoordelingen worden de risico's ingedeeld in categorieën, aan de hand waarvan vervolgens bepaald kan worden welke risico's een significante bedreiging voor de onderneming vormen. Hieruit kan ook worden afgeleid óf en zo ja hoeveel er geïnvesteerd dient te worden in de beheersing van deze risico's. De kosten moeten namelijk in verhouding staan met het nut van de beheersingsmaatregel op de geïdentificeerde risico's.²⁰⁴ Daarentegen wordt in het algemeen wel aangenomen dat grote risico's altijd enige vorm van beheersing vereisen. Beheersing kan echter ook vereist zijn wanneer risico's weliswaar geen echte bedreiging voor de continuïteit van de onderneming vormen, maar waarbij beheersing daarvan wel (financiële) voordelen met zich meebrengt.²⁰⁵

Voor de risicobeoordeling – en de mate waarin risico's beheerst dienen te worden – kan onder andere aansluiting gevonden worden bij de ethische richtlijnen voor AI van de EC.²⁰⁶ Blijkens deze richtlijnen is voor het voldoen aan wet- en regelgeving, alsmede aan ethische normen, noodzakelijk dat de autonomie van de mens gewaarborgd blijft, dat fouten of inconsistenties in systemen worden opgespoord en aangepakt, dat burgers de volledige controle hebben over hun eigen gegevens, dat er sprake is van diversiteit, non-discriminatie en billijkheid, dat systemen het maatschappelijk- en ecologisch welzijn waarborgen en dat er sprake moet zijn van een verantwoordingsplicht. Mijns inziens zouden risico's die hier betrekking op hebben – ook al zouden deze geen reële bedreiging voor de continuïteit van de vennootschap vormen – beheerst moeten worden.

Voorst is nog van belang dat de beoordeling een doorlopend proces betreft, waarbij de

²⁰² Claes, Janicijvic & Lengkeek 2012, p. 126.

²⁰³ COSO *Enterprise Risk Management* 2017, principle 12.

²⁰⁴ Claes, Janicijvic & Lengkeek 2012, p. 125.

²⁰⁵ Claes, Janicijvic & Lengkeek 2012, p. 126.

²⁰⁶ *Ethische richtsnoeren voor betrouwbare KI* 2019, p. 16-17.

risicobeoordeling steeds moet worden bijgesteld naar aanleiding van interne- en externe ontwikkelingen. Op dit laatste zal in paragraaf 6.4.2.1 nader worden ingegaan.

6.2.3.4 Risicoreacties

Principe 13 is een belangrijke schakel in het risicobeheersings- en controlesysteem, gekeken naar de toepassing van AI in de onderneming. Volgens dit principe moet de onderneming risicoreacties identificeren en selecteren.²⁰⁷ In COSO wordt onder risicoreacties louter de beheersing van risico's verstaan.²⁰⁸ Hetgeen in dit raamwerk mijns inziens ontbreekt is de reactie op de verwezenlijking van risico's. Deze verwezenlijking hoeft blijkens hoofdstuk 5 geen falend risicomanagement op te leveren. Het gebrek aan reactie op verwezenlijking kan daarentegen wel een grond voor aansprakelijkheid vormen, namelijk in de vorm van een systeemfout.

Blijkens paragraaf 6.2.3.4 is beheersing vereist indien er sprake is van risico's die een reële bedreiging voor de onderneming vormen. Daarnaast zal beheersing vereist zijn indien dit minder kosten met zich mee brengt dan de kosten die voortvloeien uit de verwezenlijking van risico's. Ook de ethische richtlijnen van de EC spelen een rol in de beheersing van risico's. In dit kader kunnen in ieder geval de risico's met betrekking tot wet- en regelgeving, ethische normen en financiële verslaggeving worden geschaard onder grote risico's die beheerst dienen te worden. De potentiële schending van wet- en regelgeving komt voort uit een samenhang van de verschillende risico's omtrent AI. In ieder geval de onbetrouwbaarheid, interpreeteerbaarheid en transparantie kunnen daaraan ten grondslag liggen.

Een belangrijk onderscheid is hier te maken tussen het gebruik van AI als risicobeheersingsmaatregel, bijvoorbeeld in het kader van compliance met de Wft en de Wwft en het gebruik van AI op zichzelf. Desalniettemin brengen beide vormen risico's met zich mee, die mogelijk in het licht van het vorenstaande beheerst dienen te worden. Gezien het potentiële gebrek aan beheersingsmaatregelen verdient opmerking dat beheersing in mijn ogen minder vereist is indien AI als risicobeheersingsmaatregel wordt ingezet en de risico's die daarmee beheerst worden groter zijn dan de risico's die AI met zich mee brengt.

Concluderend uit een rapport van Deloitte zijn een aantal maatregelen echter – ondanks de beperkte beheersingsmaatregelen – noodzakelijk.²⁰⁹ Zo moeten de zogeheten 'black box' algoritmen regelmatig intern en extern herzien worden. Ook moeten besturingselementen ingesteld worden, zoals gegevensverzameling, voorbereiding, modelselectie, training, evaluatie en implementatie. Hiermee kan mogelijk de interne onbetrouwbaarheid van een systeem ondervangen worden. Voor de externe onbetrouwbaarheid zullen in ieder geval gepaste cybermaatregelen moeten worden getroffen.

Daarnaast is het noodzakelijk om – in het kader van transparantie – gebruik te maken van

²⁰⁷ COSO Enterprise Risk Management 2017, principle 13.

²⁰⁸ Strik 2010, p. 236.

²⁰⁹ Future of risk in the digital era, p. 7.

gestandaardiseerde berichtgeving om relevante belanghebbenden te informeren in het geval dat een beslissing wordt genomen met behulp van AI.

De interpreteerbaarheid kan verhoogd worden wanneer bewakingsprocessen worden ingesteld om de resultaten die afkomstig zijn uit de AI toepassing te volgen. Omdat *explainable AI* nog in de kinderschoenen staat, zal dit bewakingsproces vandaag de dag met name moeten bestaan uit menselijke controle, waarbij de AI toepassing slechts een specifieke taak verricht. In het geval van verregaande toepassingen zal in mijn ogen in ieder geval de menselijke factor aanwezig moeten blijven.

Periodieke onafhankelijke audits kunnen bijdragen aan de interpreteerbaarheid en betrouwbaarheid. Op basis van vastgestelde parameters kan de geldigheid van trainingsgegevens getest worden. Zo is het mogelijk om manipulaties in het systeem te ontdekken en om de prestaties van het AI systeem te verbeteren.

Ook zou een separate risicobeheersingsstrategie voor AI moeten worden gebruikt, waarbij specifiek aandacht wordt besteed aan het beleid, training, rollen en verantwoordelijkheden. Dit sluit aan bij al hetgeen in de principes van COSO naar voren komt. Naar mijn mening is dit dan ook geen specifieke beheersingsmaatregel. Mogelijkerwijs kan met trainingen en een duidelijke toedeling en controle van rollen en verantwoordelijkheden wel het risico op oneigenlijk gebruik (gedeeltelijk) ondervangen worden.

Hoewel er blijkens het bovenstaande een aantal mogelijkheden tot beheersing zijn, is de potentiële beheersing nog steeds behoorlijk beperkt. Wat daarom van belang is, is dat AI systemen gezien de stand van de wetenschap op dit moment (voorlopig) onder controle van het menselijk oog dienen te blijven. Het is daarbij eveneens van belang om te blijven communiceren met onderzoekers en innovators, om nieuwe werkwijzen en geavanceerde tools te verkrijgen die tot (betere) beheersing van de risico's leiden.

