80 Nieuwe productaansprakelijkheidsregels en AI: goed voor innovatie en acceptatie?

Mr. dr. (R.W.) Roeland de Bruin *

1. Inleiding

AI, de veelgebruikte afkorting voor "artificial intelligence", in het Nederlands wel aangeduid als "kunstmatige intelligentie", staat volop in de belangstelling. Hoewel AI niet eenvoudig te definiëren is, bevat AI-technologie, door een juridische bril beschouwd, een aantal interessante aspecten dat AI onderscheidt van andere technologieën. Eén van die eigenschappen is dat AI vaak over een vorm van "autonomie" beschikt. Autonomie is ook een lastig te omkaderen concept[1], maar kan door een jurist worden begrepen als besliscapaciteit van een systeem. Daarbij gaat het om beslissingen van een systeem (dus "kunstmatig") die voorheen door mensen zouden worden genomen en die een gevolg kunnen hebben in het echt of in het recht.[2] Denk bijvoorbeeld aan de beslissing van een volledig zelfrijdend voertuig om een ander voertuig in te halen waarbij een ander voertuig wordt aangereden. Of, in positievere zin, een pathologie-algoritme dat een bepaalde celstructuur aanmerkt als tumorweefsel dat door het menselijke oog niet als zodanig zou worden geïdentificeerd. Autonomie is geen tweeledig concept en komt in vele gradaties voor: hoe groter de systemische besliscapaciteit, des te groter de mate van autonomie van het systeem.[3] Autonomie veronderstelt een bepaalde mate van "intelligentie". Intelligentie kan worden gezien als het vermogen om gedrag aan te passen aan veranderende omstandigheden. Daarvoor zijn eigenschappen nodig als leren (i.e. "machine learning")[4], redeneren, het oplossen van problemen, het waarnemen van de omgeving en het begrip van taal.[5] Technologie met bepaalde mate van AI is sterk in opkomst. Denk bijvoorbeeld aan chirurgische robots[6], medische diagnostiek[7], of aan "generatieve AI" die teksten genereert zoals het intussen vermaarde ChatGPT.[8]

* Universitair docent regulering & innovatie Universiteit Utrecht (Molengraaff Instituut, Renforce & Ucall); advocaat AI, IE, IT & Privacy KienhuisHoving NV.

Het behoeft nauwelijks betoog dat AI-technologie in vele opzichten veelbelovend is – dat laat ik hier dan ook verder achterwege – om mij in deze bijdrage te concentreren op één van de schaduwzijden, waarin AI (mede) leidt tot ongelukken en schade. Slachtoffers van ongevallen waarbij producten met AI een rol hebben gespeeld, kunnen voor grote problemen komen te staan wanneer zij hun schade proberen te verhalen op de producenten daarvan, bijvoorbeeld onder het huidige productaansprakelijkheidsregime.[9] Die problemen kunnen van diverse aard zijn. Zoals eerder in dit blad geschetst[10], hebben die onder meer te maken met het gebrek in het product dat moet worden aangetoond door het slachtoffer. Wat is de veiligheid die men mag verwachten van een zelfrijdende auto? En, hoe stel je zo'n gebrek nu vast in een technologisch complex, vaak met het internet en andere producten verbonden, en met zelflerende algoritmes doorspekt, big-data gedreven product? Minstens even ingewikkeld zal het zijn om een causale relatie te bewijzen tussen gebrek en opgetreden schade, terwijl aangesproken producenten zich "gemakkelijk" kunnen verweren door aannemelijk te maken dat het gebrek nog niet bestond bij het in het verkeer brengen van het product of dat men het gebrek toen niet had kunnen kennen op basis van de op dat moment beschikbare technische en wetenschappelijke kennis.[11]

Op 28 september 2022 publiceerde de Europese Commissie een voorstel voor een herziene richtlijn inzake productaansprakelijkheid (VRPA),[12] dat onder meer deze problemen uit de wereld zou moeten helpen. Gelijktijdig werd door de EC de Richtlijn inzake (procedurele aspecten van) civiele aansprakelijkheid voor AI (RAAI) voorgesteld[13], dat gezamenlijk met de (iets) oudere voorgestelde AI-verordening[14] het zogenaamde "AI-wetgevingspakket" vormt. In deze bijdrage zal ik de VRPA nader beschouwen. De vraag die ik stel is of de positie van slachtoffers van AV(=autonome voertuigen)-gerelateerde ongelukken onder de voorgestelde regels zou kunnen verbeteren ten opzichte van de huidige situatie. De antwoorden op die vraag zal ik meenemen in een bondige evaluatie van de mogelijke implicaties van de nieuwe regels voor innovatie op het vlak van AI, en de maatschappelijke acceptatie van de resultaten van die

1. Zie A.P. Williams, "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, via https://bit.ly/3iq01wI.
2. Zie o.a. M. de Cock Buning, L.P.C. Belder en R.W. de Bruin, "Mapping the Legal Framework for the Introduction into Society of Robots as Autonomous Intelligent Systems, in: S. Muller, S. Zouridis, M, Frishman, en L. Kistemaker, L. (red.), *The Law of the Future and the Future of Law*: Volume II, Den Haag: Torkel Opsahl Academic EPublisher 2012, p. 195-210.; V. Breemen en A. Wouters, "Hoofdstuk 5, Casestudy Zelfrijdende auto's", in: S. Kulk, & S. van Deursen, *Juridische aspecten van algoritmen die besluiten nemen. Een verkennend onderzoek*, Den Haag: WODC 2020, p. 71-104.; en R.W. de Bruin, *Regulating Innovation of Autonomous Vehicles: Improving Liability & Privacy in Europe* (diss. Universiteit Utrecht), Amsterdam: deLex 2022, p. 26-28.

innovatie. Dat doe ik aan de hand van het toetsingskader dat ik ontwikkelde tijdens mijn promotieonderzoek.[15]

De opbouw van dit artikel is als volgt. Na deze inleiding zet ik in paragraaf 2 de nieuwe regels uit de VRPA uiteen en zet die af tegen de thans geldende. Daarbij schets ik AI-gerelateerde voorbeelden ter illustratie. In paragraaf 3 wordt geëvalueerd' wat de bevindingen uit paragraaf 2 kunnen betekenen voor innovatie en acceptatie van AV's: vanuit enerzijds consumentenperspectief en anderzijds innovatorenperspectief onder de voorgestelde VRPA.

