AI, verantwoordelijkheid & aansprakelijkheid – de stand van zaken en een weg vooruit.

Roeland de Bruin – van Gogh

1. Inleiding

In deze bijdrage maak ik een momentopname van de civielrechtelijke, buitencontractuele AI-aansprakelijkheidsregulering die in Nederland geldt. Op dit moment is het begin 2026, en is de regelgeving met betrekking tot de verantwoordelijkheid en aansprakelijkheid voor kunstmatige intelligentie (AI, ik ga hieronder nader in op dit concept), volop in ontwikkeling.

AI onderscheidt zich van andere vormen van (informatie)technologie, omdat de algoritmes waarop AI-technologie gebaseerd is, beslissingen kunnen nemen die steeds onafhankelijker worden van directe menselijke sturing. Die beslissingen kunnen grote, ook schadelijke, gevolgen hebben. De Europese wetgever heeft in 2024 regels gesteld die bepaalde verantwoordelijkheden stipuleren voor aanbieders en gebruiksverantwoordelijken van AI. De AI-verordening vormt de basis van die nieuwe regels,[1] hoewel er uiteraard ook vele andere vormen van wet- en regelgeving zijn die men in acht moeten nemen bij het ontwikkelen en uitrollen van AI-technologie. Mede indachtig de ontwikkelingen op het vlak van AI, heeft de Uniewetgever ook de regels inzake productaansprakelijkheid herzien die geïmplementeerd moet worden door de Lidstaten, en een AI-aansprakelijkheidsrichtlijn voorgesteld – om die vervolgens begin 2025 weer in te trekken. Een mooi moment dus om een opname te maken van het recht dat geldt, dat komt, en dat misschien wel uitblijft.

Dit is het eerste deel van een tweeluik. Om te beginnen doe ik een poging om AI vanuit juridisch perspectief te definiëren, waarbij ik tevens aansluiting zoek bij de benadering die de Uniewetgever heeft gegeven in de AI-verordening (paragraaf 2). Het zwaartepunt van dit deel ligt in de dan volgende paragrafen, waarin ik beschouw in hoeverre de (toekomstige) productaansprakelijkheidsregels (paragraaf 3) kunnen worden toegepast om schade te verhalen op de fabrikanten van de producten in de in onderdeel 4 geschetste casus. De drie casus zijn allen fictief – maar goed voorstelbaar, en illustreren problemen waarbij AI wordt gecorreleerd met bepaalde vormen van schade, die in een civiele procedure zouden moeten worden verhaald. De beantwoording van de productaansprakelijkheidsvragen die uit de casus blijken, gebeurt in paragraaf 5. Dit deel sluit af met een – niet op alle punten tevredenstellende – (tussen)conclusie, die tevens de opmaat vormt voor het tweede deel. Daarin bezie ik of, en zo ja in hoeverre bepaalde andere buitencontractuele aansprakelijkheidsregels mogelijk meer soelaas bieden, en werp ik een blik vooruit. Tot slot doe ik aanbevelingen voor toekomstige aanvullingen van het aansprakelijkheidsregime.

---

[1] Verordening (EU) 2024/1689 van het Europees Parlement en de Raad van 13 juni 2024 tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie en tot wijziging van de Verordeningen (EG) nr. 300/2008, (EU) nr. 167/2013, (EU) nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 en (EU) 2019/2144, en de Richtlijnen 2014/90/EU, (EU) 2016/797 en (EU) 2020/1828 (AI-verordening).

Deze bijdrage borduurt voort op eerder werk, met name mijn proefschrift,[2] een boekbijdrage,[3] en een tweetal artikelen in *Verkeersrecht*.[4] Ik heb gepoogd een zo "vers" mogelijk stuk te schrijven, maar op enkele punten komen er parafrases voor uit die eerdere stukken – uiteraard met de nodige verwijzingen.

2. AI – wat is het (niet)

Alle informatietechnologische processen werken volgens het invoer-verwerking-uitvoer-principe. Als je bijvoorbeeld een calculatorprogramma een "2", de operator "+" en dan nog een "2" *ingeeft*, zal het een optel-algoritme aanspreken, die vervolgens de input *verwerkt*, 2 en 2 bij elkaar optelt, en het resultaat "4" zal *uitvoeren*.[5]

AI-technologie doet dat ook, zij het dat sommige toepassingen zelf kunnen bepalen welke *input* wordt geselecteerd, waarbij het mogelijk is dat de *verwerkingsalgoritmes* zichzelf aanpassen (vaak op basis van externe feedback), en ook dat de algoritmes tot variabele *output* kunnen komen.

> *Het is bijvoorbeeld mogelijk dat AI-toepassingen zo worden getraind dat ze patronen kunnen herkennen in beeldbestanden. Op basis van analyse van een grote hoeveelheid beelden van katten in diverse poses, kan een AI-systeem op den duur (en na – menselijke – feedback), ten aanzien van ingevoerde foto's (invoer) katten van honden en andere beesten onderscheiden (verwerking), en dat verschil benoemen (uitvoer). Zou dat systeem verder evolueren, en worden geïnstalleerd op een smartphone waarop allerhande beeldmateriaal wordt opgeslagen door een gebruiker, kan dat systeem bijvoorbeeld foto's van mensen koppelen aan namen, en zelf een selectie maken van een bepaalde, veel in de fotodatabank voorkomende persoon, en dan een suggestie doen aan de gebruiker voor een beeldverslag van foto's met die persoon die in een bepaalde periode zijn genomen. In dit voorbeeld heeft het algoritme dus het onderscheid tussen bepaalde geportretteerde personen in de fotodatabase (invoer) aangeleerd, en maakt het systeem dus een bepaalde keuze (verwerking) ten aanzien van de betreffende persoon die het voorwerp vormt voor het aan de gebruiker gepresenteerde beeldverslag (uitvoer).*

Wat AI-technologie onderscheidt van meer "traditionele" vormen van computertechnologie, wordt in functioneel opzicht bepaald door een tweetal eigenschappen. Ten eerste bevat AI een zekere mate van *autonomie* en ten tweede een bepaalde vorm van *intelligentie*. Beide concepten

---

[2] R.W. de Bruin, *Regulating Innovation of Autonomous Vehicles: Improving Liability & Privacy in Europe* (diss.), Amsterdam: Delex 2022 & Utrecht: UU 2022, via https://dspace.library.uu.nl/bitstream/handle/1874/416533/proefschrift%20totaal%20en%20finaal%20-%20621f3ca9db52d.pdf?sequence=1&isAllowed=y (De Bruin 2022).

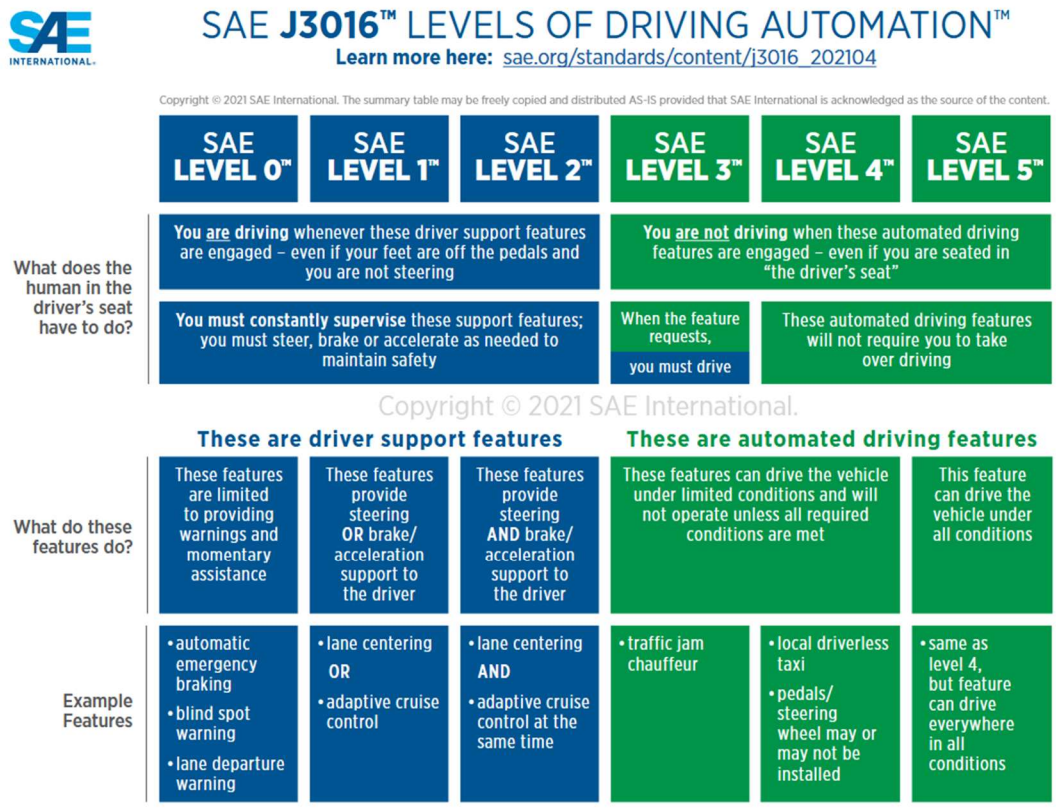
[3] R.W. de Bruin, Informational Privacy and Trust in Autonomous Intelligent Systems. In M. I. Aldinhas Ferreira (Ed.), *Intelligent Systems, Control and Automation: Science and Engineering* (pp. 47-60). (Intelligent Systems, Control and Automation: Science and Engineering; Vol. 102). Springer Science and Business Media https://doi.org/10.1007/978-3-031-09823-9_3 (De Bruin 2022a).