6.2.3.5 Portfolio-weergave risico's

Principe 14 schrijft voor dat een portfolio-weergave van risico's ontwikkeld en geëvalueerd moet worden.²¹⁰ Middels deze weergave kan het bestuur aantonen welke risico's geïdentificeerd, geanalyseerd en waar nodig en mogelijk beheerst zijn. Het vormt een belangrijk bewijsstuk van de besluitvormingsprocedure. Het bestuur moet blijkens paragraaf 4.2 namelijk verantwoording afleggen over de uitvoering, opzet, werking en eventuele tekortkomingen van het systeem.

²¹⁰ COSO Enterprise Risk Management 2017, principle 14.

6.2.4 Evaluatie en bijsturen

6.2.4.1 Identificatie en beoordeling veranderingen

Binnen de evaluatie en bijsturen component ziet principe 15 toe op de identificatie en beoordeling van veranderingen die wezenlijk van invloed kunnen zijn op de strategie en bedrijfsdoelstellingen.²¹¹ In het geval van AI zal dit principe een belangrijk element in het risicobeheersingssysteem vormen, omdat AI aan hevige ontwikkeling onderhevig is en het gebruik daarvan vaak ter discussie staat. Zo kan het gebruik van AI in de (nabije) toekomst onderworpen worden aan nadere wet- en regelgeving, waardoor toepassingen mogelijk anderszins aangepast moeten worden. Ook kan de razendsnelle ontwikkeling van AI het noodzakelijk maken om de systemen aan te passen of aan te vullen. Dit is in ieder geval nodig indien een nieuwe toepassing minder risico's met zich meebrengt, maar wel tot hetzelfde eindresultaat leidt. Het is in dat kader ongewenst om grotere risico's te nemen dan dat nodig is.

Daartegenover staat dat nieuwe toepassingen van AI vaak verder gaan dan de huidige toepassingen, wat vaak vele kansen maar ook juist grotere risico's met zich mee brengt. Verregaande toepassingen kunnen wel noodzakelijk zijn om te kunnen blijven concurreren, innoveren en daarmee de doelstellingen te behalen. De vraag of de strategie in dat geval aangepast mag worden, is een vraag die lastig te beantwoorden is. Mijns inziens zou de strategie aangepast kunnen worden, mits deze aanpassing niet in strijd is met de *risk appetite* van de onderneming en de risico's voldoende geïdentificeerd, geanalyseerd en beheerst kunnen worden.

Mogelijk anderszins vinden er tezamen met de ontwikkelingen van AI eveneens ontwikkelingen plaats in de beheersbaarheid van risico's die daar betrekking op hebben. In dat geval zal de onderneming deze mogelijkheden moeten evalueren en waar mogelijk implementeren, als dat leidt tot beheersing die beter aansluit bij de *risk appetite* van de onderneming.

Vast staat in ieder geval dat AI op vele fronten aan hevige ontwikkeling onderhevig is, waardoor evaluatie van deze ontwikkelingen uiterst noodzakelijk is. Het bijsturen dient plaats te vinden als uit de evaluatie blijkt dat dat nodig is, in het licht van het behalen van doelstellingen, maar ook om non-compliance te voorkomen en om de beheersingsmaatregelen beter te laten aansluiten bij de *risk appetite*.

6.2.4.2 Prestatiebeoordeling

Principe 16 ziet erop toe dat de prestaties van de onderneming worden beoordeeld, waarbij de risico's in overweging moeten worden genomen.²¹² Deze prestatiebeoordeling vindt allereerst plaats in het licht van de gestelde doelstellingen. Hierbij hoeft niet alleen te worden gekeken naar een geldelijk perspectief, ook kunnen de verantwoordelijkheden en activiteiten van de onderneming worden

²¹¹ COSO Enterprise Risk Management 2017, principle 15.

²¹² COSO Enterprise Risk Management 2017, principle 16.

getoetst aan de gestelde doelstellingen.²¹³ Ook moet beoordeeld worden of deze verantwoordelijkheden en activiteiten passen binnen de gedefinieerde *risk appetite* van de onderneming. Indien dit niet het geval is, zal actie dienen te worden ondernomen ten aanzien van de doelstellingen, de *risk appetite* of de prestaties van de onderneming. Van groot belang is namelijk dat deze in verhouding tot elkaar zijn.

6.2.4.3 Verbetering risicobeheersing

Principe 17 is mijns inziens vanzelfsprekend. Dit principe schrijft namelijk voor dat er gestreefd worden naar verbetering van de risicobeheersing in de onderneming.²¹⁴ Daartoe zal de werking van het systeem frequent gemonitord en geëvalueerd moeten worden, alvorens aanpassingen door te voeren die tot verbetering leiden. Het nalaten hiervan zal dan ook tot de systeem- en werkingsfouten kunnen leiden die in paragraaf 5.4.2.2 en paragraaf 5.4.2.3 uiteen zijn gezet.

6.2.5 Informatie, communicatie en rapportage

De laatste component van het COSO raamwerk kent drie principes die toezien op de informatievoorziening, communicatie en rapportage. Zo moet er gebruik worden gemaakt van informatie- en technologiesystemen om het risicomanagement te ondersteunen.²¹⁵ Daarnaast moeten daarvoor eveneens communicatiekanalen worden gebruikt.²¹⁶ Tevens moet er op meerdere niveaus binnen de onderneming worden gerapporteerd over de risico's, de heersende cultuur en prestaties.²¹⁷ Omdat dit voor het gebruik van AI niet afwijkt ten opzichte van 'normaal' risicobeheer, zal hier niet verder op in worden gegaan.

6.3 Systeem- werkings- en beoordelingsfouten

Blijkens de conclusie van hoofdstuk 5, vormen beoordelingsfouten het grootste risico op bestuurdersaansprakelijkheid voor falend risicomanagement inzake AI. Daarnaast kunnen systeem- en werkingsfouten voorkomen. De invulling van het COSO raamwerk in paragraaf 6.2 illustreert hoe groot het risico op beoordelingsfouten is, daar bestuurders op vele verschillende fronten, zoals de strategie, doelstellingen, *risk appetite* en de risico identificatie en -beheersing, beoordelingen dienen te maken. Voorts is gezien dat er ten aanzien van het gebruik van AI niet één norm vast te stellen is die moet worden gevolgd. De beoordeling is namelijk voor iedere onderneming verschillend en afhankelijk van tal van factoren. Van belang is dat de beoordeling past binnen de schakels van het risicobeheersings- en controlesysteem en dat er sprake is van onderlinge samenhang. Zo moet de *risk appetite* van de onderneming in lijn zijn met de context van de onderneming en de strategie en doelstellingen moeten

²¹³ Strik 2010, p. 235.

²¹⁴ COSO Enterprise Risk Management 2017, principle 17.

²¹⁵ COSO Enterprise Risk Management 2017, principle 18.

²¹⁶ COSO Enterprise Risk Management 2017, principle 19.

²¹⁷ COSO Enterprise Risk Management 2017, principle 20.

passen binnen de *risk appetite*. Daarnaast moet een goede balans worden gevonden tussen de kansen die AI met zich meebrengt en de risico's die daarmee gepaard gaan.