2. Hoofdlijnen van de VRPA

a. Uitgangspunten VRPA

De VRPA beoogt de productaansprakelijkheidsregels bij de tijd te brengen mede gelet op de "groene en digitale transitie".[16] Wat dat laatste betreft merkt de Uniewetgever op dat het oude regime onduidelijkheden bevat aangaande onder meer het toepassingsbereik van de thans geldende regels, en verduidelijkt dat deze ook van toepassing zouden moeten zijn op software en AI, en dat in principe altijd een partij in de EU aansprakelijk gehouden moet kunnen worden voor producten die schade veroorzaken.[17] Dat kan de producent van hardware zijn waarin AI zit vervat, maar ook een softwareproducent, of een aanbieder van "digitale diensten die van invloed zijn op de werking van het product (zoals een navigatiedienst in een autonoom voertuig)".[18] De verantwoordelijkheid om AI-producten veilig te houden eindigt niet bij het op de markt brengen van een betreffend product: gedurende de economische levensduur dient de producent, voor zover mogelijk, veiligheidsupdates ter beschikking te stellen.[19] Omdat AI een hoge mate van technische complexiteit in zich bergt, meent de wetgever dat het in de rede ligt om slachtoffers van AI-ongelukken tegemoet te komen in hun bewijspositie. Deze moeten onder andere gemakkelijker toegang kunnen krijgen tot bewijsmateriaal dat zich onder een producent bevindt.[20] Daarnaast zal een nationale rechter in veel gevallen moeten werken met (weerlegbare) bewijsvermoedens aangaande gebrekkigheid en/of causaliteit als het aannemelijk is dat een AI-product heeft bijgedragen aan de ontstane schade.[21] Om de balans tussen slachtofferbescherming en innovatie te bewaren, blijft het echter nodig om bewijslast (en bewijsrisico) te laten liggen bij de partij die schadevergoeding eist van een producent.[22]

Hierna zet ik uiteen hoe deze uitgangspunten gestalte hebben gekregen in het thans voorliggende wetsvoorstel. Daarbij beperk ik mij tot de onderwerpen die mijns inziens het meest relevant zijn voor innovatoren en consumenten van AI-producten. Onder b beschouw ik de aanpassingen van de product-definitie en onder c leg ik uit op welke manier het gebreksbegrip wordt uitgebreid. Een korte bespreking van de innovatoren die aansprakelijk kunnen worden gehouden komt aan bod onder d. In punt e behandel ik het recht op schadevergoeding, en de vergoedbare schade. Onder f sta ik stil bij de (waarschijnlijk) meest relevante aansprakelijkheidsverweren, inzake gebreken die na marktintroductie zijn ontstaan, en het ontwikkelingsrisicoverweer. Daarna beschouw ik onder g de voorgestelde procedurele hulpmiddelen voor slachtoffers.

b. Aanpassingen in definitie 'product' en gerelateerde digitale diensten

De VRPA definieert een product als "roerende zaak, ook nadat zij is geïntegreerd in een andere [roerende of onroerende] zaak", en ook worden onder product "elektriciteit, dossiers voor digitale fabricage en software verstaan".[23] Met deze definitie wordt het oude productbegrip uit 1985 flink uitgebreid. De wetgever brengt software expliciet onder het toepassingsbereik van de richtlijn om een einde te maken aan de eerdere rechtsonzekerheid op dit punt[24], en vanwege het groeiende belang van software voor de veiligheid van producten.[25] Daarbij maakt het niet uit op welke manier de software ter beschikking wordt gesteld: ook software "uit de cloud" en standalone software vallen onder de nieuwe definitie.[26] Ook zijn gratis- en open-source software "die buiten het kader van een handelsactiviteit wordt ontwikkeld of geleverd"[27] buiten het toepassingsbereik van de richtlijn. Software die weliswaar "gratis" wordt aangeboden, maar waarbij de gebruiker betaalt in de vorm van zijn persoonsgegevens (die vervolgens anders worden aangewend dan ten behoeve van het verbeteren van de beveiliging, interoperabiliteit of compatibiliteit software) valt dan wél weer binnen het bereik.

> *Toelichting 1: Voor producenten van (AI-) software is de voorgestelde productdefinitie van wezenlijke betekenis. Bijvoorbeeld producenten van software voor zelflerende medische robots worden nu direct normadressaat onder de VRPA. Ook fabrikanten van opzichzelfstaande AI-programmatuur (zonder dat deze met hardware is verbonden), denk bijvoorbeeld aan via internet toegankelijke "generatieve AI" zoals ChatGPT of Dall-E, worden risico-aansprakelijk voor schade die het gevolg is van de software.*

Ook "componenten" worden expliciet benoemd in de VRPA. Een component wordt begrepen als elk materieel of immaterieel voorwerp, of een "bijbehorende dienst" die