[4] R.W. de Bruin, Verkeersrecht en Autonome Voertuigen: "zoek de fout" wordt problematisch. *Verkeersrecht*, *1*(2), 9-14 (De Bruin 2023); en R.W. de Bruin, Nieuwe productaansprakelijkheidsregels en AI: goed voor innovatie en acceptatie? *Verkeersrecht*, *7/8*(80), 200-206 (De Bruin 2023a).

[5] Overigens kunnen Large Language Models zoals OpenAI's ChatGPT (en andere *taal*modellen) erg slecht rekenen, zo blijkt uit eigen ervaring, en discussies in onder meer de OpenAI Developer Community: https://community.openai.com/t/chatgpt-simple-math-calculation-mistake/62780 (laatst geraadpleegd op 14 november 2025).

zijn op verschillende wijzen te definiëren en vormen goede bronnen voor academisch debat.[6] Gelet op de aard en het doel van deze bijdrage, beperk ik mij hier echter tot een functioneel-juridische beschrijving van beide begrippen.[7]

Vanuit dat perspectief bezien, beschrijft het begrip *autonomie* een spectrum van beslisvaardigheid van een systeem in verhouding tot de noodzaak van menselijk ingrijpen daarin. Hoe minder menselijke tussenkomst er nodig is om een systeem een bepaalde beslissing met een bepaald (rechts)gevolg te laten nemen, des te groter de mate van systeem-autonomie en vice versa. Ter illustratie: zelfrijdende voertuigen kunnen worden ingedeeld op basis van diverse stadia van autonomie. De Amerikaanse Society of Automotive Engineers (SAE) maakt het onderscheid dat hieronder staat afgebeeld:[8]



[6] Zie bijvoorbeeld over *autonomie:* A.P. Wiliams, "Defining Autonomy in Systems: Challenges and Solutions", in A.P. Williams, & P.D. Scharre, *Autonomous Systems – issues for Defence Policymakers*, Den Haag: NATO Communications and Information Agency 2015, via https://www.researchgate.net/publication/282338125_Autonomous_Systems_Issues_for_Defence_Policymakers, en over *intelligentie:* C.R. Davies, "An Evolutionary Step in Intellectual Property Rights – Artificial Intelligence and Intellectual Property", *Computer Law & Cybersecurity Review* 2011, vol. 27, p. 603.

[7] Zie voor een uitgebreidere bespreking De Bruin 2022, hoofdstuk 2.2.

[8] Zie https://brx-content.fullsight.org/site/binaries/content/assets/sae-org/content/news/blog/sae-j3016-visual-chart_5.3.21.pdf.

Deze tabel beschrijft dus zes stadia van autonomie, waarbij er in elk opvolgend stadium minder menselijk ingrijpen nodig is om een auto van A naar B te laten rijden en waarbij er ultimo geen menselijke bestuurder meer noodzakelijk is.

Naast autonomie speelt *intelligentie* een belangrijke rol bij de ontwikkeling van AI. Intelligentie is te beschrijven als het vermogen om gedrag aan te passen aan veranderende omstandigheden.[9] Daarvoor is het nodig dat een systeem in meer of mindere mate in staat is de omgeving waar te nemen (*input*), te leren (*verwerking*) en problemen op te lossen (*output*), onder andere door middel van het verwerken van menselijke taal.[10] "Machine learning" speelt hierbij vaak een rol,[11] en draagt daarmee bij aan de intelligentie van een systeem, om zodoende bijvoorbeeld brondata om te kunnen zetten in meer betekenisvolle informatie.

> *In het eerdergenoemde voorbeeld, is intelligentie waar te nemen: de smartphone-toepassing heeft geleerd welke personen in de fotodatabank waarschijnlijk belangrijk zijn voor de gebruiker. Vervolgens heeft het aan de hand daarvan een selectie gemaakt, die op autonome wijze (dus zonder daartoe een rechtstreekse opdracht te hebben gekregen) aan de gebruiker is gepresenteerd*.

De elementen autonomie en intelligentie zijn ook te herkennen in de definitie die de Europese Uniewetgever hanteert van een "AI-systeem", in de AI-verordening:

> *"een op een machine gebaseerd systeem dat is ontworpen om met verschillende niveaus van autonomie te werken en dat na het inzetten ervan aanpassingsvermogen kan vertonen, en dat, voor expliciete of impliciete doelstellingen, uit de ontvangen input afleidt hoe output te genereren zoals voorspellingen, inhoud, aanbevelingen of beslissingen die van invloed kunnen zijn op fysieke of virtuele omgevingen"*[12]

De rood gemarkeerde onderdelen van de definitie zijn te relateren aan *autonomie* (het spectrum van verschillende niveaus van autonomie, en de beslissingen die effect kunnen hebben op de omgeving), en de blauw gemarkeerde elementen aan het hiervoor besproken begrip van *intelligentie* (aanpassingsvermogen, het vermogen om af te leiden hoe er output moet worden gegenereerd).

3. De nieuwe Richtlijn Productaansprakelijkheid

De herziene richtlijn productaansprakelijkheid (hierna: RPA, of Richtlijn)[13] is in werking getreden op 8 december 2024, en dient op 9 december 2026 te zijn geïmplementeerd in de lidstaten. De RPA vervangt haar voorganger uit 1985, en is op veel punten ingrijpend herzien, mede met het oog op ontwikkelingen in (AI-)technologie.

---

[9] Zie C.R. Davies, "An Evolutionary Step in Intellectual Property Rights – Artificial Intelligence and Intellectual Property", *Computer Law & Cybersecurity Review* 2011, vol. 27, p. 603.
[10] Zie S. Chopra & L.F. White, *A Legal Theory for Autonomous Artificial Agents*, Ann Arbor: The University of Michigan Press 2014, p. 9.
[11] Zie R. Deville, N. Sergeyssels, en C. Middag, "Chapter 1 Basic Concepts of AI for Legal Scholars", in: J. de Bruyne & C. Vanleenhove, *Artificial Intelligence and the Law*, Cambridge: Intersentia 2021, p. 1-22.
[12] Artikel 3 lid 1 AI-verordening.
[13] RICHTLIJN (EU) 2024/2853 VAN HET EUROPEES PARLEMENT EN DE RAAD van 23 oktober 2024 inzake aansprakelijkheid voor gebrekkige producten en tot intrekking van Richtlijn 85/374/EEG van de Raad (Oude Richtlijn, of ORPA).

De hoofdregel van de Richtlijn is dat:

> *iedere natuurlijke persoon die schade lijdt ten gevolge van een gebrekkig product [...] recht heeft op schadevergoeding overeenkomstig deze richtlijn.*[14]

De schade kan worden verhaald op de producent of een andere marktdeelnemer.

Hieronder bespreek ik de hoofdlijnen van de nieuwe regels en ga ik, voor zover in verband met deze bijdrage relevant, achtereenvolgens in op de productdefinitie; de normadressaten (fabrikanten of andere marktdeelnemers); het gebrekkigheidsbegrip; bewijslast en bewijsmiddelen; types schade die voor vergoeding in aanmerking komen; en de verweren inzake ontwikkelingsrisico en gebreken die na marktintroductie zijn ontstaan.

Ik belicht daarbij op welke punten de nieuwe regels afwijken van, of een aanvulling vormen op de "oude" regels, echter zonder die oude regels *en detail* te bespreken.

a. Producten

Een wezenlijke herziening in de nieuwe RPA betreft de reikwijdte. Waar de "oude" richtlijn louter zag op (de meeste) roerende zaken en elektriciteit, is de productdefinitie significant opgerekt in de RPA. Nu luidt deze als volgt:

> *elke roerende zaak, ook nadat zij is geïntegreerd in of onderling is verbonden met een andere roerende of onroerende zaak, met inbegrip van elektriciteit, digitale fabricagedossiers, grondstoffen en software*.[15]

Voor deze bijdrage is met name het laatste element van belang: waar onder de oude regels bij gebrekkige software steeds de vraag moest worden beantwoord of de betreffende (onroerende) software zodanig met de (roerende) hardware verbonden was, dat daardoor ook de hardware gebrekkig werd, is dat niet langer nodig. Immateriële zaken als computerprogrammatuur (en digitale fabricagedossiers) *an sich* zijn nu expliciet begrepen onder het toepassingsbereik van de richtlijn.