Een beoordelingsfout kan schuilen in het vaststellen van de *risk appetite*, indien er gekozen wordt voor een te risicovol beleid ten aanzien van de context van de vennootschap. Ook kan een beoordelingsfout worden gemaakt wanneer de doelstellingen veel te hoog worden vastgelegd, waardoor risiconemend gedrag – dat niet past binnen de *risk appetite* – in de hand wordt gewerkt. Tevens kan een beoordelingsfout schuilen in het opstellen van de strategie, waarin de mate waarin AI toepassing zal vinden in de onderneming wordt vervat. Deze toepassing moet immers in lijn zijn met de potentiële risico's en de mogelijke verplichte en voor handen zijnde beheersing daarvan.

Voorts kunnen in de processen van risico identificatie, beoordeling en beheersing eveneens beoordelingsfouten worden gemaakt. Zo kan de risico identificatie onvolledig zijn, waarbij bijvoorbeeld toekomstige risico's onvoldoende naar voren komen. Deze zijn echter wel relevant voor de aansprakelijkheidsvraag. Ook zou foutieve risicobeoordeling kunnen leiden tot gebrekkige beheersing. Gezien de redelijk beperkte mogelijkheden tot beheersing zal mijns inziens door de onderneming een keuze moeten worden gemaakt tussen de mate waarin AI toegepast wordt in de onderneming en de mogelijkheden tot beheersing. De onderneming is namelijk verplicht tot het beheersen van bepaalde risico's. Een compleet verkeerde inschatting daaromtrent zal dan in mijn ogen ook zonder meer tot onbehoorlijke taakvervulling kunnen leiden, omdat in dat geval kan worden gesteld dat risicobeheersing met betrekking tot wet- en regelgeving onvoldoende beheerst wordt en daar gezien de beperkte beleidsvrijheid van het bestuur strengere eisen aan worden gesteld.

Zoals eerder gesteld ontbreken de feitelijke risico reacties in het beheersingssysteem van COSO. Wanneer een risico zich verwezenlijkt, is het de taak van het bestuur om te bepalen welke sanctie daarop volgt.²¹⁸ Wanneer door het bestuur louter het COSO raamwerk wordt toegepast en derhalve geen feitelijke risicoreacties geeft, zal het bestuur mogelijk aansprakelijk kunnen worden gesteld, omdat er in dat geval sprake is van een systeemfout. Het systeem biedt dan immers onvoldoende beheersing ten aanzien van de verwezenlijking van risico's.

Ook werkingsfouten kunnen leiden tot aansprakelijkheid. In het licht van hetgeen in dit hoofdstuk is uitgewerkt kan dan bijvoorbeeld gedacht worden aan het onvoldoende creëren en uitdragen van de risicocultuur, waardoor besluitvorming niet volgens die cultuur (en daarmee de *risk appetite* van de onderneming) plaatsvindt. Het gebrek aan training en opleiding kan er eveneens voor zorgen dat maatregelen niet (juist) worden toegepast.

²¹⁸ Strik 2010, p. 236.

6.4 Conclusie

Kan een risicobeheersingssysteem zoals COSO 2017 bestuurdersaansprakelijkheid voor falend risicomanagement inzake AI voorkomen?

Het COSO 2017 raamwerk bevat 5 componenten met elk een aantal principes. De eerste component governance en cultuur schrijft voor dat het bestuur verantwoordelijk is voor de strategie van de onderneming. In het kader van AI zal het bestuur dus moeten bepalen in welke mate AI toepassing zal vinden in de onderneming, om op die manier de bedrijfsdoelstellingen te bereiken. Dit moet in lijn zijn met de *risk appetite* en de doelstellingen van de onderneming. Daarnaast draagt het bestuur de verantwoordelijkheid over het neerzetten van een operationele structuur, welke aangeeft welke taken, bevoegdheden en verantwoordelijkheden de werknemers hebben. Ook is het bestuur verantwoordelijk voor de (risico) cultuur in de onderneming, welke aan moet sluiten bij de strategie en de *risk appetite* van de onderneming. De cultuur moet als rode draad door de besluitvormingsprocessen in de onderneming lopen. Daarbij zal het bestuur commitment aan de kernwaarden van de onderneming dienen te tonen. Tevens moet er gezorgd worden voor het aantrekken en behouden van menselijk kapitaal, wat in het geval van AI met zich meebrengt dat specialisten aangetrokken en behouden moeten worden. Ook andere werknemers dienen training en begeleiding te krijgen.

De tweede component omvat de strategie- en doelstellingen. Hierin wordt voorgeschreven dat de context van de onderneming moet worden bepaald. Deze context is van groot belang voor de werking van het systeem, omdat onder andere aan de hand daarvan een passende *risk appetite* gekozen kan worden. Er moet hierbij zowel gekeken worden naar de interne- als externe context van de onderneming. Er zal dus goed naar de sector en het eventuele publieke belang gekeken moeten worden. Op basis van de context, de risicohouding, de *risk tolerance* en de *desired level of risk* moet de *risk appetite* worden geformuleerd. Dit vormt in feite een weergave van de cultuur ten aanzien risico's. Van groot belang is dat deze past bij de onderneming, de strategie en de doelstellingen. Tevens moeten alternatieve strategieën in kaart worden gebracht, waarna geëvalueerd kan worden welke strategie het beste past bij de *risk appetite* en doelstellingen. Voorts moeten bedrijfsdoelstellingen worden geformuleerd die aansluiten bij het bovenstaande.

De derde component betreft prestatiemeting. Allereerst moeten risico's worden geïdentificeerd, waarbij ten aanzien van AI gekeken moet worden naar alle risico's, zowel huidige als toekomstige. Door het bestuur moet dus eveneens rekening worden gehouden met risico's die bij verregaande toepassingen van AI om de hoek kunnen komen kijken. Zorgvuldigheid is in dit kader dan ook gewenst. De geïdentificeerde risico's moeten vervolgens op basis van prioriteit worden ingedeeld. Dit kan worden bepaald aan de hand van de kans op verwezenlijking van de risico's en de potentiële impact daarvan. Daarnaast dienen risico's met betrekking tot wet- en regelgeving en financiële verslaggeving altijd hoge prioriteit te krijgen. Middels risicobeoordeling kan bovenstaande indeling

worden gemaakt. Risico's worden ingedeeld in categorieën, waarbij de hoogste categorieën altijd enige vorm van beheersing vereisen. De strategie die bepaalt in welke mate AI toepassing vindt in de onderneming, moet zo worden opgesteld dat er rekening wordt gehouden met de mogelijkheid tot beheersing van de daaruit voortvloeiende risico's. De beheersingsmaatregelen die getroffen kunnen worden zijn tot op heden redelijk beperkt, maar voor de mate waarin AI reeds toepassing vindt zouden deze toereikend kunnen zijn, omdat voor ieder risico in ieder geval een mogelijkheid tot beheersing bestaat. Van belang voor de beheersing blijft wel dat een menselijke component voorlopig gegarandeerd blijft, omdat dat een van de weinige mogelijkheden tot controle biedt. Als laatste in deze component zal het bestuur een portfolio weergave van de risico's moeten maken, dat als bewijsstuk kan dienen bij de verantwoording over de risicobeheersingssystemen.

De vierde component is gericht op evaluatie en bijsturen. Wezenlijke veranderingen die van invloed kunnen zijn op de identificatie en beoordeling van risico's moeten geëvalueerd worden. In het kader van AI is dit een ontzettend belangrijk element, daar AI voortdurend aan hevige ontwikkeling onderhevig is. Tevens moet de werking van het systeem beoordeeld en waar nodig aangepast worden, zodat deze steeds meer toeziet op de adequate beheersing van risico's. Er moet dan ook altijd gestreefd worden naar verbetering van het systeem. De vijfde component is inhoudelijk niet uitgewerkt, omdat deze voor het gebruik van AI niet verschilt ten opzichte van andere risico's.