3. S. Chopra & L.F. White, *A Legal Theory for Autonomous Artificial Agents*, Ann Arbor: The University of Michigan Press 2014.
4. Zie bijvoorbeeld R. Devillé, N. Sergeyssels & C. Middag, "Chapter 1 – Basic Concepts of AI for Legal Scholars", in J. De Bruyne & Cedric Vanleenhove (eds.), *Artificial Intelligence and the law*, p. 1-22.
5. Zie De Bruin 2022, p. 28 en de referte in voetnoot 74 naar onder meer C.R. Davies, "An Evolutionary Step in Intellectual Property Rights – Artificial Intelligence and Intellectual Property", *Computer Law & Cybersecurity Review* 2011, vol. 27, p. 603.
6. Zie bijvoorbeeld: https://www.deingenieur.nl/artikel/robot-voert-zelf-kijkoperatie-uit.
7. Zie bijvoorbeeld: https://www.radboudumc.nl/nieuws/2020/naar-een-aidiagnose-zoals-die-van-de-dokter.
8. Zelf te testen via: https://openai.com/blog/chatgpt.
9. Een mogelijk nog groter probleem vormen schuldaansprakelijkheidsregels. Zie voor een verkenning daarvan eerder in dit blad: R.W. de Bruin, "Verkeersrecht en Autonome Voertuigen: "zoek de fout" wordt problematisch", *VR* 2022/2.
10. Ibidem.
11. Zie artikel 6:185 lid 1 onder b en e BW.
12. Europese Commissie, COM(2022) 495 - Proposal for a directive of the European Parliament and of the Council on liability for defective products (https://single-market-economy.ec.europa.eu/document/3193da9a-cecb-44ad-9a9c-7b6b23220bcd_en).
13. Europese Commissie, COM(2022) 496, final – Richtlijnvoorstel betreffende de aanpassing van de regels inzake niet-contractuele civielrechtelijke aansprakelijkheid aan artificiële intelligentie (AI), (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0496).
14. Voorgestelde Verordening van het Europees Parlement en de Raad COM (2021) 206 final, tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie (https://eur-lex.europa.eu/legal-content/NL/ALL/?uri=CELEX:52021PC0206).
15. R.W. de Bruin, *Regulating Innovation of Autonomous Vehicles: Improving Liability & Privacy in Europe* (diss. Universiteit Utrecht), Amsterdam: deLex 2022, p. 131-134.
16. Toelichting bij de VRPA, p. 1, 6.
17. Ibidem, p. 1-2. Zie eveneens considerans 12, 13, 15, 22-23 (productbegrip) en 26-28, 40 (one-stop-shop voor slachtoffers).
18. Ibidem, p. 6.
19. Zie onder meer considerans 23, 37-38 en ook 41, 43-44.
20. Ibidem, p. 6, en considerans 30-33.
21. Considerans 33-34.
22. Considerans 35.
23. Artikel 4 lid 1 VRPA.
24. Zie De Bruin 2022, p. 79 voor een overzicht van dat discours.
25. Zie considerans 12.
26. Overigens merkt de wetgever op dat de broncode van software niet in scope is, "aangezien het hier louter om informatie gaat". Met die bevinding kan men het oneens zijn (zonder de broncode immers geen functionerende software; en gecompileerde broncode is óók informatie, zij het dat deze direct wordt gebruikt om een processor aan het werk te zetten en daarmee verschilt van de broncode nu die nog gecompileerd ("vertaald") moet worden om uitvoerbaar te zijn voor een systeem), maar hier ligt voor de wetgever de grens. Deze grens lijkt in lijn met de heersende leer uit de Europese jurisprudentie, nu het HvJEU twee jaar

door, of onder zeggenschap[28] van een fabrikant is geïntegreerd in, of verbonden met het product.[29] De VRPA ziet ook op "bijbehorende diensten" die zodanig zijn geïntegreerd in, of verbonden met een product dat het product één of meer van zijn functies niet zou kunnen verwezenlijken zonder de betreffende dienst.[30] Onder de VRPA zijn ook producenten van dit soort componenten (naast de fabrikant van het product waarin een en ander is geïntegreerd) risico-aansprakelijk als deze gebreken vertonen.[31]

Toelichting 2: Naast softwareproducenten kunnen onder de VRPA bijvoorbeeld ook de toeleveranciers van brondata aansprakelijk worden gesteld als de brondata leiden tot gebrekkige producten en schade. Daarbij kan onder andere gedacht worden aan leveranciers van databestanden, modellen en algoritmes om kredietwaardigheid of frauderisico's te voorspellen.[32] Ook "bijbehorende dienstverleners" worden risico-aansprakelijk. Dat zijn bijvoorbeeld de leveranciers van verkeersgegevens die nodig zijn voor het navigeren van zelfrijdende auto's, of de leveranciers van opslagdiensten die worden gebruikt voor het opslaan en bewerken van beeldmateriaal dat wordt geanalyseerd door autonome medische diagnostische software.

c. *Uitbreiding gebreksdefinitie*

Artikel 6 VRPA stelt, vergelijkbaar met de huidige regeling, dat een product geacht wordt gebreken te vertonen "wanneer het niet de veiligheid biedt die het grote publiek gerechtigd is te verwachten".[33] Vervolgens voegt de wetgever een heel aantal omstandigheden toe waarmee rekening moet worden gehouden bij het vaststellen van gebrekkigheid ten opzichte van de thans geldende definitie. De meest in het oog springende in verband met deze bijdrage zijn opgenomen in subs c tot en met f.

Sub c vermeldt het effect van zelflerend vermogen op het product nadat het in de handel is gebracht of in gebruik is gesteld. Gelezen in combinatie met sub d, dat ziet op het effect op andere producten[34], sub e, dat ziet op het moment waarop het product in de handel werd gebracht en rekening houdt met de mate waarin de producent ná dat moment nog zeggenschap hield over het product, en in samenhang bezien met nieuwe verplichtingen om bijvoorbeeld software na marktintroductie te voorzien van veiligheidsupdates, behelst dit een forse opdracht aan producenten om (AI-)producten "in het gareel" en veilig te houden nadat deze in het verkeer zijn gebracht.[35] Sub f vult nog aan dat "de productveiligheidsvoorschriften, met inbegrip van veiligheidsgerelateerde cyberbeveiligingsvoorschriften" ook kunnen worden meegewogen in dezen. Voldoen producenten niet aan de redelijke verwachtingen van het algemene publiek[36] (en wettelijke verplichtingen) op deze vlakken, kan dat leiden tot gebrekkigheid van hun producten in de zin van de VRPA.