Naast producten zijn ook *componenten* opgenomen in de RPA. Een component is:

> *elk materieel of immaterieel voorwerp dat, of elke grondstof of bijbehorende dienst die in een product is geïntegreerd of daarmee onderling is verbonden*.[16]

De fabrikant kan tevens aansprakelijk zijn voor gebrekkige componenten, en als deze een product op zich vormen, kan ook de fabrikant van de betreffende component worden aangesproken.[17]

b. Producenten en andere normadressaten

Net als onder de oude richtlijn, beoogt de Uniewetgever een "one-stop-shop" te creëren voor benadeelden.[18] De belangrijkste actor ("marktdeelnemer") die onder de RPA aansprakelijk kan

---

[14] Artikel 5 RPA. Artikel 1 ORPA formuleert net iets anders: "De producent is aansprakelijk voor de schade, veroorzaakt door een gebrek in zijn product", maar komt op hetzelfde neer.
[15] Artikel 4 lid 1 RPA.
[16] Artikel 4 lid 4 RPA.
[17] Zie artikel 8 lid 1 sub b (en c) RPA.
[18] Daar werd als producent aangemerkt: "fabrikant van een eindprodukt, de producent van een grondstof of de fabrikant van een onderdeel, alsmede een ieder die zich als producent presenteert door zijn naam, zijn merk of een ander onderscheidingsteken op het produkt aan te brengen"(artikel 3 lid 1 van de oude

worden gesteld is de *fabrikant*.[19] Dat is degene die een product ontwikkelt, vervaardigt of produceert (zelfs voor eigen gebruik), heeft ontworpen, *of* die zich presenteert als de fabrikant, door zijn naam, handelsmerk of andere onderscheidende tekens erop aan te brengen.[20] Andere marktdeelnemers die aansprakelijk kunnen worden gesteld zijn *componentfabrikanten*;[21] en als de fabrikant buiten de EU is gevestigd, de *importeur*;[22] de *gemachtigde* van de fabrikant;[23] of als die ontbreken, de *fulfilmentdienstverlener*.[24]

Als geen van deze marktdeelnemers kan worden gevonden, kan de *distributeur* aansprakelijk worden gesteld,[25] indien deze niet binnen één maand na ontvangst van een daartoe strekkend verzoek de identiteit bekend maakt van de voornoemde marktdeelnemers (of zijn eigen distributeur) die het betreffende product aan hem heeft/hebben geleverd.[26]

Tot slot moet nog één andere actor worden genoemd, en dat is degene die een product

> *ingrijpend wijzigt zonder dat de fabrikant daarover zeggenschap heeft en het vervolgens in de handel brengt*.[27]

Deze *ingrijpende wijziger* wordt door de RPA als *fabrikant* beschouwd. Wat ingrijpend wijzigen behelst, staat ook beschreven in de RPA. Eerst verwijst het naar productveiligheidsregels voor een definitie daarvan, maar als daarin een beschrijving ontbreekt moet men ervan uitgaan dat er sprake is van een ingrijpende wijziging als de oorspronkelijke prestaties, het doel of het type van een product wijzigen, zonder dat deze wijziging was voorzien in de oorspronkelijke risicobeoordeling van de fabrikant, en indien deze wijziging de aard van het gevaar verandert, een nieuw gevaar creëert of het risiconiveau verhoogt.[28]

Benadeelden in de zin van de RPA, kunnen elke marktdeelnemer hoofdelijk aansprakelijk stellen.[29] Vervolgens kan een aangesproken marktdeelnemer regres nemen op een andere marktdeelnemer overeenkomstig het nationale recht.[30] Hoewel aansprakelijkheid jegens benadeelden niet (wettelijk of contractueel) mag worden uitgesloten,[31] lijkt een contractuele uitsluiting van regres (of vrijwaring) niet in scope van de Richtlijn – althans niet volledig

---

Richtlijn Productaansprakelijkheid 1985 (ORPA)). Ook onder die vlag aansprakelijk: “een ieder die een produkt in de Gemeenschap invoert om dit te verkopen, te verhuren, te leasen of anderszins te verstrekken, in het kader van zijn commerciële activiteiten, beschouwd als producent in de zin van deze richtlijn” (lid 2)

[19] Artikel 8 lid 1 sub a RPA.

[20] Artikel 4 lid 10 RPA.

[21] Zie vorige alinea en artikel 8 lid 1 sub b en c RPA.

[22] Sub c, onder i: *een natuurlijke persoon of rechtspersoon die een product uit een derde land in de Unie in de handel brengt* (artikel 4 lid 12).

[23] Sub c onder ii: *een in de Unie gevestigde natuurlijke persoon of rechtspersoon die schriftelijk door een fabrikant is gemachtigd om namens die fabrikant specifieke taken te vervullen* (artikel 4 lid 11).

[24] Sub c onder iii: *een natuurlijke persoon of rechtspersoon die in het kader van een handelsactiviteit minstens twee van de volgende diensten aanbiedt: opslag, verpakking, adressering en verzending van een product, zonder eigenaar van dat product te zijn, met uitzondering van postdiensten [en pakketdiensten; andere postdiensten of vrachtvervoersdiensten]* (artikel 4 lid 13).

[25] De distributeur is *een andere natuurlijke persoon of rechtspersoon in de toeleveringsketen dan de fabrikant of importeur die een product op de markt aanbiedt* (artikel 4 lid 14).

[26] Artikel 8 lid 3 RPA.

[27] Artikel 8 lid 2 RPA.

[28] Artikel 4 lid 18 RPA.

[29] Artikel 12 lid 1 RPA.

[30] Artikel 14 RPA.

[31] Artikel 15 RPA.

geharmoniseerd. Wat hierin namelijk opvalt, is dat fabrikanten van producten waarin software als component is geïntegreerd, *geen* regres kunnen nemen jegens de softwarefabrikant, als die laatste kwalificeert als micro- of kleine onderneming in de zin van het Unierecht, *mits* contractueel is overeengekomen dat de productfabrikant geen regresrecht heeft jegens de kleine softwarefabrikant.[32] Of deze regeling (a contrario) meebrengt dat regres-uitsluitingen van andersoortige marktdeelnemers onderling in strijd zou zijn met de RPA, vraag ik mij af – maar is op het eerste gezicht niet geheel helder.

c. Gebrekkigheid

Ingevolge artikel 7 RPA, is een product *gebrekkig*

> *indien het niet de veiligheid biedt die een persoon mag verwachten of die uit hoofde van het Unierecht of het nationale recht is vereist*.[33]

Deze definitie verschilt subtiel van de "oude", die niet aangreep op de verwachtingen van een persoon, maar meer in algemene zin verwees naar "de veiligheid [...] die men gerechtigd is te verwachten",[34] en waarin niet werd expliciet werd verwezen naar Unierechtelijke of nationale (product)veiligheidsregels. In verband met deze bijdrage is het van belang om hier te wijzen op een wezenlijke uitbreiding van de Europese productveiligheidsregels in verband met AI: in 2024 is de AI-verordening in werking getreden. Deze bevat een veelheid aan nieuwe verplichtingen voor *aanbieders*[35] (producenten) en *gebruiksverantwoordelijken*[36] (professionele gebruikers) van AI-systemen[37] en AI-modellen voor algemene doeleinden.[38] Al naargelang de risico's die de AI-systemen of -modellen behelzen voor burgers, zijn er in 5 categorieën regels opgesteld waaraan ex-ante voldaan moet worden. Wat betreft de AI-systemen wordt er onderscheid gemaakt tussen "gewone" AI-systemen; systemen met "hoge risico's"[39] respectievelijk "onacceptabele risico's".[40] Voor de eerste categorie gelden met name transparantie-eisen waaraan aanbieders en gebruiksverantwoordelijken moeten voldoen.[41] AI-systemen met onacceptabele risico's mogen *niet* worden ontwikkeld of geëxploiteerd binnen de EU.[42] Voor het mogen inzetten van hoog-risico AI-systemen gelden de meeste, vaak ook ingrijpende regels waaraan aanbieders en gebruiksverantwoordelijken moeten voldoen.[43] De Uniewetgever onderscheidt AI-modellen voor algemene doeleinden van AI-systemen. Er zijn twee categorieën AI-modellen voor algemene doeleinden gedefinieerd: met en zonder "systeemrisico's".[44] Aanbieders van modellen met systeemrisico's moeten aan meer (veiligheids)verplichtingen voldoen,[45] dan wanneer er geen sprake is van systeemrisico's.[46] Voor een korte algemene toelichting van de AI-verordening

[32] Artikel 12 lid 2 RPA.
[33] Artikel 7 lid 1 RPA.
[34] Artikel 6 ORPA.
[35] Artikel 3 lid 3 AI-verordening.
[36] Lid 4.
[37] Lid 1.
[38] Lid 63
[39] Artikel 6 AI-verordening.
[40] Artikel 5 AI-verordening.
[41] Zie onder meer artikel 4 en artikel 50 AI-verordening.
[42] Artikel 5 AI-verordening.
[43] Hoofdstuk III, afdeling 2-3 AI-verordening,
[44] Artikel 51 AI-verordening.
[45] Hoofdstuk V, afdeling 3 AI-verordening.
[46] Hoofdstuk V, afdeling 2 AI-verordening.

verwijs ik naar onderdeel 5 hierna, waar ik voor zover van belang nader inga op enkele verplichtingen voor AI-producenten.