Het risico op aansprakelijkheid voor beoordelingsfouten is het grootste. Zo is het formuleren van de *risk appetite* een belangrijke schakel in het geheel. Ook andere elementen, zoals de cultuur, strategie, doelstellingen en beheersingsmaatregelen vallen of staan met een juiste beoordeling. Zowel de beoordeling betreffende de onderlinge afstemming van de elementen als de beoordeling van de elementen op zichzelf. Onzorgvuldige beoordelingen leiden tot een systeem dat niet goed op elkaar afgestemd is en risico's onvoldoende beheerst. Werkingsfouten kunnen zich voordoen wanneer de juiste risico cultuur onvoldoende heerst of wanneer onvoldoende menselijk kapitaal in de vennootschap aanwezig is. Hieruit blijkt dat het niet mogelijk is om te definiëren wat een onderneming ten aanzien van het gebruik van AI exact moet doen, omdat een en ander van ontzettend veel factoren afhankelijk is. Wel is duidelijk dat het gehele systeem valt of staat met de beoordeling van de elementen. Wanneer het systeem goed gevolgd wordt en risicobeoordelingen precies volgens de principes worden gedaan, kan een risicobeheersingssysteem als COSO 2017 zonder meer aansprakelijkheid op grond van beoordelingsfouten veelal voorkomen. Wel is dan van belang dat er een samenspel tussen alle elementen bestaat en dat deze niet afzonderlijk worden behandeld. Dit geldt eveneens ten aanzien van werkingsfouten. Ten aanzien van systeemfouten kan niet hetzelfde gesteld worden. In dat kader ontbreekt een principe betreffende risicoreacties, in het geval dat risico's zich daadwerkelijk verwezenlijken. Hierdoor ligt aansprakelijkheid voor een systeemfout voor de hand wanneer louter het COSO-raamwerk gevolgd wordt.

7. CONCLUSIE

Definitie en werking AI

Om een antwoord te kunnen geven op de hoofdvraag, is eerst onderzocht wat AI is en hoe het werkt. Daaruit is voortgekomen dat AI gedefinieerd kan worden als een reeks methoden en softwaretechnieken (algoritmen en datastructuren) waarmee informatiesystemen kunnen worden gebouwd die mentale taken aankunnen. Onder mentale taken wordt in dit kader verstaan: taken waarvoor *enige* intelligentie vereist is. De informatiesystemen die worden gebouwd bestaan in de meeste gevallen uit een probleem- en kennisrepresentatie, een inferentiemachine en een leeralgoritme. Voor de voeding van het systeem kunnen bestaande kennis (van experts) en grote hoeveelheden data worden gebruikt. In de meeste gevallen vormt een combinatie van beide de input voor een systeem. Zo'n systeem kan *weak* of *strong*, ofwel *narrow* of *deep* zijn. Deze classificatie geeft weer hoe verregaand een systeem is. Wanneer een systeem als *deep* gekwalificeerd is, kan een algoritme middels patroonherkenning zelf (ingewikkelde) problemen oplossen.

Toepassing, risico's en kansen AI

Voorts is onderzocht hoe AI vandaag de dag binnen kapitaalvennootschappen wordt gebruikt en welke risico's en kansen daarmee gepaard gaan. Hiermee is vast te stellen wat momenteel als normale toepassing gezien kan worden, wat het een en ander met zich mee brengt ten aanzien van aansprakelijkheid. Hieruit is gebleken dat AI reeds in vele sectoren op verschillende wijzen wordt toegepast, waarbij het doorgaans om een vorm van *deep learning* gaat. Deze methode wordt in de praktijk gebruikt om te anticiperen op gebeurtenissen en uitkomsten, om taken uit te voeren zonder menselijke tussenkomst, om patronen en trends te identificeren en te begrijpen, om te personaliseren en om oplossingen ten aanzien van problemen voor te stellen. Zo worden bijvoorbeeld leningen toegekend of geweigerd met behulp van AI en worden chatbots ingezet om mensen van dienst te kunnen zijn. Bijna in alle gevallen wordt AI louter ingezet als hulpmiddel ten aanzien van een specifieke taak, waarbij de mens als controlerende factor fungeert. Het is echter wel waarschijnlijk dat dit in de toekomst niet altijd het geval meer zal zijn. Bij deze toepassingen van AI komen tal van risico's kijken, zoals: oneigenlijk gebruik, de interne- en externe onbetrouwbaarheid, het gebrek aan interpretatie, transparantie en verantwoordelijkheid en het risico op de schending van wet- en regelgeving en ethische principes. De mate waarin AI wordt toegepast binnen de onderneming speelt een belangrijke rol bij de grootte van de risico's. Zo zal een AI systeem dat slechts ter invulling van een specifieke taak met controle van de mens wordt gebruikt, minder risico's met zich meebrengen dan een verregaande toepassing van AI. Daarentegen biedt AI ook grote kansen en mogelijkheden. Het is bevorderlijk voor de innovatie en concurrentiepositie van ondernemingen en het brengt grote kostenbesparingen met zich

mee, welke ten gunste kunnen komen aan het bedrijfsresultaat. Daarnaast kan het in positieve zin bijdragen aan de beheersing van risico's die met andere bedrijfsactiviteiten gepaard gaan, doordat het meer 'ziet' dan de mens.

Adequate Corporate Governance

Verder is gekeken wat onder adequate Corporate Governance kan worden verstaan, omdat dit van belang is voor de vraag wanneer bestuurders aansprakelijk kunnen zijn. Al eerder is gebleken dat Corporate Governance een veelomvattend begrip is, dat in ieder geval over het functioneren van vennootschappelijke organen ten aanzien van hun taken en bevoegdheden gaat. Hieraan wordt invulling gegeven door wet- en regelgeving, alsmede de NCGC. Op grond van art. 2:129 lid 1 BW en art. 2:239 lid 1 BW heeft het bestuur een bestuursplicht, welke blijkens art. 2:9 BW behoorlijk moet worden uitgevoerd. Risicomanagement behoort tot een van de taken die vallen onder deze plicht. Voor het bepalen van het begrip behoorlijk bestuur, kan worden aangesloten bij de bepalingen in de NCGC. Deze geldt ten aanzien van beursvennootschappen, maar middels de reflexwerking ook voor sommige niet beursgenoteerde vennootschappen. In welke mate dit het geval is hangt af van de omvang van de onderneming, omdat het waarschijnlijker is dat zeer grote ondernemingen onder het bereik van de NCGC vallen. Echter kan ook van kleine ondernemingen worden verwacht dat zij, afhankelijk van aard, omvang, complexiteit en levensfase van de onderneming alsmede de gebruiken binnen de branche en de aard van de gelopen risico's, op enige wijze aan risicobeheersing doen. De basis daarvoor kan gevonden worden in de NCGC. Schending van de principes van de NCGC leidt niet per definitie tot slechte governance of onbehoorlijk bestuur, het kan echter wel invulling geven aan de relatief open norm van art. 2:9 BW. Blijkens de NCGC moet het bestuur zorg dragen voor het vaststellen van de risicobereidheid, alvorens een systeem te ontwerpen, implementeren, controleren en monitoren. Ook moet in het bestuursverslag verantwoording afgelegd worden over de uitvoering, opzet, werking en eventuele tekortkomingen van het systeem. Gebleken is, dat het ontwerpen en beheren van zo'n systeem in het geval van AI tot moeilijkheden kan leiden, omdat identificatie en beheersing van de daaruit voortvloeiende risico's een uitdaging blijkt te zijn. De mate waarin AI wordt gebruikt speelt hierbij een belangrijke rol, eerder geconcludeerd is immers dat verregaande toepassingen meer risico's met zich mee brengen. Naast de beginselen uit de NCGC moet eveneens gekeken worden naar compliance met wet- en regelgeving. Slechts één verordening is vandaag de dag van toepassing, te weten de AVG. Het risico op schending daarvan is echter, gekeken naar de risico's gebrek aan interpreteerbaarheid, transparantie en onbetrouwbaarheid, zonder meer aanwezig. De potentiële schending van grondrechten speelt daarbij ook een grote rol. In dit kader zijn ook de ethische richtlijnen voor betrouwbare AI van belang, omdat hierbij aan kan worden gesloten bij de vraag op welke wijze bestuurders met de risico's om zouden moeten gaan. Uiteindelijk kan gesteld worden dat het bestuur in het licht van adequate Corporate Governance zorg moet dragen voor een risicobeheersings- en