Toelichting 3: Waar de verantwoordelijkheid van de producent onder de huidige regels vaak ophoudt na het in het verkeer brengen van een product, geldt onder het voorgestelde regime een voortdurende verplichting om bijvoorbeeld AI-algoritmes veilig te houden. Dit brengt mee,dat producenten zullen moeten voorkomen dat het zelflerende vermogen van de systemen die zij op de markt brengen, na verloop van tijd ertoe leidt dat de systemen onveilig raken, of kwetsbaar worden op het vlak van cyberbeveiliging. Doen zij dat niet, kan dat leiden tot een gebrek in de zin van de VRPA.
Hoe de "redelijke" verwachtingen van consumenten ten aanzien van AI-techniek moeten worden bepaald, is in algemene zin nog niet vast te stellen – althans niet op basis van de huidige VRPA-tekst. Die verwachtingen zijn daarmee vooralsnog open normen, die wel een grote impact kunnen hebben voor zowel consumenten als producenten. Bijvoorbeeld ten aanzien van zelfrijdende auto's zou je enerzijds kunnen betogen dat men mag verwachten dat die veiliger rijden dan de beste menselijke coureur[37] – terwijl je aan de andere kant ook zou kunnen stellen dat (zeker zolang de techniek nog in ontwikkeling is) de gemiddelde menselijke bestuurder als maatman genomen zou moeten worden[38], wat mijns inziens het absolute minimum zou moeten zijn.[39]

d. *Innovatoren die aansprakelijk kunnen worden gehouden: One-stop-shop*

Naast de fabrikant van gebrekkige producten moet een slachtoffer onder de VRPA onder andere ook de fabrikant van een defect component (waaronder dus ook digitale diensten) kunnen aanspreken, als dat een gebrek in het (eind)product tot gevolg heeft.[40] Is de fabrikant buiten de Unie gevestigd, kunnen de importeur en de gemachtigde van de fabrikant aansprakelijk worden gesteld.[41] Zo'n gemachtigde is de "in de Unie gevestigde natuurlijke of rechtspersoon die door een fabrikant is gemachtigd om namens hem specifieke taken te vervullen".[42] Is er geen importeur of gemachtigde in de EU te vinden, dan kan een slachtoffer zich ook wenden tot de "fulfilmentdienstverlener".[43] Dat is degene die op commerciële basis tenminste twee van de volgende diensten levert: "opslag, verpakking, adressering en verzending van een product"[44] – bepaalde postdiensten, pakketbezorgdiensten en vrachtvervoersdiensten uitgezonderd.

geleden in het *Krone Verlag* arrest vaststelde dat inaccurate medische informatie die was opgenomen in een krant, niet onder het productbegrip kan vallen als bedoeld in de (oude) richtlijn. Zie HvJEU 10 juni 2021, C-65/20, ECLI:EU:C:2021:471, r.o. 42.

27. Considerans 13.
28. Dat wil zeggen dat een fabrikant toestemming heeft gegeven voor hetzij de integratie, interconnectie of toelevering van een component door een derde, waaronder ook begrepen software-updates of -upgrades, of de wijziging van een product (lid 5).
29. Artikel 1 lid 3 VRPA.
30. Artikel 1 lid 4 VRPA.
31. Zie verder onderdeel d; artikel 7 lid 1 en ook considerans 26 VRPA.
32. Dit staat natuurlijk los van de vraag of dit soort functionaliteit überhaupt mag worden ingezet, waarover onder andere in de AI-verordening regels zullen worden gesteld, en waarop onder meer ook de Algemene Verordening Gegevensbescherming van toepassing zal zijn.
33. De referentie naar "het *grote publiek*" codificeert in feite de in de jurisprudentie vastgestelde regels: zie bijvoorbeeld HvJEU 5 maart 2015, gevoegde zaken C-503/14 en C-504/14 (*Boston Scientific Medizintechnik GMBH),* r.o. 37.
34. "waarvan redelijkerwijs kan worden verwacht dat zij in samenhang met het product worden gebruikt" (sub d).
35. Zie bijvoorbeeld ook de verplichtingen uit hoofde van Richtlijn 2019/770, betreffende bepaalde aspecten van overeenkomsten voor de levering van digitale inhoud en digitale diensten. In artikel 8 van die richtlijn wordt onder meer bepaald dat "veiligheid" van software een rol speelt bij het beoordelen van conformiteit (lid 1 sub b), en in lid 2 is geregeld dat een handelaar dient te zorgen voor "updates, waaronder beveiligingsupdates, die nodig zijn om de conformiteit van de digitale inhoud of de dienst te handhaven aan de consument worden gemeld en geleverd […]" gedurende een zekere periode. Zie bijvoorbeeld ook Verordening 2017/745, betreffende medische hulpmiddelen, waarin vergelijkbare verplichtingen worden opgelegd aan producenten van medische hulpmiddelen voor de gehele levenscyclus; considerans 38 VRPA, en natuurlijk de voorgestelde AI-verordening.
36. Artikel 6 lid 1 VRPA hanteert het "grote publiek" als maatman, maar lid 1 sub h verwijst daarentegen ook naar "de specifieke verwachtingen van de eindgebruikers voor wie het product is bestemd" als omstandigheid waarmee rekening moet worden gehouden.
37. Zie bijvoorbeeld M. Schellekens, "Self-driving cars and the chilling effect of liability law", *Computer Law & Security Review* 2015, vol. 31, p. 517.
38. Zie Erica Palmerini, Federico Azzarri, Fiorella Battaglia et al., D 6.2, "Guidelines on Regulating Robotics", 22 september 2014, p. 57.
39. Zie De Bruin 2022, p. 83 voor meer argumenten ter zake.
40. Artikel 7 lid 1 VRPA.
41. Lid 2.
42. Artikel 4 lid 12 VRPA.
43. Artikel 7 lid 3 VRPA.
44. Artikel 4 lid 14 VRPA.