In zowel het oude als het nieuwe productaansprakelijkheidsregime, worden omstandigheden genoemd die in aanmerking kunnen worden genomen bij de vaststelling van gebrekkigheid, en ook dat lijstje is uitgebreid onder artikel 7 lid 2 RPA (overeenkomstige tekst met de Oude RPA (ORPA) rood; nieuwe tekst: zwart):

a) de presentatie en de kenmerken van het product, met inbegrip van de etikettering, het ontwerp, de technische kenmerken, de samenstelling en de verpakking, alsook de assemblage-, installatie-, gebruiks- en onderhoudsinstructies;
b) het redelijkerwijs te verwachten gebruik van het product;
d) het effect op het product van het vermogen om te blijven leren of nieuwe functies te verwerven nadat het in de handel is gebracht of in gebruik is gesteld;
e) het redelijkerwijs te verwachten effect op het product van andere producten waarvan kan worden verwacht dat zij samen met het product worden gebruikt, onder meer door middel van onderlinge verbindingen;
f) het tijdstip waarop het product in de handel is gebracht of in gebruik is gesteld of, indien de fabrikant na dat tijdstip de zeggenschap over het product behoudt, het tijdstip met ingang waarvan de fabrikant niet langer de zeggenschap over het product heeft;
g) alle terugroepingen van het product of alle andere relevante interventies met betrekking tot de productveiligheid door een bevoegde autoriteit of een marktdeelnemer zoals bedoeld in artikel 8;
h) de specifieke behoeften van de gebruikersgroep voor wie het product is bestemd;
i) in het geval van een product dat juist bedoeld is om schade te voorkomen, elk falen van het product om aan dat doel te voldoen.

Wat hier onder andere opvalt, is dat de Uniewetgever nu rekening heeft gehouden met het lerend en ontwikkelend vermogen van (software)producten. Als een product als zodanig wordt vermarkt en de producent laat na om te beantwoorden aan de leer- en ontwikkelverwachtingen, of het product (of een verbonden product) raakt onveilig vanwege die capaciteiten, kan dat een *gebrek* meebrengen in de zin van de RPA. Dit betekent dus, dat een producent ook na de eerste verkoop van zijn product, het product moet monitoren en veilig houden (of terugroepen). Die, en aanvullende verplichtingen die daarmee in lijn zijn, komen op meerdere plekken terug in de RPA, en bespreek ik hierna verder in onderdeel d en e.

Overigens is het (nog steeds) zo dat het verschijnen van nieuwe, betere producten, niet meebrengt dat de oudere daarom als gebrekkig moeten worden aangemerkt.[47]

d. Bewijslast en bewijsmateriaal

i. Bewijslast en bewijsvermoedens

De bewijslastverdeling is niet gewijzigd in de RPA. Benadeelden moeten ingevolge artikel 10 lid 1 RPA stellen en bewijzen dat er sprake was van een *gebrek*, van *schade* (die onder de Richtlijn valt, zie onderdeel e), en van een *causaal verband* tussen het gebrek en de opgetreden schade.[48]

[47] Artikel 7 lid 3 RPA; 5 lid 2 ORPA.
[48] Vgl de overeenkomstige regeling in artikel 4 ORPA.

Indachtig de steeds complexer wordende technologische (software en AI-)producten die op de markt beschikbaar zijn, heeft de wetgever wel een aantal bewijshulpmiddelen geïntroduceerd. Zo dient een rechter een bewijsvermoeden van gebrekkigheid te hanteren, wanneer:

a) *de verweerder verzuimt toegang te verlenen tot relevant bewijsmateriaal op grond van artikel 9, lid 1;*[49]
b) *de eiser [aantoont] dat het product niet voldoet aan [Unie- of nationaalrechtelijke] dwingende productveiligheidsvoorschriften die bedoeld zijn om bescherming te bieden tegen het risico van de door de benadeelde geleden schade;*[50] *of*
c) *de eiser [aantoont] dat de schade werd veroorzaakt door een kennelijk disfunctioneren van het product, bij redelijkerwijs te verwachten gebruik of onder normale omstandigheden*[51]

De verplichting tot het ontsluiten van relevant bewijsmateriaal (dat ik hierna in onderdeel ii verder bespreek) komt overeen met een verplichting uit de AI-verordening die ziet op transparantie van algoritmische besluitvorming – maar gaat dus verder dan AI-gerelateerde gevallen. De bepaling dat een gebrek moet worden aangenomen in geval er een specifieke productveiligheidsregel is geschonden, strookt met de voorziening in artikel 7 lid 1, laatste zin RPA, en toont eens te meer de samenhang aan tussen de productveiligheids- en productaansprakelijkheidsregels. De derde voorziening maakt het (wellicht) makkelijker dan voorheen om bij een objectiveerbaar disfunctioneren gebrekkigheid vast te stellen, hoewel dat nog altijd moet worden aangetoond door het slachtoffer.

Een tweede bewijsvermoeden betreft het causale verband. Dat moet worden aangenomen:

> *wanneer is vastgesteld dat het product gebrekkig is en dat de soort veroorzaakte schade doorgaans strookt met het betrokken gebrek.*[52]

Ook hier harmoniseert de wetgever een objectieve(re) benadering van het causale verband tussen gebrek (dat nog maar moet worden vastgesteld) en de opgetreden schade.[53] Hier zouden slachtoffers bijvoorbeeld wat kunnen hebben aan eerder opgetreden schades: als die al eens (in rechte) zijn vastgesteld, is het in een volgend geval wellicht makkelijker om causaliteit vast te stellen bij eenzelfde gebrek.

Een derde bewijsvermoeden kan zowel het gebrek als de causaliteit betreffen. Als een slachtoffer ondanks de omstandigheid dat hij toegang heeft gekregen tot het betreffende bewijsmateriaal, en rekening houdend met alle omstandigheden van het geval:

a) *de eiser wordt geconfronteerd met buitensporige moeilijkheden, met name als gevolg van technische of wetenschappelijke complexiteit, om de gebrekkigheid van het product en/of het oorzakelijk verband tussen de gebrekkigheid van het product en de schade aan te tonen,*[54] *en*

---

[49] Artikel 10 lid 2 sub a RPA.
[50] Sub b.
[51] Sub c.
[52] Artikel 10 lid 3 RPA.
[53] Zie uitgebreider: M.J.J. de Ridder, 'Het bewijs van gebrekkigheid en causaal verband bij complexe producten in het voorstel voor een nieuwe productaansprakelijkheidsrichtlijn', *NTBR* 2023/39, afl. 9 (De Ridder 2023), onderdeel 4.4.
[54] Artikel 10 lid 4 sub a RPA.

b) *de eiser aantoont dat het waarschijnlijk is dat het product gebrekkig is en/of dat er een oorzakelijk verband bestaat tussen de gebrekkigheid van het product en de schade,*[55]

moeten gebrekkigheid en/of causaliteit worden aangenomen.

De lat om gebruik te kunnen maken van dit derde bewijsvermoeden ligt daarmee wellicht hoog voor slachtoffers, hoewel de wetgever geen aanwijzingen geeft omtrent de exacte hoogte daarvan. De tekst luidt echter wel dat benadeelden moeten aantonen dat het "buitensporig moeilijk" is om een gebrek of causaliteit aan te tonen.[56] Het is een kenmerk van AI-technologie, dat het per definitie ingewikkeld is, vanwege bijvoorbeeld de ondoorzichtigheid van algoritmes en de enorme hoeveelheid data die daarmee worden verwerkt, om te achterhalen welke *input* er tot bepaalde *output* heeft geleid, hetgeen vaak nodig zal zijn om gebrekkigheid en causaliteit aan te tonen.[57] Dat is echter niet voldoende: er moet aangetoond worden dat het daarenboven *buitensporig* moeilijk is om een en ander te bewijzen. Men kan zich dan afvragen in welke gevallen daarvan sprake zal zijn, en hoe dat moet worden aangetoond. Een andere lezing van deze bepaling zou mee kunnen brengen dat juist omdat AI-technologie zo complex is, het daarom welhaast per definitie buitensporig moeilijk is om een en ander te bewijzen – en een vermoeden daarbij zou moeten helpen, en dat de lat daarmee niet al te hoog mag komen te liggen.