controlesysteem dat (in het geval van kleine ondernemingen gedeeltelijk) aansluit bij de eisen in de NCGC, waarbij in ieder geval de risico's die betrekking hebben op de AVG en grondrechten dienen te worden beheerst. Daarnaast dienen de andere risico's te worden geïdentificeerd, geanalyseerd en eventueel beheerst, voor zover dat op dat moment mogelijk is. Hierbij kan wel worden aangesloten bij de ethische richtsnoeren van de EC.

Aansprakelijkheid voor falend risicomanagement

Als vierde is onderzocht op welke wijze bestuurders aansprakelijk kunnen worden gesteld voor falend risicomanagement. Daaruit is voort gekomen dat bestuurders op grond van art. 2:9 BW intern en op grond van art. 6:162 BW extern aansprakelijk gesteld kunnen worden. Dit is het geval wanneer zij *onbehoorlijk hebben bestuurd* en hen daartoe een *ernstig verwijt* kan worden gemaakt. Het ernstig verwijt criterium wordt ingevuld aan de hand van de *maatman bestuurder*, waarbij de omstandigheden van het geval van groot belang zijn. Later is in de jurisprudentie bepaald dat dit criterium eveneens geldt voor bestuurdersaansprakelijkheid op grond van art. 6:162 BW. Voor het verdere onderzoek is besloten de normen *onbehoorlijk bestuur* en *ernstig verwijt* middels een geïntegreerde aanpak te gebruiken. Voorts is uit het onderzoek gebleken dat bestuurdersaansprakelijkheid niet te snel mag worden aangenomen, omdat het bestuur ten aanzien van de bestuurstaak een zekere beleidsvrijheid heeft, en het gevaar van *hindsight bias* op de loer ligt. Het zou in dit kader wel onwenselijk zijn dat bestuurders AI op verregaande wijze kunnen implementeren, doordat het bestuur niet bekend was met de gevolgen daarvan. Mijns inziens zou dan ook van een bestuurder mogen worden verwacht dat hij bekend is met een (deel) van de risico's betreffende AI, ook wanneer deze in zekere zin onvoorspelbaar zijn. Daarentegen zou het gebrek aan identificatie- en beheersingsmaatregelen het gebruik van AI niet geheel in de weg mogen staan, doordat het naast de risico's ook grote kansen biedt. De belangrijkste vraag die rijst is waar de grens ligt bij het begrip *maatman bestuurder*, wat wist of behoorde de bestuurder te weten? Een deel van het antwoord hierop kan gevonden worden in het handelen in strijd met wet- en regelgeving. Ten aanzien van die risico's zal het bestuur dan ook te allen tijde moeten beheersen. Daarbij is van belang dat het verwezenlijken van risico's niet per definitie met zich mee brengt dat het risicomanagementsysteem gefaald heeft. Daarvan is alleen sprake in het geval van een risicobeheersingsfout. De afwezigheid van een risicobeheersings- en controlesysteem levert in grotere ondernemingen zonder meer onbehoorlijke taakvervulling op. Systeem- en werkingsfouten leveren – op basis van de omstandigheden van het geval – mogelijkwerwijs een onbehoorlijke taakvervulling op. Datzelfde geldt voor het gebrek aan transparantie aan de markt over risico's en risicobeheersing. In het onderzoek is verder ingegaan op beoordelingsfouten omdat deze in het geval van AI waarschijnlijk het meeste voorkomen. Beoordelingsfouten kunnen ten aanzien van tal van elementen van een systeem worden gemaakt. Zo zal de bestuurder een goede afweging moeten maken tussen innovatie, kostenbesparing en beheersingsmogelijkheden binnen de onderneming middels het toepassen van AI

enerzijds en de risico's die daarbij komen kijken anderzijds. Van belang is dat een onderscheid wordt gemaakt tussen risico's met betrekking tot wet- en regelgeving en financiële verslaggeving en risico's betreffende operationele- en strategische doelstellingen. Het bestuur heeft in dat eerste geval minder beleidsvrijheid. Hierbij valt wel aan te merken dat het bestuur kansen kan en mag benutten, maar dat de uiteindelijke beslissing onder toezicht van de mens zal moeten worden gemaakt. Daarnaast moet – voor de omstandigheden van het geval – gekeken worden naar de sector waarin de kapitaalvennootschap zich bevindt en wat de bestuurder wist en behoorde te weten, gelet op het *maatman bestuurder* criterium. Hieruit is dan ook af te leiden dat bestuurdersaansprakelijkheid voor falend risicomanagement inzake AI zeer zeker mogelijk is, maar dat daarbij dient te worden gekeken naar de soort risicobeheersingsfout en naar alle omstandigheden van het geval.

Inrichting risicobeheersings- en controlesysteem

Nu onomstotelijk vaststaat dat bestuurders – onder bepaalde omstandigheden – aansprakelijk kunnen worden gesteld voor falend risicomanagement inzake AI, is onderzocht of het COSO-raamwerk deze aansprakelijkheid kan voorkomen. Het is in feite een weergave van hetgeen als behoorlijk bestuur inzake AI zou kunnen worden gezien. Daarvoor zijn de vijf componenten, met elk een aantal principes, van COSO 2017 uitgewerkt. De eerste component betreft governance en cultuur, waarin is bepaald dat het bestuur verantwoordelijk is voor de strategie, het neerzetten van de operationele structuur, de (risico)cultuur van de onderneming, commitment aan kernwaarden en het menselijk kapitaal. In de tweede component strategie en doelstellingen, is bepaald dat de context van de onderneming moet worden bepaald. Onder andere aan de hand daarvan moet de *risk appetite* worden opgesteld. Tevens moeten alternatieve strategieën en bedrijfsdoelstellingen worden geformuleerd. De derde component, prestatiemeting, schrijft voor dat risico's moeten worden geïdentificeerd, beoordeeld, beheerst en weergegeven in een portfolio. Ook moeten de risico's op prioriteit worden gerangschikt. De vierde component is gericht op evaluatie en bijsturen. Ingevolge deze component moeten wezenlijke veranderingen geëvalueerd worden, moet de werking van het systeem beoordeeld- en aangepast worden en moet gestreefd worden naar verbetering van het beheersingssysteem. De vijfde component is – gekeken naar de algemene aard daarvan – niet verder uitgewerkt.