Toelichting 4: De fulfilmentprovider zou bijvoorbeeld een partij kunnen zijn die producten niet onder eigen naam en op verzoek van een ander in het buitenland bestelt, (al dan niet in bulk) opslaat en na verkoop doet versturen aan consumenten zoals opslagbedrijven en expediteurs.

Kan er geen fabrikant, gemachtigde, importeur of fulfilmentdienstverlener worden gelokaliseerd binnen de Unie, dan kan een productaansprakelijkheidsclaim worden gericht aan "elke distributeur" indien die distributeur op verzoek van de eiser niet binnen een maand de identiteit van de verantwoordelijke marktdeelnemer of de betreffende toeleverancier onthult.[45]

Naast de distributeur geldt deze verplichting (en aansprakelijkheid) ook voor de "aanbieders van een onlineplatform[46] dat consumenten in staat stelt overeenkomsten op afstand met handelaren te sluiten en die geen fabrikant, importeur of distributeur zijn".[47]

Degene die een product dat reeds in omloop is gebracht, ingrijpend wijzigt, wordt onder de nieuwe richtlijn ook als fabrikant aangemerkt – mits de oorspronkelijke fabrikant daar geen controle over heeft.[48]

Toelichting 5: Gesteld dat een "robot-companion", die oorspronkelijk bedoeld was als gezelschap om mee te kletsen, na een bij de lokale programmeur gekochte, door hemzelf gefabriceerde "upgrade" wordt ingezet als algemene huishoudelijke hulp, een Chinese vaas uit de Ming-dynastie aanziet voor grofvuil, zou het gedupeerde slachtoffer verhaal kunnen halen bij de lokale programmeur die voor de modificatie heeft gezorgd.

Met de toevoeging van de fulfilmentdienstverlener, de "modifcator" en de aanbieders van onlineplatforms breidt de wetgever de "one-stop-shop" voor consumenten om een aansprakelijkheidsclaim aanhangig te maken aanzienlijk uit. Artikel 11 bepaalt dat alle relevante partijen hoofdelijk aansprakelijk kunnen worden gesteld; een eigen regresregeling kent de VRPA niet. Eigen schuld van de eiser kan leiden tot vermindering of uitsluiting van aansprakelijkheid – net als onder de huidige regeling.[49] Daarnaast is bepaald dat "de aansprakelijkheid van een marktdeelnemer niet wordt verminderd wanneer de schade zowel door de gebreken van een product als door handelen of nalaten van een derde [niet zijnde de eiser zelf, RWdB.] wordt veroorzaakt".[50] Volgens mij impliceert deze bepaling dat als de feitelijke causale relatie (tussen gebrek en opgetreden schade) vaststaat, dit in principe zou moeten leiden tot een volledige toerekening van de schade aan de fabrikant[51], zij het uiteraard dat de eigen schuld van het slachtoffer daarop in mindering kan worden gebracht.

Toelichting 6: Concreet zou deze regeling bijvoorbeeld betekenen dat indien een hacker zich toegang heeft verschaft tot de software of de daarmee verwerkte data, en die heeft gemanipuleerd waardoor er schade is ontstaan, de producent ook voor die schade aansprakelijk is – ongeacht of de producent heeft voldaan aan zijn verplichtingen om de producten na marktintroductie veilig te houden.[52]

e. Recht op schadevergoeding: nu ook corruptie van gegevens in scope

Onder de VRPA is de producent aansprakelijk jegens natuurlijke personen die schade lijden door een product met gebreken. In artikel 4 lid 6 worden drie categorieën "materiële verliezen" opgesomd die voor vergoeding in aanmerking komen. Ten eerste wordt gerefereerd aan schade ten gevolge van overlijden of lichamelijk letsel (nu expliciet met inbegrip van "medisch erkende geestelijke gezondheidsaandoeningen").[53] "Aantasting of vernietiging van goederen" wordt als tweede categorie genoemd. Uitgesloten zijn de schade aan het product zelf, producten die vanwege een defecte component zijn beschadigd en "goederen die uitsluitend beroepsmatig worden gebruikt".[54] Een novum is vervat in onderdeel c, dat bepaalt dat "verlies of corruptie van gegevens die niet uitsluitend beroepsmatig worden gebruikt" ook onder het schadebegrip zullen vallen.

Toelichting 7: Als een AI-systeem dat "in de cloud" draait en brongegevens verwerkt van een consument, bijvoorbeeld een collectie foto's of een verzameling van documenten, is de producent waarschijnlijk aansprakelijk voor het verloren gaan, of het ontoegankelijk raken van die informatie ten gevolge van een defect algoritme. Het is echter de vraag of dat principe uitzondering leidt op het moment dat een AI-algoritme wordt geïnstalleerd op/geladen in een eigen apparaat (telefoon, tablet, laptop, auto, et cetera) van een consument, en er vervolgens een gebrek ontstaat in het algoritme, waardoor het apparaat (en de daarmee verwerkte data/informatie) niet meer functioneert en vervangen moet worden.

f. Aansprakelijkheidsverweren: grenzen aan excepties bij AI-gerelateerde producten

Met het oog op een rechtvaardige risicoverdeling tussen consumenten en producenten[55], is er ook in de VRPA (artikel 10) een limitatieve lijst met excepties opgenomen. Naast de "gebruikelijke" en deels herkenbare

In art. 10 van de VRPA is een limitatieve lijst met excepties opgenomen.

45. Artikel 7 lid 5 VRPA.
46. In de zin van de voorgestelde EU Verordening inzake digitale diensten (COM/2020/825 final).
47. Artikel 7 lid 6 VRPA.
48. Artikel 7 lid 4. Daarbij moet het gaan om wijzigingen die "op grond van de toepasselijke [wettelijke] voorschriften […] als ingrijpend worden beschouwd".
49. Artikel 12 lid 2 VRPA.
50. Lid 1.
51. Een en ander voor zover de schade in redelijke verbinding staat met de oorzaak in de zin van 6:98 BW.
52. Zie ook considerans 41 VRPA.
53. Sub a.
54. Sub b.
55. Zie considerans 24.