Daarnaast moet een slachtoffer aantonen dat het waarschijnlijk was dat het product gebrekkig was, en/of dat er sprake was van causaliteit. Daarmee lijkt deze voorziening enigszins in de eigen staart te bijten: dit hulpmiddel kan worden ingeroepen bij bewijsmoeilijkheden die zien op gebrekkigheid en causaliteit, maar daarvoor is dan dus wel nodig dat kan worden bewezen dat gebrek respectievelijk causaliteit *waarschijnlijk* zijn. Ook hier geldt, dat de criteria nadere uitwerking in de jurisprudentie behoeven (welke ruimte zou moeten bestaan, gelet op de openheid van de formulering).

Overigens heeft de aangesproken marktdeelnemer altijd het recht om aangenomen bewijsvermoedens te weerleggen.[58]

ii. Bewijsmateriaal

Artikel 9 RPA biedt een nieuwe voorziening voor slachtoffers met een productaansprakelijkheidsclaim. Waar er traditioneel sprake is van een flinke informatie-asymmetrie tussen producenten en slachtoffers,[59] wordt daarvoor een regeling getroffen in de nieuwe Richtlijn om te pogen tot een betere informatiebalans te komen.

Het eerste lid voorziet erin, dat wanneer een slachtoffer *aannemelijk kan maken* (op basis van "feiten en bewijsmateriaal" – de wetgever specificeert niet wanneer daarvan sprake is) dat hij een vordering tot schadevergoeding heeft jegens een marktdeelnemer ("verweerder"), deze

---

[55] Sub b.

[56] Zie overigens, en milder: R.L. Markus & Y. el Ghaddar, 'De nieuwe Richtlijn productaansprakelijkheid ontward: belangrijkste wijzigingen en impact op collectieve acties en de verzekeringsbranche in kaart gebracht', *AV&S* 2023/21, afl. 4 (Markus en El Ghaddar 2023, onderdeel 2.5), die stellen dat *bewijs* te dien aanzien niet van de benadeelde mag worden verwacht. Elbert de Jong is stelliger, en werpt de vraag op of de "gelaedeerde niet blij wordt gemaakt met een dode mus", E.R. de Jong, 'Europeanisering van bewijs en aansprakelijkheid', *NTBR* 2023/8, (hierna: De Jong 2023); Zie voorts: De Ridder 2023, onderdeel 4.6.

[57] Zie De Bruin 2022, p. 281. Zie ook De Jong 2023.

[58] Artikel 10 lid 5 RPA.

[59] Zie De Bruin 2022, p. 290.

aangesproken verweerder onder bepaalde voorwaarden het relevante bewijsmateriaal ter beschikking moet stellen waarover hij of zij beschikt.

Die verplichting is wederzijds: ook een verweerder die in aantoonbare bewijsnood verkeert om een vordering te betwisten, kan van de eiser inzage vorderen op grond van lid 2.

Het is aan de nationale rechter om te bepalen wat "noodzakelijk en evenredig" is aan te verstrekken bewijs,[60] waarbij er rekening dient te worden gehouden met

> *de rechtmatige belangen van alle betrokken partijen, met inbegrip van die van derden, met name met betrekking tot de bescherming van vertrouwelijke informatie en bedrijfsgeheimen.*[61]

Als de verweerder meent dat de te ontsluiten informatie bedrijfsgeheimen bevat, moet de betreffende rechterlijke instantie hetzij op verzoek, hetzij ambtshalve, maatregelen treffen om de bedrijfsgeheime informatie vertrouwelijk te houden.[62]

Lid 6 bepaalt vervolgens dat een rechter, op verzoek van een eisende partij, van een verweerder kan verlangen dat het verzochte bewijsmateriaal "op een gemakkelijk toegankelijke en begrijpelijke wijze wordt overgelegd", voor zover dat evenredig is in termen van kosten of inspanningen aan de zijde van de verweerder. Deze voorziening kan nuttig zijn voor slachtoffers: een integrale "dump" van alle logbestanden zal vaak niet volstaan, een verweerder moet (voor zover dat evenredig en niet te duur is) betekenisvolle, begrijpelijke informatie overleggen.[63]

Deze bepalingen sluiten enigszins aan op de loggingvereisten uit de AI-verordening. Die komen op enkele plaatsen terug, maar de volgende zijn in dit verband met name van belang. Aanbieders van hoog-risico AI-systemen zijn verplicht om die systemen automatische logs te laten genereren, die de "gebeurtenissen gedurende de levenscyclus van het systeem automatisch [registreren]".[64] Die logs moeten onder meer informatie bevatten over de risico's voor de grondrechten van burgers; moeten monitoring van de werking van het systeem mogelijk maken; moeten in bepaalde gevallen vastleggen wanneer het systeem werd gebruikt; en moeten informatie bevatten over de inputdata (en de referentiedata) en vermelden welke personen de output hebben geverifieerd.[65] Dergelijke logs moeten worden bewaard door aanbieders[66] en gebruiksverantwoordelijken,[67] gedurende (in beginsel) tenminste zes maanden.

Daarnaast hebben burgers die te maken krijgen met een besluit dat wordt genomen op basis van de output van een hoog-risico AI-systeem,[68] recht op duidelijke inhoudelijke uitleg van de gebruiksverantwoordelijke over de rol van het systeem bij de besluitvorming, en de voornaamste

---

[60] Artikel 9 lid 3 RPA.
[61] Lid 4.
[62] Lid 5.
[63] Zie ook: K.A.P.C. van Wees & N.E. Vellinga, 'Voorstel nieuwe richtlijn productaansprakelijkheid: Naar een toekomstbestendig productaansprakelijkheidsrecht?', *Verkeersrecht* 2023/79, onderdeel 5 (Van Wees & Vellinga 2023).
[64] Artikel 12 lid 1 AI-verordening.
[65] Zie lid 2 en 3.
[66] Artikel 19 lid 1 AI-verordening.
[67] Artikel 26 lid 6 AI-verordening.
[68] Uitgezonderd AI-systemen die onderdeel uitmaken van de kritieke infrastructuur.

elementen van het genomen besluit.[69] Dat recht bestaat overigens alleen voor zover het betreffende besluit

> *rechtsgevolgen heeft voor die persoon, of op deze op vergelijkbare wijze aanzienlijke invloed heeft die hij of zij als nadelige gevolgen voor zijn of haar gezondheid, veiligheid of grondrechten beschouwt.*[70]

e. Schadetypen

De schadetypen die onder de RPA voor vergoeding in aanmerking komen, behelzen schade door overlijden, letselschade (met inbegrip van medisch erkende schade aan de geestelijke gezondheid);[71] zaakschade[72] - uitgezonderd schade aan het product zelf,[73] of een product dat is beschadigd door een door of vanwege de fabrikant geïntegreerde/verbonden component,[74] of uitsluitend voor beroepsdoeleinden gebruikte zaken;[75] en vernietiging of corruptie van niet voor beroepsdoeleinden gebruikte gegevens.[76]

Er is geen "franchisebedrag" meer van 500 Euro, waarvan wel sprake was onder de Oude Richtlijn.[77] In plaats daarvan bepaalt artikel 6 lid 2 dat "alle materiële verliezen" moeten worden vergoed, en ook immateriële schades, "voor zover die uit hoofde van het nationale recht kunnen worden vergoed".

Voor andere schadetypen (op grond van andere aansprakelijkheidsregelingen) dan de in de RPA genoemde, wordt verwezen naar de nationale regimes, waaraan de RPA overigens geen afbreuk doet.[78]

f. Verweren (een selectie)

Artikel 11 RPA stipuleert "vrijstellingen van aansprakelijkheid". Een aangesproken marktdeelnemer kan zich kwijten van een claim, als hij bijvoorbeeld bewijst (hier rust wel de bewijslast op de betreffende marktdeelnemer) dat hij het product niet in de handel heeft gebracht of in gebruik heeft gesteld (als fabrikant of importeur);[79] of dat hij het niet op de markt heeft aangeboden (als distributeur).[80] Ook kan een verweer in stelling worden gebracht als kan worden bewezen dat het gebrek het gevolg is van handelen in overeenstemming met wettelijke voorschriften;[81] dat, in het geval van een gebrekkige component, dat gebrek is toe te schrijven aan het ontwerp van het "hoofdproduct", of aan de instructies van de producent van dat product.[82] Als de aangesproken producent een ingrijpend wijziger is (in de zin van artikel 8 lid 2),

---

[69] Artikel 86 AI-verordening.
[70] Ibid. Vergelijk overigens met artikel 22 AVG, dat een verbod behelst op volledig geautomatiseerde besluitvorming zonder contractuele noodzaak, specifieke wettelijke grondslag, of opt-in toestemming van een betrokkene, en bepaalt dat er altijd recht is op "menselijke tussenkomst".
[71] Artikel 6 lid 1 sub a RPA.
[72] Sub b.
[73] Sub b onder i.
[74] Onder ii.
[75] Onder iii.
[76] Sub c.
[77] Artikel 9 sub b ORPA.
[78] Artikel 6 lid 3 RPA.
[79] Artikel 11 lid 1 sub a.
[80] Sub b.
[81] Sub d.
[82] Sub f.

kan diegene zich verweren als het opgetreden gebrek geen verband houdt met het gewijzigde onderdeel van het product.[83]

Voor deze bijdrage zijn er twee andere verweren van groter belang, te weten die zijn vermeld sub c (later ontstane gebreken) en sub e (ontwikkelingsrisicoverweer).