Zoals uit het onderzoek in hoofdstuk 5 is gebleken, is de kans op het maken van beoordelingsfouten het grootste. Van belang bij de invulling van de componenten is dat het een samenspel betreft tussen de verschillende componenten. Een beoordelingsfout kan in dat geval gemakkelijk schuilen in de invulling van een bepaald principe, maar in het gebrek aan overeenstemming tussen de principes. Onzorgvuldige beoordelingen leiden in dat geval tot een systeem dat de risico's onvoldoende beheerst. Dit zou tot aansprakelijkheid van de bestuurders kunnen leiden. Werkingsfouten kunnen eveneens voorkomen, bijvoorbeeld doordat een principe niet goed wordt uitgevoerd. Systeemfouten kunnen voor de hand liggen, omdat het COSO-raamwerk niet toeziet op de

risicoreacties, welke ingevolge adequate corporate governance wel vereist zijn.

Uit dit gedeelte van het onderzoek blijkt dat het onmogelijk is om uiteen te zetten wat wél behoorlijk bestuur is en wat niet. Dit is namelijk van vele factoren afhankelijk, iedere vennootschap heeft immers zijn eigen omstandigheden. Er is wel duidelijk naar voren gekomen dat een systeem valt of staat met de beoordeling van de elementen. Hierbij moeten de elementen in ieder geval in overeenstemming zijn met elkaar. Op die manier zal het grootste risico ondervangen kunnen worden.

Kan het bestuur van een kapitaalvennootschap aansprakelijk worden gesteld wegens onvoldoende risicomanagement inzake artificiële intelligentie?

Ja, het bestuur van een kapitaalvennootschap kan aansprakelijk worden gesteld wegens onvoldoende risicomanagement inzake artificiële intelligentie, op grond van art. 2:9 BW en art. 6:162 BW. Beoordelingsfouten zullen de voornaamste grond van aansprakelijkheid vormen. Dit zal met name aangenomen worden wanneer het risicobeheersings- en controle systeem onvoldoende op elkaar is afgestemd, of wanneer een grove beoordelingsfout is gemaakt ten aanzien van een specifiek onderdeel in het systeem. Alle omstandigheden van het geval zijn van belang bij de beoordeling van aansprakelijkheid, alsmede voor de invulling van het risicobeheersings- en controlesysteem.

BIBLIOGRAFIE

Boeken

Asser/Maeijer & Kroeze 2-I* 2015

M.J. Kroeze (m.m.v. H. Beckman, M.A. Verburgh), *Mr. C. Assers Handleiding tot de beoefening van het Nederlands Burgerlijk Recht. 2. Rechtspersoonrecht. Deel I*. De Rechtspersoon*, Deventer: Kluwer 2015.

Asser/Maeijer, Van Solinge & Nieuwe Weme 2-II* 2009

G. van Solinge & M.P. Nieuwe Weme, *Mr. C. Assers Handleiding tot de beoefening van het Nederlands burgerlijk recht. 2. Rechtspersonenrecht. Deel II*. NV en BV. Oprichting, vermogen en aandelen*, Deventer: Kluwer 2013.

Assink 2007

B.F. Assink, *Rechterlijke toetsing van bestuurlijk gedrag binnen het vennootschapsrecht van Nederland en Delaware* (diss.; Serie Instituut voor Ondernemingsrecht, nr. 59), Deventer: Kluwer 2007.

Assink e.a. 2011

B.F. Assink e.a., *Evolutie in het bestuurdersaansprakelijkheidsrecht* (uitgave vanwege het Instituut voor Ondernemingsrecht, nr. 76), Deventer: Kluwer 2011.

Assink & Slagter 2013

B.F. Assink & W.J. Slagter, *Compendium Ondernemingsrecht*, Deventer: Kluwer 2013.

Borrius 2003

Y. Borrius, 'Behoorlijk bestuur; één gedragsnorm?', in: G. van Solinge en M. Holtzer, *Geschriften vanwege de Vereniging Corporate Litigation 2002-2003*, Deventer: Kluwer 2003.

Claes, Janicijvic & Lengkeek 2012

P. Claes, S. Janicijvic, R. Lengkeek, *Risicomanagement*, Deventer: Kluwer 2012.

Duursma 2017

J. Duursma, *De digitale butler. Kansen en bedreigingen van kunstmatige intelligentie*, Zaltbommel: Uitgeverij Haystack 2017.

Emaus 2013

J.M. Emaus, *Handhaving van EVRM-rechten via het aansprakelijkheidsrecht*, (diss. Utrecht), Den Haag: Boom Juridische Uitgevers 2013.

Harbers 2018

M. Harbers, *Verstand erbij. Verantwoord ontwerp van toepassingen met kunstmatige intelligentie*, Rotterdam: Hogeschool Rotterdam Uitgeverij.

Huizink 2009

J.B. Huizink, *Ondernemingsrecht. Cases in control*, Kluwer: Deventer 2009.

Huizink, in: GS Rechtspersonen, art. 2:64 BW, aant. 4.7

J.B. Huizink, 'Corporate Governance', in: J.B. Huizink (red.), *Groene Serie Rechtspersonen*, Deventer: Kluwer, (online, bijgewerkt 26 november 2018).

Kroeze 2004

M.J. Kroeze, *Afgeleide schade en afgeleide actie*, Deventer: Kluwer 2004.

Kroeze, Timmerman & Wezeman 2007

M.J. Kroeze, L. Timmerman & J.B. Wezeman, *De kern van het ondernemingsrecht*, Deventer: Kluwer 2007.

Nieuwenhuis 2003

M.A. Nieuwenhuis, *The Art of Management. Deel 1 Strategie en Structuur*, Apeldoorn: Art of Management.

O'Reilly 2018

T. O'Reilly, *De nieuwe economie*, Uithoorn: Karakter Uitgevers 2018.

Poggio 2016

T. Poggio, 'Een nieuwe Turingtest', in: *Machines die denken*, Amsterdam: Maven Publishing 2016.

Pitlo/Raaijmakers 2017

M.J.G.C. Raaijmakers, *Ondernemingsrecht* (Het Nederlands Burgerlijk recht: Pitlo deel 2), Deventer: Kluwer 2017.

Raaijmakers 2016

M.J.G.C. Raaijmakers, 'Hoe juridisch is corporate governance?', in: *C.D.J. Bulten e.a. (red.), Marius geannoteerd* (Serie vanwege het Van der Heijden Instituut, deel 133), Deventer: Kluwer 2016.

Roest, in: T&C Burgerlijk Wetboek, art. 2:9 BW

J. Roest, 'commentaar op artikel 2:9 Burgerlijk wetboek', in: *Tekst & Commentaar Burgerlijk Wetboek*, Deventer: Kluwer 2017, (online, bijgewerkt 1 juli 2019).

Schilfgaarde, van 2013

P. van Schilfgaarde, *Van de BV en de NV*, Deventer: Kluwer 2013.

Schilfgaarde, van, e.a. 2017

P. van Schilfgaarde, J. Winter, J.B. Wezeman & J. Schoonbrood, *Van de BV en de NV*, Deventer: Kluwer 2017.

Sejnowski 2019

T.J. Sejnowski, *Kunstmatige intelligentie. De revolutie van neurale netwerken en deep learning*, Utrecht: Veen Media 2019.

Soerjatin 2012

E. Soerjatin, 'Rechterlijke toetsing van corporate governance', In: *M. Lückerath-Rovers, B. Bier, H. van Ees en M. Kapitein (eds.), Jaarboek Corporate Governance 2012-2013*, Deventer: Kluwer 2012.