Bewijslast voor aantonen van defect, schade en causaliteit blijft rusten op de schouders van het slachtoffer.

verweermiddelen[56], kan de producent weliswaar een beroep doen op een exceptie indien een gebrek na marktintroductie is ontstaan[57], maar *niet* als : a) het gebrek wordt veroorzaakt door een bijbehorende dienst, waarover de fabrikant zeggenschap heeft; b) het gebrek is te wijten aan software, en updates of upgrades daarvan waarover de fabrikant zeggenschap heeft; of c) het gebrek is ontstaan door het ontbreken van software-updates of -upgrades die nodig zijn om de veiligheid te handhaven – een en ander eveneens voor zover de fabrikant daar zeggenschap over heeft.

In datzelfde licht moet het aangescherpte ontwikkelingsricoverweer worden bezien.[58] Producenten kunnen zich van een claim bevrijden indien ze kunnen aantonen[59] dat 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 hij de zeggenschap over het product had*, [cursivering RWdB] niet mogelijk was de gebreken te ontdekken.

> *Toelichting 8: Zet men deze uitzonderingen op de aansprakelijkheidsexceptie naast de aangescherpte gebreksdefinitie en de (cyber)beveiligingsverplichtingen uit deze en aanpalende Unieregelingen, moge duidelijk zijn dat de zorgplichten van (AI-)producenten veel verder zullen reiken dan voorheen. Kort en goed: AI-producenten die hun producten niet veilig en/of functioneel houden terwijl ze daartoe wel gehouden zijn, hetzij op grond van wettelijke voorschriften, hetzij op grond van de redelijke verwachtingen van het grote publiek, riskeren dat hun product als gebrekkig wordt aangemerkt, en kunnen zich niet exonereren door te stellen en aan te tonen dat men het gebrek niet kende op het moment van marktintroductie. Dat brengt mee dat, wil men zelflerende, autonome systemen exploiteren, er zeer zorgvuldig moet worden toegezien op de al dan niet door het systeem zelf geïnitieerde ontwikkelingen daarvan. Een verweer van de producent dat hij het gebrek in kwestie niet kende, zal hem achteraf vaak niet bevrijden als hij het gebrek had kunnen kennen, voorkomen of repareren.*

g. *Procedurele hulpmiddelen voor slachtoffers*

De bewijslast voor het aantonen van een defect, schade en causaliteit blijft onder de VRPA rusten op de schouders van de slachtoffers[60], om zodoende "een rechtvaardige verdeling van risico's te verwezenlijken".[61] De Uniewetgever komt echter de eisende partijen stevig tegemoet – en dat is ook hoognodig: het zal voor slachtoffers meestal lastig zijn om een gebrek aan te tonen in zelflerende AI-producten, en de causale relatie tussen gebrek en schade.[62] Dat komt mede doordat AI-technologie per definitie complex is, vaak samenhangt met andere technologie, waarbij gebruik wordt gemaakt van grote hoeveelheden data, en ook nog eens zichzelf in de loop van de tijd kan aanpassen vanwege het zelflerende karakter. Toegang tot, en de mogelijkheden omtrent analyse van de programmatuur, de logica van de beslissende algoritmes en de verwerkte data zullen slachtoffers voor de nodige uitdagingen plaatsen om bewijs te kunnen leveren van een gebrek in een AI-product.[63] Waar verschillende factoren een rol zouden kunnen spelen bij de totstandkoming van schade waarbij ook AI betrokken is, zal vaak ook de causaliteitspuzzel lastig te leggen zijn. Omdat deze causaliteit in principe een binair concept is (verankerd door de conditio sine qua non toetssteen) en het bij samenkomende omstandigheden waarbij AI betrokken is, vaak gecompliceerd zal zijn om zekerheid te krijgen over welke factor nu precies de schade heeft veroorzaakt, zal het ingewikkeld blijken om causaliteit vast te stellen – en dus om productaansprakelijkheid te kunnen vestigen.

De Uniewetgever komt eisers op twee manieren tegemoet. Enerzijds wordt er een regeling voorgesteld om toegang te verkrijgen tot bewijsmateriaal[64], en anderzijds moeten nationale rechters met bewijsvermoedens werken onder bepaalde omstandigheden waarin het moeilijk is voor slachtoffers om het bewijs rond te krijgen.[65] Wat betreft de toegang tot bewijsmateriaal wordt in artikel 8 VRPA geregeld dat de nationale rechter een producent kan gelasten om "het relevante bewijsmateriaal waarover hij beschikt openbaar te maken"[66] – althans aan de eisende partij. Daarvoor is het wel nodig dat de eiser "feiten en bewijsmateriaal heeft overgelegd die volstaan om de schadevergoeding aannemelijk te maken". Het maakt niet uit of de verweerder het materiaal reeds heeft. Deze verplichting ziet ook op "documenten [...] die de verweerder ex novo moet vervaardigen door het beschikbare bewijsmateriaal te compileren of te rubriceren".[67] Komt de producent in kwestie niet over de brug met het betreffende materiaal, leidt dit tot het bewijsvermoeden dat er sprake was van een gebrek in zijn product.[68] De verplichting tot overlegging van bewijsmateriaal geldt niet onverkort. Zo moet er een proportionaliteitstoets en een subsidiariteitstoets worden uitgevoerd.[69] Daarbij moet er ook rekening worden gehouden met de "gerechtvaardigde belangen van alle partijen, met inbegrip van die van betrokken derden, met name wat bescherming van vertrouwelijke informatie en bedrijfsgeheimen"[70] betreft, in de zin van de Unierichtlijn inzake de bescherming van bedrijfsgeheimen.[71] Dit betekent niet dat als er sprake is van bedrijfsgeheime