Als het

> *Aannemelijk is dat de gebrekkigheid die de schade heeft veroorzaakt, niet bestond op het tijdstip waarop het product in de handel werd gebracht, in gebruik werd gesteld, of in het geval van een distributeur, op de markt werd aangeboden, of dat die gebrekkigheid na dat tijdstip is ontstaan*,[84]

kan de aangesproken marktdeelnemer onder de vestiging van productaansprakelijkheid uitkomen. Hierbij moet wel direct worden gewezen op het tweede lid, dat bepaalt dat stelt dat er geen beroep kan worden gedaan op dit verweer inzake later ontstane verweren, als bewezen kan worden dat het gebrek te wijten is aan

a) *Een bijbehorende dienst,*
b) *Software, met inbegrip van software-updates of -upgrades*
c) *een ontbreken van software-updates of -upgrades die nodig zijn om de veiligheid te handhaven,* [of]
d) *een ingrijpende wijziging van het product*

een en ander voor zover de aangesproken fabrikant daar zeggenschap over had.

Dit brengt dus onder meer mee dat een producent zich niet kan verschuilen achter het argument dat de (AI-)software veilig was op het moment van marktintroductie, als hij verzuimd heeft het product daarna veilig te houden.

Dan is er ook nog het ontwikkelingsrisicoverweer. Dat kan worden ingeroepen wanneer het

> *op grond van de objectieve stand van de wetenschappelijke en technische kennis op het tijdstip waarop het product in de handel werd gebracht of in gebruik werd gesteld dan wel gedurende de periode waarin de fabrikant de zeggenschap over het product had, niet mogelijk was de gebrekkigheid te ontdekken.*[85]

Deze regeling reflecteert eveneens het principe dat producenten hun (AI-)product veilig moeten houden na marktintroductie, bij gebreke waarvan ze geen beroep kunnen doen op het ontwikkelingsrisicoverweer.

Net als onder de Oude Richtlijn, mogen nationale wetgevers er overigens voor kiezen om het ontwikkelingsrisicoverweer in het geheel niet op te nemen in hun stelsels. Bestaande regelingen mogen worden gehandhaafd,[86] en nieuwe beperkingen van dit specifieke verweer mogen worden ingevoerd, voor zover dit a) wordt beperkt tot specifieke categorieën van producten; b) verenigbaar zijn met het algemeen belang; en c) proportioneel zijn gelet op die doelstellingen van algemeen belang.[87]

---

[83] Sub g.
[84] Artikel 11 lid 1 sub c RPA.
[85] Sub e.
[86] Artikel 18 lid 1.
[87] Lid 2, jo. 3.

4. Ca(i)sus

Hieronder beschrijf ik drie casus die weliswaar fictief zijn, maar niet onwaarschijnlijk gelet op de AI-technologie die al beschikbaar of nog in ontwikkeling is, in combinatie met voor de hand liggende toepassingen. In onderdeel 4 beschrijf ik het toepasselijk productaansprakelijkheidskader, en in onderdeel 5 pas ik dat kader toe op de hierna beschreven casus:

a) CleanAId – de overijverige schoonmaakrobot

CleanAId is een Franse producent van een AI-gedreven schoonmaakrobot, voor in huis en op kantoor. Hun CleanAId Pro wordt geadverteerd als "zelflerend, prudent en efficiënt". CleanAId Pro is de eerste op grote schaal geproduceerde humanoïde robot van het bedrijf. De robot lijkt dus op een mens, en beweegt zich op benen voort door een ruimte, met in de armen het nodige schoonmaakgerei, dat al naargelang de klus kan worden aangepast: voor de grotere klussen is er een grijper, voor de kleinere een stoffer en blik, schoonmaak- en stofdoeken. CleanAId Pro beschikt ook over een ingebouwde stofzuiger met een maalmechanisme, zodat grotere stukken afval kunnen worden vergruisd. Alle CleanAId Pro's zijn via internet met elkaar verbonden, en werken gezamenlijk aan een algoritme en een daaraan gekoppelde database. Dat moet leiden tot het zo efficiënt mogelijk schoonmaken van allerhande typen ruimtes, met allerhande typen op te ruimen materie: de CleanAId Pro's leren daarmee van de eigen en elkaars schoonmaakervaringen. De welgestelde familie Van Antwerpen tot Breda heeft een CleanAId Pro aangeschaft, als schoonmaakhulp voor hun aanzienlijke landhuis. De robot doet aanvankelijk goed werk. Totdat deze op enig moment de kostbare collectie Netsuke-beeldjes (kleine, vaak uit steen of hout gesneden Japanse beeldjes die als gordelknoop werden gebruikt) als hardgeworden kauwgom bestempelde, ze uit de vitrine opzoog en vergruisde. CleanAId was op de hoogte van een *bug* die in het algoritme was geslopen, maar liet na deze te repareren, uit vrees voor hun reputatie. Daarbij dacht CleanAId ook dat het wel los zou lopen, en de *bug* vanzelf weer zou verdwijnen. De heer Van Antwerpen tot Breda stelt CleanAId aansprakelijk: de geheel verdwenen collectie was getaxeerd op een waarde van € 100.000,-.

b) lAidger – voor al uw boekhoudingen

lAidger is een nieuwe AI-gedreven tool die boekhoudingen voor het MKB volledig automatiseert. Een ondernemer hoeft maar een foto te maken van de bonnetjes en ze worden geboekt; via spraakberichten gekoppeld aan gegevens van de ERP-database en de digitale urenlijsten van de medewerkers kunnen facturen worden gegenereerd en verstuurd naar klanten; en aan het eind van ieder kwartaal wordt er automatisch een omzetbelasting-aangifte voorbereid. Natuurlijk moet de ondernemer zelf wel even controleren of alles klopt, maar in 9 van de 10 gevallen is aanpassing onnodig. Ook de betaling geschiedt geheel geautomatiseerd: 2,5% van de maandelijkse omzet wordt betaald aan SlAidger BV. Voor Graaisma BV betekent lAidger dat er geen fulltime boekhouder meer nodig is. ZZP'er Blaat wordt voor een paar uurtjes per maand ingehuurd voor de noodzakelijke boekhoudkundige controles – die dus niet veel om het lijf hebben. Eind augustus (Blaat zit de gehele zomer op Gran Canaria en werkt naar eigen zeggen af en toe online) crasht de server waar de database van Graaisma op draait – lekker goedkoop in Pakistan. SlAidger heeft via een derde partij wel een backup, maar bij controle daarvan blijken er vanaf juni tot aan de crash grote fouten te zitten in de boekhouding: inkomende gelden zijn geboekt als uitgaven, urenlijsten kloppen niet en vrijwel alle facturen zijn kwijtgeraakt. Gerard

Graaisma zit met zijn handen in het haar: niet alleen is zijn boekhouding naar de maan, ook lopen er klanten weg die geen vertrouwen meer hebben in de dienstverlening, en vanwege de slechte reputatie die het gevolg is van dit gehannes blijven nieuwe klanten weg. Graaisma raakt in een burn-out waardoor hij drie maanden uit de running is en nóg meer schade lijdt omdat zijn bedrijf stilstaat, en stelt SlAidger aansprakelijk. Die wijst op haar beurt naar Blaat. Het primaire standpunt is dat een fout in lAidger niet bekend is bij hen, en dat Blaat zelf zou hebben zitten rommelen in de database. Subsidiair wordt aangevoerd dat indien er al sprake was van een softwarefout, de schade nooit zo hoog zou zijn opgelopen als Blaat zou hebben opgelet.

c) Drive by wAIre

Het is 7 januari 2028, 2 uur 's nachts. Er ligt een dik pak sneeuw. Amanda Aalbers komt van een feestje en laat zich door haar level 3 autonome auto (zie het tabelletje boven) naar huis rijden. Op enig moment bemerkt ze dat de auto niet op tijd afremt voor een opgevroren stuk weg bij een kruising met verkeerslichten. Te laat! Er ontstaat een aanrijding met twee 60-jarige fietsers (die duidelijk hun rode stoplicht hebben genegeerd), en in de slipstream botste Aalbers' auto ook nog op de bestelbus van Berends. De schade is enorm. De fietsers komen er relatief goed vanaf met enkele botbreuken (niets blijvends) en beschadigde e-bikes. Aalbers' auto en Berends' bestelbus zijn total loss. Berends heeft een whiplash en moet lang revalideren. Aalbers zal nog jaren last hebben van rugklachten. Aalbers spreekt de Duitse autofabrikant dAImW aan. De fietsers en Berends spreken Aalbers aan.