Stolp & Nijs Bik, de 2015

Stolp & de Nijs Bik, 'De positie van bestuurders en commissarissen ter zake van risicomanagement', in: *A. Tervoort, H. Bruisten & S. Drion, Be (a)ware. Legal risk management* (Bundel van het Nederlands Genootschap van Bedrijfsjuristen 1930-2015), Den Haag: SDU 2015.

Strik 2009

D.A.M.H.W. Strik, *Aansprakelijkheid voor een falend risicomanagement. Preadvies van de Vereniging Handelsrecht*, Deventer: Kluwer 2009.

Strik 2010

D.A.M.H.W. Strik, *Grondslagen bestuurdersaansprakelijkheid. Een maatpak voor de Board Room* (diss. Rotterdam; Instituut voor Ondernemingsrecht, nr. 73), Deventer: Kluwer 2010.

Tegmark 2017

M. Tegmark, *Life 3.0. Mens zijn in het tijdperk van kunstmatige intelligentie*, Amsterdam: Maven Publishing 2017.

Vetzo, Gerards & Nehmelman 2018

M. Vetzo, J. Gerards & R. Nehmelman, *Algoritmes en grondrechten*, Den Haag: Boom Juridische Uitgevers 2018.

Waals, van der 2017

S.E. van der Waals, *De optimale rechtsvorm voor de samenwerking in het beroep. Confectie of maatpak?* (diss. Utrecht; Serie Van der Heijden Instituut nr. 139) Deventer: Kluwer 2017.

Westenbroek 2017

W.A. Westenbroek, *Bestuurdersaansprakelijkheid in theorie*, (diss. Rotterdam; Instituut voor Ondernemingsrecht nr. 108), Deventer: Kluwer 2017.

Wezeman 1998

J.B. Wezeman, *Aansprakelijkheid van bestuurders*, (diss. Groningen; Uitgave vanwege het Instituut voor Ondernemingsrecht nr. 29) Deventer: Kluwer 1998.

Tijdschriften

Bier, *OR* 2005/188, afl. 16

B. Bier, 'Het risico van de risicobeheersing- en interne controle systemen: de 'in control' verklaring van de Code Tabaksblad', *OR* 2005/188, afl. 16.

Dirican, *PSBS* 2015, vol. 195, p. 564-573

C. Dirican, 'The Impact of Robotics, Artificial Intelligence On Business and Economics', *PSBS* 2015, vol. 195, p. 564-573.

Gorter, *OR* 2016/73, afl. 9

C. Gorter, 'Het complexe samenspel bij risicomanagement', *OR* 2016/73, afl. 9.

Hijink, *OR* 2019/3, afl. 1

J.B.S. Hijink, 'Robots in de boardroom', *OR* 2019/3, afl. 1.

Honée, *OR* 2016/67, afl. 9

C. Honée, 'Corporate Governance, een vogelvlucht', *OR* 2016/67, afl. 9.

Josephus Jitta, *OR* 2007/135, afl. 12

M.W. Josephus Jitta, '(G)een Code voor niet-beursgenoteerde ondernemingen', *OR* 2007/135, afl. 12.

Kleipool & Olffen, van, *OR* 2017/56, afl. 7

R.H. Kleipool & M. van Olffen, 'De Nederlandse Corporate Governance Code 2016', *OR* 2017/56, afl. 7.

Kluiver, de, *NJB* 2017/839, afl. 15

H.J. de Kluiver, 'Kroniek van het ondernemingsrecht', *NJB* 2017/839, afl. 15.

Koster, *OR* 2018/5, afl. 1

H. Koster, 'De wettelijke verankering van de Nederlandse Corporate Governance Code 2016', *OR* 2018/5, afl. 1.

Kraker, de, *Bb* 2017/44, afl. 11

H.J. de Kraker, 'Het praktisch nut van de herziene Corporate Governance Code voor het MKB', *Bb* 2017/44, afl. 11.

Kroeze, *OR* 2006/3, afl. 1

M.J. Kroeze, 'Bange bestuurders', *OR* 2006/3, afl. 1.

Olden, *OR* 2019/83, afl. 8

P.D. Olden, 'Bestuur en aansprakelijkheid: intuïtief door de grijze tussenzone', *OR* 2019/83, afl. 8.

Rietveld & Cremers, *OR* 2017/97, afl. 12

S. Rietveld en M. Cremers, 'De Corporate Governance Code en haar inwerkingtreding', *OR* 2017/97, afl. 12.

Schreiber, TGP 1986/2

G. Schreiber, 'De computer: heemeester van de toekomst?', *TGP* 1986/2.

Stolp, NJB 2013/1344, afl. 22

M.M. Stolp, 'Enkele belangrijke aspecten van bestuurdersaansprakelijkheid ex art. 6:162 BW belicht', *NJB* 2013/1344, afl. 22.

Strikwerda, MAB 2002/76(1/2)

J. Strikwerda, 'Wat is ondernemingsbestuur?', *MAB* 2002/76(1/2).

Timmerman, OR 2019/45, afl. 5

V. Timmerman, 'Ernstige verwijten over ernstig verwijt', *Ondernemingsrecht* 2019/45, afl. 5.

Vaessen, MvV 2017, afl. 12.

R.T.L. Vaessen, 'Bestuurdersaansprakelijkheid en Corporate Governance', *MvV* 2017, afl. 12.

Nieuwsberichten

Bergen, van, De Telegraaf 8 april 2019

W. van Bergen, 'Kom met ethische normen voor kunstmatige intelligentie', *De Telegraaf* 8 april 2019, te raadplegen via: <https://www.telegraaf.nl/financieel/3413631/kom-met-ethische-normen-voor-kunstmatige-intelligentie>

Bremmer, Algemeen Dagblad 11 januari 2018

D. Bremmer, 'Kunstmatige intelligentie is de grootste kans die de mensheid heeft', *Algemeen Dagblad* 11 januari 2018, te raadplegen via: <https://www.ad.nl/economie/kunstmatige-intelligentie-is-de-grootste-kans-die-de-mensheid-heeft~abd4c551/>

Cellan-Jones, BBC 2 december 2014

R. Cellan-Jones, 'Stephen Hawking warns artificial intelligence could end mankind', *BBC* 2 december 2014, te raadplegen via: <https://www.bbc.com/news/technology-30290540>

Haegens, de Volkskrant 4 september 2018

K. Haegens, 'Hoogste boete ooit voor ING: winst bank ging boven controle op witwassen', *de Volkskrant*, 4 september 2018, te raadplegen via: <https://www.volkskrant.nl/nieuws-achtergrond/hoogste-boete-ooit-voor-ing-winst-bank-ging-boven-controle-op-witwassen~ba845cd1/>

Madeiros, Wired 28 november 2017

J. Madeiros, 'Stephen Hawking: 'I fear AI may replace humans altogether'', *Wired* 2 november 2017, te raadplegen via: <https://www.wired.co.uk/article/stephen-hawking-interview-alien-life-climate-change-donald-trump>

Middendorp, *de Volkskrant* 26 mei 2019

J. Middendorp, 'Op naar een nieuwe balans tussen overheid, markt en algoritmen', *de Volkskrant* 26 mei 2019, te raadplegen via: <https://www.volkskrant.nl/columns-opinie/op-naar-een-nieuwe-balans-tussen-overheid-markt-en-algoritmen~b378b396/?referer=https%3A%2F%2Fwww.google.nl%2F>