56. Onder andere in stelling te brengen door fabrikanten, importeurs, distributeurs of modificatoren die de betreffende (onderdelen van) producten niet op de markt hebben gebracht, respectievelijk in de handel gebracht, in gebruik gesteld of op de markt aangeboden dan wel hebben gewijzigd (artikel 10 lid 1 sub a-b en g); of indien het gebrek het gevolg was van dwingende overheidsvoorschriften (sub d); dan wel de expliciete instructies van de fabrikant, gericht aan de componentenproducent of het ontwerp van het product waarin de component is geïntegreerd (sub f).
57. Artikel 10 lid 1 sub c VRPA.
58. Artikel 10 lid 1 sub e VRPA.
59. In de huidige regeling hoeven producenten doorgaans slechts "aannemelijk te maken" dat er een exceptie van toepassing is, ook hier lijken de duimschroeven te worden aangedraaid.
60. Artikel 9 lid 1 VRPA.
61. Considerans 30 VRPA.
62. Zie De Bruin 2022, hoofdstuk 6.2.2.2 en 6.2.2.3, en in dit blad De Bruin 2022, p. 11-12.
63. Dit wordt onderkend door de wetgever, zie bijvoorbeeld considerans 30 VRPA.
64. Zie voor een uitgebreidere reflectie hieromtrent ook K.A.P.C. van Wees & N.E. Vellinga, "Voorstel nieuwe richtlijn productaansprakelijkheid. Naar een toekomstbestendig aansprakelijkheidsrecht", in deze aflevering (zie *VR* 2023/79).
65. Zie wederom Van Wees & Vellinga in deze aflevering (zie *VR* 2023/79) – die overigens kritischer zijn dan ik ten aanzien van de betekenis van deze vermoedens voor slachtoffers.
66. Artikel 8 lid 1 VRPA.
67. Considerans 31 VRPA.
68. Artikel 9 lid 2 sub a VRPA.
69. Artikel 8 lid 2 VRPA.
70. Lid 3.
71. Richtlijn 2016/943, in Nederland geïmplementeerd in de Wet bescherming bedrijfsgeheimen.

informatie, deze nooit kan worden gebruikt in een procedure, maar wel dat een rechter specifieke maatregelen kan nemen om de "vertrouwelijkheid van de informatie te eerbiedigen".[72]

Toelichting 9: Stel dat een autonoom, zelflerend pathologie-algoritme bepaald celmateriaal ten onrechte niet heeft gekwalificeerd als tumorweefsel, waardoor de betreffende patiënt een bepaalde behandeling die mogelijk levensreddend zou zijn geweest niet aangeboden heeft gekregen – doordat er mogelijk een fout is geslopen in het beoordelingsmechanisme. Voor een succesvolle productaansprakelijkheidsclaim moet onder andere worden vastgesteld dat er sprake was van een gebrek in het algoritme, en een oorzakelijk verband tussen dat gebrek en de ontstane schade. Daarvoor is het nodig dat de eiser toegang verkrijgt tot de beslismethodiek om het aangeboden weefsel mee te beoordelen. Deze bevindt zich doorgaans onder de (software-)producent. Als deze op verzoek van de eiser de betreffende beslismethodiek (i.e. de algoritmes), de (zelflerende) ontwikkeling daarvan en de toepassing in de concrete situatie niet inzichtelijk maakt voor de eiser, kan de rechter de producent daartoe veroordelen onder de voorgestelde regels. Mocht de producent in kwestie menen dat daardoor bedrijfsgeheime informatie zou moeten worden prijsgegeven, kan de rechter bijvoorbeeld bepalen dat bepaalde delen van de informatie onleesbaar worden gemaakt, of dat het gebruik van de informatie in de rechtszaak beperkt blijft tot een kleine kring van personen, en dat deze informatie geen onderdeel wordt van een eventueel openbaar vonnis.

Met de toegang tot het relevante bewijsmateriaal is een eiser al een heel eind op weg, maar, zeker waar het AI-technologie betreft, zijn daarmee nog niet alle hobbels genomen. De informatie zal nog moeten worden geanalyseerd en geduid om onder meer defect en causaliteit te kunnen onderbouwen. Wat betreft het bewijzen van een gebrek schiet de wetgever de eisende partij op twee specifieke manieren te hulp (naast de hierboven reeds genoemde) en één generieke. Zo wordt een product geacht gebreken te vertonen wanneer de eiser aantoont dat het product in kwestie niet voldeed aan specifieke dwingende veiligheidsvoorschriften "die bedoeld zijn om bescherming te bieden tegen het risico van de voorgevallen schade".[73] Een gebreksvermoeden wordt ook aangenomen als de eiser aantoont dat de schade optrad "door een kennelijk disfunctioneren van het product bij normaal gebruik of onder normale omstandigheden".[74]

Toelichting 10: Stel dat de robot-companion uit toelichting 5 ineens en zonder specifieke aanleiding op tilt slaat, en het bezoek van zijn eigenaar een klap verkoopt, zal dit denkelijk te kwalificeren zijn als "kennelijk disfunctioneren bij normaal gebruik". Ook zal een gebrek kunnen worden vermoed als een zelfrijdende auto in strijd met (toekomstige) specifieke wettelijke veiligheidsvoorschriften onvoldoende afstand houdt, en na abrupt remmen botst op diens voorganger.

Causaliteit tussen gebrek en schade wordt op grond van artikel 9 lid 3 VRPA aannemelijk geacht als er een gebrek is vastgesteld, en "de soort veroorzaakte schade doorgaans strookt met het betrokken gebrek".

Toelichting 11: Stel dat bij de botsing uit het vorige voorbeeld ook nog andere omstandigheden een rol speelden, zoals dichte mist en een glad wegdek, zal causaliteit desalniettemin mogen worden aangenomen als kan worden aangetoond dat schade ten gevolge van de opgetreden kop-staart-aanrijding een typisch resultaat is van "gebrekkig" onvoldoende afstand houden.