5. Toepassing van de nieuwe regels op de casus

a) CleanAId

De CleanAId Pro is een product in de zin van de RPA (en de software 'sec' zou eveneens als product kunnen worden aangemerkt in de zin van artikel 4 lid 1 RPA). De Franse firma CleanAId is fabrikant in de zin van 8 lid 1 sub a RPA. De vraag is vervolgens of deze humanoïde robot als 'gebrekkig' kan worden gekwalificeerd. Daarvoor moet worden gekeken naar de wettelijk vereiste, of de redelijkerwijs te verwachten veiligheid. Nu een specifieke veiligheidsnorm voor de kwalificatie van "afval" door schoonmaakrobots bij mijn weten ontbreekt, moet dus worden bezien wat de redelijke veiligheidsverwachting van "een persoon" in dezen zou kunnen behelzen. Daarbij kan bijvoorbeeld een rol spelen wat CleanAId daarover aan verwachtingen heeft opgewekt bij de productpresentatie, maar ook het redelijkerwijs te verwachten gebruik en het zelflerend effect dat CleanAId Pro zou kunnen ontplooien na de verkoop aan Van Antwerpen tot Breda, in combinatie met de mogelijkheid tot controle over het functioneren door de fabrikant na ingebruikstelling. In dit geval is het vrij eenvoudig aannemelijk te maken dat de redelijke veiligheidsverwachting behelst, dat er een afdoende onderscheid wordt gemaakt tussen "afval" en "geen afval", en dat er bij twijfel van uit wordt gegaan dat het oormerk "geen afval" de juiste standaardaanname is. Zeker nu CleanAId Pro wordt vermarkt als "zelflerend, prudent en efficiënt" zou een koper/gebruiker ervan uit mogen gaan dat deze geen kostbaarheden voor kauwgom aanziet. Ook nu CleanAId wist van de betreffende *bug*, en naliet daar wat aan te doen, draagt bij aan de in casu eenvoudige aantoonbaarheid van gebrekkigheid in de zin van artikel 7 RPA.

De opgetreden zaakschade valt onder de reikwijdte van artikel 6 lid 1 sub b RPA, en komt daarmee voor vergoeding in aanmerking, mits de causale relatie tussen het gebrek en de schade

kan worden aangetoond. De causaliteit is hier eveneens eenvoudig te bewijzen: zonder de “actie” van CleanAId Pro, was deze vergruizingsschade niet opgetreden.

Het antwoord op de vraag of CleanAId met succes een verweer in de zin van artikel 11 RPA in stelling kan brengen, luidt denkelijk negatief. Het ontwikkelingsrisicoverweer zal niet opgaan, nu bekend is dat CleanAId op de hoogte was van de kauwgombug, en naliet daar wat aan te doen – hetzelfde geldt voor het “later ontstane gebreken-verweer”.

De conclusie in dezen is dan ook dat het waarschijnlijk is dat CleanAId € 100.000,- euro schadevergoeding zal moeten betalen aan Van Antwerpen tot Breda.

b) lAidger

lAidger is een softwareproduct in de zin van artikel 4 lid 1 van de RPA, en SlAidger is de fabrikant.

Wat de schade betreft, moet worden opgemerkt dat de schade aan de database, die bestaat uit verkeerde boekingen en zoekgeraakte facturen *niet* voor vergoeding in aanmerking komt onder de RPA: artikel 5 lid 1 sub c ziet alleen op “vernietiging of corruptie van niet voor beroepsdoeleinden gebruikte gegevens” – en dus niet op professionele databases en gegevens. Wat wel mogelijk voor vergoeding in aanmerking komt, is de schade die Graaisma zelf lijdt ten gevolge van zijn burn-out voor zover dit “medische schade aan de geestelijke gezondheid” behelst. Ook kan de reputatieschade voor vergoeding in aanmerking komen uit hoofde van artikel 5 lid 2 RPA, juncto 6:106 BW.

Het is de vraag of lAidger gebrekkig is in de zin van artikel 7. Uit de casus wordt weliswaar duidelijk dat de backupdatabase “gecorrumpeerd is”, maar de exacte oorzaak daarvan is ongewis. Voor zover mij bekend zijn er geen specifieke (veiligheids)normen voor boekhoudkundige AI-gedreven software op dit moment, en zou de tool als een “gewoon” AI-systeem kwalificeren onder de AI-verordening (er zijn geen redenen om aan te nemen dat dit systeem een onacceptabel of hoog-risico met zich brengt). Men zou kunnen kijken naar de marketing aangaande lAidger, en naar de redelijke veiligheidsverwachting van de gebruikers in combinatie met het gebruik dat er is gemaakt van lAidger (en de controles die er hebben plaatsgevonden). Mijns inziens behelst de redelijke veiligheidsverwachting van een als boekhoudkundige ondersteuning vermarkte tool weliswaar dat men ervan uit mag gaan dat deze inkomsten niet als uitgaven boekt, en facturen gewoon bewaart in plaats van vernietigt. Het is echter de vraag of deze omstandigheden het gevolg zijn van een gebrek in de tool of dat deze een andere oorzaak hebben.

In dezen zou Graaisma inzage kunnen vorderen in het bewijsmateriaal (waaronder de logs, als die er zijn) van de lAIdger-toepassing. SlAidger moet desgevorderd daaraan meewerken ingevolge artikel 9 lid 1 jo. lid 6 RPA, voor zover Graaisma diens vordering aannemelijk kan maken. Gelet op de aanwezige feiten, is het weliswaar niet onaannemelijk dat de tool een rol heeft gespeeld bij het ontstaan van de schade, maar het is onzeker of dat voldoende is. Zou dit wel voldoende blijken, zijn er twee situaties denkbaar: SlAidger kan erin toestemmen het betreffende bewijs op een begrijpelijke wijze (voor zover evenredig, lid 6) over te leggen, in welk geval Graaisma kan proberen daaruit een gebrek te distilleren. SlAidger zou ook kunnen weigeren gevolg te geven aan de bewijsoverleggingsverplichting. In dat geval zal de rechter ingevolge artikel 10 lid 2 sub a, een bewijsvermoeden moeten aannemen dat het product gebrekkig was.

Als Graaisma de beschikking krijgt over het bewijsmateriaal, moet hij vervolgens bezien in hoeverre er aan de hand daarvan kan worden vastgesteld dat sprake was van een gebrek. Dat zou erin kunnen liggen dat er fouten zijn geslopen in de boekhoudkundige processen (verkeerd boeken van inkomsten en uitgaven bijvoorbeeld). Daarvoor zal Graaisma waarschijnlijk de hulp moeten inroepen van een boekhoudkundig specialist, en een technisch specialist die kan bezien of er fouten in de software zaten. Dat is niet onmogelijk (de rechter kan ook getuigendeskundigen aanwijzen), maar wel tijdrovend en waarschijnlijk duur. Als het *niet* mogelijk is om een gebrek vast te stellen, treft de productaansprakelijkheidsclaim geen doel.

Als het *wel* mogelijk is om een gebrek vast te stellen, moet de vraag worden beantwoord of de schade niet zou zijn ontstaan als de software niet gebrekkig was. Ook dat is een lastig te beantwoorden vraag, op basis van de (on)bekende feiten en omstandigheden. Graaisma zou een beroep kunnen doen op het bewijsvermoeden van artikel 10 lid 3 RPA. Hij zou dan moeten aantonen dat het type schade (hier dus beperkt tot de burn-out en reputatieschade) doorgaans strookt met het opgetreden gebrek – hetgeen niet voor de hand ligt. Een andere mogelijkheid zou zijn dat hij tracht aan te tonen dat hij wordt geconfronteerd met "buitensporige moeilijkheden" vanwege de technische of wetenschappelijke complexiteit (artikel 10 lid 4 sub a) om het causale verband aan te tonen. Ook in dezen is (nog) niet helder wanneer daar sprake van zou kunnen zijn. Bovendien zal hij dan al moeten hebben aangetoond dat het *waarschijnlijk* is dat er sprake was van een gebrekkig product *en/of* van causaliteit met de opgetreden schade. Dat zal waarschijnlijk niet gemakkelijk slagen, ook gelet op het verweer dat SlAidger al heeft aangevoerd met betrekking tot de heer Blaat die zijn werk niet goed zou hebben gedaan.