Rooij, van *Algemeen Dagblad* 3 mei 2019

B.J. van Rooij, 'D66 pleit voor miljardeninvestering in Eindhovens instituut kunstmatige intelligentie', *Algemeen Dagblad* 3 mei 2019, te raadplegen via: <https://www.ad.nl/eindhoven/d66-pleit-voor-miljardeninvestering-in-eindhovens-instituut-kunstmatige-intelligentie~ab2fcbad/>

Teunis, *RTLZ* 2 oktober 2018

H. Teunis, 'Nederlandse bedrijven lopen voor in kunstmatige intelligentie', *RTLZ* 2 oktober 2018, te raadplegen via: <https://www.rtlz.nl/tech/artikel/4435321/nederland-bedrijven-kunstmatige-intelligentie-artificial-intelligence>

Verheggen, *Duurzaam bedrijfsleven* 28 juni 2017

E. Verheggen, 'Hoe Volvo kunstmatige intelligentie inzet voor zelfrijdende auto's', *Duurzaam bedrijfsleven* 28 juni 2017, te raadplegen via: <https://www.duurzaambedrijfsleven.nl/mobiliteit/23661/hoe-volvo-kunstmatige-intelligentie-inzet-voor-zelfrijdende-autos>

Kamerstukken

Kamerstukken II/2008/09, 31 763, 3, (MvT).

Overige bronnen

***Artificial Intelligence in Europe* 2018**

Artificial Intelligence in Europe. The Netherlands. Outlook for 2019 and Beyond, Ernst & Young LLP 2018 (commissioned by Microsoft).

Brooks 2017

R. Brooks, 'The seven deadly sins of AI predictions', *MIT Technology review* 2017, te raadplegen via: <https://www.technologyreview.com/s/609048/the-seven-deadly-sins-of-ai-predictions/>

***COSO Enterprise Risk Management* 2013**

COSO Enterprise Risk Management 2013. Internal Control – Integrated Framework, te raadplegen via: <https://www.coso.org/Documents/990025P-Executive-Summary-final-may20.pdf>

***COSO Enterprise Risk Management* 2017**

COSO Enterprise Risk Management 2017. Integrating with Strategy and Performance, te raadplegen via: <https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf>

Culture as a Corporate Asset 2017

Culture as a Corporate Asset 2017, (Report of the NACD Blue Ribbon Commission), The National Association of Corporate Directors.

De transitie naar een digitale samenleving 2017

De transitie naar een digitale samenleving. Een verkenning van kansen en uitdagingen, (Startnota Sociaal-Economische Raad van Vlaanderen van 3 mei 2017), Brussel: SERV 2017, te raadplegen via: <https://www.serv.be/serv/pagina/digitalisering>

Ethische richtsnoeren voor betrouwbare KI 2019

Ethische richtsnoeren voor betrouwbare KI, Onafhankelijke deskundigengroep op hoog niveau inzake kunstmatige intelligentie 2019, (opgericht door de Europese Commissie in 2018), te raadplegen via: <https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top>

Future of risk in the digital era 2019

Future of risk in the digital era. Transformative change. Disruptive risk, Deloitte 2019, te raadplegen via: <https://www2.deloitte.com/nl/nl/pages/risk/articles/future-of-risk-in-the-digital-era.html>

Herziene NCGC 2016

Herziene Nederlandse Corporate Governance Code 2016, te raadplegen via: <https://www.mccg.nl/?page=5178>

Hiemstra & Nevels 2018

A. Hiemstra & I. Nevels, *Algoritmes leiden niet automatisch tot eerlijkere selectie*, Sociale Vraagstukken 3 december 2018, te raadplegen via: <https://www.socialevraagstukken.nl/algoritmes-leiden-niet-automatisch-tot-eerlijkere-selectie/>

MCCGC 2016

Monitoring Commissie Corporate Governance Code, 'De Nederlandse Corporate Governance Code: Voorstel voor herziening: een uitnodiging voor commentaar', 11 februari 2016, p. 11, te raadplegen via: <http://www.mccg.nl/download/?id=2786>

Schatsky, Davenport & Loucks 2018

D. Schatsky, T. Davenport & J. Loucks, *Artificial Intelligence in het bedrijfsleven, de stand van zaken*, Deloitte 2018, te raadplegen via: <https://www.deloitteforward.nl/artificial-intelligence/artificial-intelligence-in-het-bedrijfsleven-de-stand-van-zaken/>

Steels e.a. 2018

L. Steels, B. Berenft, A. Pizurica, J. Vandewalle, 'Artificiële intelligentie. Naar een vierde industriële revolutie?', *Koninklijke Vlaamse Academie van België voor Wetenschappen en Kunsten*, 2018-01, te raadplegen via: https://limo.libis.be/primo-explore/fulldisplay?docid=LIRIAS1999889&context=L&vid=Lirias&search_scope=Lirias&tab=default_tab&lang=en_US&fromSitemap=1

Stulz 2008

R. Stulz, 'Risk management failures. What are they and when do they happen?', *Fisher College of Business Working Paper Series*, oktober 2018, te raadplegen via:
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1278073

Waarde(n)volle zorgtechnologie 2019

Waarde(n)volle zorgtechnologie. Een verkennend advies over de kansen en risico's van kunstmatige intelligentie in de zorg, Raad voor de Volksgezondheid en Samenleving, Den Haag: 2019, te raadplegen via: <https://www.raadvv.nl/documenten/publicaties/2019/02/05/waardenvolle-zorgtechnologie>

Jurisprudentie

Hoge Raad

HR 10 januari 1997, ECLI:NL:HR:1997:ZC2243 (*Staleman/Van de Ven*).
HR 11 juni 1999, ECLI:NL:HR:1999:ZC2925 (*Van Dooren qq/Hendriks*).
HR 8 juni 2001, ECLI:NL:HR:2001:AB2053 (*Panmo*).
HR 29 november 2002, ECLI:NL:HR:2002:AE7011 (*Swandt/Berghuizer Papierfabriek*).
HR 8 april 2005, ECLI:NL:HR:2005:AS010 (*Laurus*).
HR 29 juni 2006, ECLI:NL:HR:2007:BA033.
HR 8 december 2006, ECLI:NL:HR:2006:AZ0758 (*Ontvanger/Roelofsen*).
HR 2 maart 2007, ECLI:NL:HR:2007:AZ3535 (*Holding Nutsbedrijf Westland*).
HR 13 juli 2007, ECLI:NL:HR:2007:BA7970 (*ABN AMRO*).
HR 20 juni 2008, ECLI:NL:HR:2008:BC4959 (*Willemsen/NOM*).
HR 9 juli 2010, ECLI:NL:HR:2010:BM0976 (*ASMI*).
HR 23 november 2012, ECLI:NL:HR:2012:BX5881 (*Spaanse Villa*).
HR 5 september 2014, ECLI:NL:HR:2014:2628, NJ 2015/21 (*Tulip Air*).

Ondernemingskamer

Hof Amsterdam (OK) 16 november 2005, ECLI:NL:GHAMS:2005:AV0121 (*UMI-Beheer*).
Hof Amsterdam (OK) 6 juli 2006, ECLI:NL:GHAMS:2006:AY0520 (*TCA*).
Hof Amsterdam (OK) 9 oktober 2006, ECLI:NL:GHAMS:2006:AZ6791 (*UMI-Beheer*).
Hof Amsterdam (OK) 2 november 2015, ECLI:NL:GHAMS:2015:4454 (*Maevita*).

Rechtbank

Rb. Overijssel 28 mei 2019, ECLI:NL:RBOVE:2019:1827.