Het is dus onzeker of gebrekkigheid en causaliteit kunnen worden bewezen. En zelfs áls dat lukt, zou SlAidger wellicht het ontwikkelingsrisicoverweer en het later-ontstane-gebreken-verweer in stelling kunnen brengen. Met name dat laatste verweer acht ik kansrijk (het gebrek bestond immers niet op het moment dat lAIdger voor het eerst in gebruik werd genomen), als Graaisma vervolgens niet kan bewijzen dat SlAidger niet al het nodige heeft gedaan om het product van (veiligheids)updates te voorzien.

De conclusie in dezen luidt dus dat Graaisma hooguit zijn burn-out en reputatieschade-gerelateerde nadeel vergoed zou kunnen krijgen onder de RPA, maar dat diens kansen om een en ander bewezen en dus vergoed te krijgen niet erg groot zijn.

c) Drive by wAIre

Ook in deze derde casus is sprake van een product in de zin van de RPA, en dAImW is de fabrikant. De schade van Aalbers aan haar eigen auto komt *niet* voor vergoeding in aanmerking (ook niet als de meegeleverde software als gebrekkige component van het product zou kwalificeren – zie artikel 6 lid 1 sub i en ii RPA). Haar letselschade komt wel mogelijk voor vergoeding in aanmerking, ingevolge artikel 6 lid 1 sub a RPA.

Met betrekking tot de mogelijke gebrekkigheid van de auto(software) moet ook hier gekeken worden naar de veiligheidsverwachtingen te dien aanzien, of de ter zake relevante (product)veiligheidsnormen. In het algemeen geldt er onder het algemene publiek een hogere veiligheidsstandaard met betrekking tot (deels) zelfrijdende auto's wordt verwacht dan met betrekking tot "klassieke" door mensen bestuurde voertuigen. Of die verwachting ook in het perspectief van de RPA tot een hogere standaard leidt, moeten we nog afwachten.[88]

[88] Zie De Bruin 2023, onderdeel c en de verwijzingen aldaar.

Wat de tweede categorie betreft met betrekking tot specifieke veiligheidsregels, moet worden opgemerkt dat er een omvangrijk raamwerk van productveiligheidsregels bestaat, en dat voertuigen waarin AI is verwerkt, hoog-risico AI-systemen zijn in de zin van artikel 6 lid 1 AI-verordening.

In concreto biedt de casus weinig aanknopingspunten om met zekerheid te kunnen stellen dat er sprake was van gebrekkigheid in de zin van de RPA, hoewel dat ook weer niet onaannemelijk is. Om te beginnen was er sprake van een semi-autonoom voertuig, level 3 volgens de SAE-tabel. Uitgangspunt bij een level 3 autonoom voertuig, is dat het onder bepaalde voorwaarden zelf kan rijden, maar dat het dat niet zal doen als niet aan al die voorwaarden wordt voldaan. Dat betekent onder meer dat de menselijke bestuurder de mogelijkheid heeft om zelf te rijden, en zeker ook de verplichting daartoe als het systeem aangeeft dat dat nodig is (wanneer dus niet aan alle voorwaarden voor autonoom rijden wordt voldaan). Er zal dus moeten worden vastgesteld of het voertuig zelf reed, of het daartoe (gelet op de voorwaarden daarvoor) geëigend was, en of er al dan niet werd of moest worden ingegrepen door Aalbers. Als er autonoom werd gereden, en er geen signaal werd gegeven dat Aalbers moest ingrijpen, terwijl dat gelet op de wegtoestand en de overige omstandigheden wél zou hebben gemoeten, kan dat in de richting wijzen van een gebrek in het product. Daarvoor zijn wel enkele aanwijzingen gegeven: de auto remde te laat voor een glad weggedeelte in de nabijheid van verkeerslichten (oplettendheid geboden(!)), waarbij het aannemelijk is dat men zou mogen verwachten dat dat *wel* tot de te verwachten veiligheidssystemen behoort. Net als onder casus b, zou een gehonoreerd bewijsinzageverzoek misschien meer richting geven, hoewel ook in dezen ingewikkeld zal zijn om daaruit gebrekkigheid te distilleren.

Als gebrekkigheid kan worden vastgesteld, is causaliteit de volgende te nemen hobbel. Ook in deze casus is dat geen gegeven. Was het systeem te laat met signaleren of het “teruggeven” van de controle aan Aalbers? Had Aalbers zelf niet beter op moeten letten en het zelfrijdende systeem überhaupt niet moeten inschakelen? Was het ongeval (deels) te wijten aan de fietsers die door rood reden? Zolang de causale relatie tussen het (veronderstelde) gebrek en de opgetreden schade niet 100% zeker is, kan deze niet worden vastgesteld. Wellicht kan een bewijsvermoeden worden ingezet. Dan moet (ook in dezen) bijvoorbeeld worden aangetoond dat de schade (letsel) doorgaans horen bij het opgetreden gebrek in de auto. Dat ligt in dezen voor de hand en kan wellicht tot een (weerlegbaar) bewijsvermoeden leiden. Een tweede bewijsvermoeden zou kunnen worden geput uit de “buitensporige complexiteit” om de causaliteit te bewijzen, indien de gebrekkigheid en/of de causaliteit waarschijnlijk zijn. Gelet op de eerdere overwegingen met betrekking tot de gebrekkigheid, is het wellicht eenvoudiger dan onder casus b om ook dit bewijsvermoeden gehonoreerd te krijgen (mits de lat van de “buitensporige complexiteit” niet te hoog wordt gelegd door de rechter).

Wat de verweren betreft, geldt dat ook in dezen een ontwikkelingsrisicoverweer en een later-ontstane-gebreken verweer kan worden gevoerd. Als een gebrek kan worden aangetoond, zal het lastig zijn om die succesvol in stelling te brengen als dAImW heeft verzuimd de nodige veiligheidsupdates te verstrekken waar hij dat kon.

Hier moet overigens nog worden gewezen op een mogelijk eigen schuld-verweer in de zin van artikel 13 lid 2 RPA. Als dAImW kan aantonen dat de schade niet alleen het gevolg is van een gebrekkig voertuig, maar ook van Aalbers (als zij niet had ingegrepen waar dat wel had gemoeten), kan dat leiden tot een reductie van de schadevergoeding.

Al met al lijkt het erop dat het niet onaannemelijk is dat dAImW productaansprakelijk is, maar dat het lastig zal zijn om gebrek en causaliteit te bewijzen, en het denkbaar is dat eventuele aansprakelijkheid afketst op een verweer, of wordt verminderd met het “eigen schuld”-aandeel van Aalbers.

6) Conclusie en opmaat naar deel 2

In dit eerste deel van het tweeluik heb ik besproken wat AI vanuit juridisch perspectief kan behelzen aan de hand van de invoer-verwerking-uitvoer principes. Als er in die processtappen sprake is van autonomie en intelligentie (waarbij “de machine” besliscapaciteit en aanpassingsvermogen kan ontplooien) resulteert dat in situaties waarin het traditionele (aansprakelijkheids)recht niet voorziet. Dat heb ik nader toegelicht in drie casus. Vervolgens heb ik bezien in hoeverre het productaansprakelijkheidsrecht is aangepast om met vraagstukken om te gaan die voortvloeien uit (onder andere) deze vorm van nieuwe technologie. Daarna heb ik het nieuwe productaansprakelijkheidsregime toegepast op de drie casus. Daaruit volgt dat het productaansprakelijkheidsregime in de eerste, vrij simpele, casus waarschijnlijk prima geëquipeerd is om te worden ingezet ten faveure van het slachtoffer. Bij de twee andere casus, is het voor de respectievelijke benadeelden aanmerkelijk lastiger om hun schade op grond van dit regime te verhalen. Daarbij valt onder meer op dat een typische vorm van AI-gerelateerde schade, namelijk schade aan gegevens en bestanden *niet* voor vergoeding in aanmerking komt als die van “professionele aard” zijn. Ook blijft het lastig om in situaties waarbij het niet evident is dat een AI-product gebrekkig was omdat er bijvoorbeeld een veiligheidsnorm werd geschonden, die gebrekkigheid in rechte aan te tonen (waarbij de verplichting om bewijs over te leggen wel degelijk nuttig is, maar de bewijsvermoedens inhoudelijk weinig evident soelaas bieden), hetgeen ook geldt voor het door de benadeelde te leveren bewijs van causaliteit tussen gebrek en opgetreden schade.

In het tweede deel zal ik beschouwen in hoeverre andere aansprakelijkheidsregimes die van toepassing kunnen zijn op de casus, met succes kunnen worden ingezet door de benadeelden om hun schade te verhalen. Daarbij kijk ik met name naar de Wegenverkeerswet, en het generieke regime inzake onrechtmatige daad, als gecodificeerd in artikel 6:162 BW. Zijdelings kijk ik ook naar het ingetrokken voorstel voor een Europese Richtlijn inzake AI-aansprakelijkheid. Vervolgens trek ik enkele conclusies en (her)formuleer aanbevelingen aan het adres van de (Unie)wetgever.