Naast deze specifieke bewijsvermoedens geeft de Uniewetgever nog een algemeen bewijsvermoeden dat als vangnet kan gaan functioneren. In artikel 9 lid 4 wordt de opdracht verstrekt aan de nationale rechter om de eiser tegemoet te komen. Dat moet als hij oordeelt dat het "vanwege de technische of wetenschappelijke complexiteit voor de eiser buitensporig moeilijk is om de gebreken van het product en/of het oorzakelijk verband […]" te bewijzen. In die gevallen moet de rechter het gebrek en/of de causale relatie aannemen als er voldoende bewijs is van a) het feit dat het "product heeft bijgedragen tot de schade", en "b) het waarschijnlijk is dat het product gebreken vertoonde en/of dat de gebreken ervan een waarschijnlijke oorzaak van de schade zijn". Overigens heeft de verweerder het recht om de aangevoerde buitensporige moeilijkheden, de genoemde waarschijnlijkheid en de overigens vastgestelde bewijsvermoedens te betwisten respectievelijk te weerleggen.[75]

Toelichting 12: Stel, de benodigde informatie aangaande het pathologie-algoritme uit toelichting 9 wordt verstrekt aan de eiser, maar het doorgronden daarvan zou een zeer langdurige, tijdrovende en dure exercitie betekenen vanwege de omvang en complexe aard. Als de eiser kan aantonen dat het algoritme heeft bijgedragen aan de beslissing om niet te behandelen, waardoor er schade is opgetreden die te vermijden was geweest (ik laat de rol en verantwoordelijkheid van de arts in kwestie hier bewust verder buiten beschouwing), en dat het waarschijnlijk is dat er een "bug" is geslopen in het beoordelingsalgoritme, zou de rechter een vermoeden van zowel gebrekkigheid als causaliteit moeten aannemen.

Naast specifieke bewijsvermoedens geeft de Uniewetgever nog een algemeen bewijsvermoeden dat als vangnet kan gaan functioneren.

72. Lid 4, en zie ook considerans 32, waar een aantal mogelijke maatregelen wordt gegeven.
73. Artikel 9 lid 2 sub b VRPA.
74. Sub c.
75. Lid 4, laatste zin; lid 5.

Wat de nieuwe regeling nóg mooier zou maken, is het treffen van een passende regeling inzake de verwerking van persoonsgegevens.

3. Alle problemen opgelost?

De voorgestelde regels impliceren mijns inziens een wezenlijke verbetering voor slachtoffers van AI-gerelateerde ongelukken ten opzichte van het huidige regime. Het uitbreiden van het productbegrip waardoor (AI-)software expliciet binnen het toepassingsbereik komt en het stelsel van nieuwe verplichtingen aangaande de duurzame overeenstemming met geldende normen van de betreffende producten, zullen mogelijk bijdragen aan het vertrouwen van consumenten dat AI-systemen veilig zijn en blijven.[76] Daarnaast betekenen de voorgestelde verplichtingen ten aanzien van het beschikbaar stellen van bewijs aan eisers en zeker ook de bewijsvermoedens van gebrekkigheid en causaliteit krachtige procedurele middelen dat het makkelijker wordt dan nu het geval is om met succes een productaansprakelijkheidsclaim in stelling te brengen. In combinatie met het beperken van de verweermiddelen van producenten die de gelegenheid hadden om hun producten na marktintroductie veilig te houden (maar dat desalniettemin nalieten), lost het nieuwe stelsel een heel aantal van de problemen die ik eerder in dit blad en in mijn proefschrift aan de orde stelde, op.[77] Het risico dat consumenten blijven zitten met hun schade, zal waarschijnlijk aanzienlijk afnemen.[78]

Tegelijkertijd behelst het voorgestelde regime weliswaar op bepaalde punten voor innovatoren een vooruitgang (de rechtszekerheid[79] is gediend met een heldere en toekomstbestendig flexibele[80] bepaling dat AI-(software) onder de richtlijn valt, en welke factoren kunnen worden meegewogen bij het beoordelen van gebrekkigheid, en dat geldt ook voor de verheldering en uitbreiding van de procedurele middelen die slachtoffers ten dienste staan), maar er kleven ook ogenschijnlijke nadelen aan. In praktijk zullen de nieuwe regels dus waarschijnlijk sneller leiden tot productaansprakelijkheid van innovatoren. Dat betekent dat de financiële lasten dienaangaande zullen toenemen.[81] Het bezwaar van producenten dat het voorgestelde raamwerk daardoor tot "chilling effects"[82] voor innovatie zal leiden, laat zich gemakkelijk raden. Het is natuurlijk niet ondenkbaar dat groeiende financiële risico's door strenger (en helderder) wordende regels voor sommige producenten een hobbel betekenen om te kunnen investeren in AI-innovatie. Aan de andere kant is het van belang om uiteindelijke schade eerlijk te verdelen tussen innovatoren en consumenten, en is het mijns inziens zo dat de VRPA de risico's belegt bij de partijen (de innovatoren) die deze in beginsel een stuk beter kunnen beheersen dan de slachtoffers. Daarbij geldt ook dat als men *niets* zou wijzigen aan het geldende productaansprakelijkheidsregime, en slachtoffers derhalve hun schade niet of nauwelijks kunnen verhalen, dit kan leiden tot een afname in het vertrouwen in AI-technologie. A contrario, het regelen van een gemakkelijker schadeverhaal zou wellicht kunnen leiden tot groter consumentenvertrouwen en omarming van AI-technologie.

Wat de nieuwe regeling nóg mooier zou maken, is het treffen van een passende regeling inzake de verwerking van persoonsgegevens. Zeker nu de wetgever kiest voor een systeem waarbij producenten geacht worden om bewijsmateriaal te bewaren, waar nodig te construeren en over te leggen aan eisende partijen, moet men zich rekenschap geven van het feit dat er daarmee op grote schaal persoonsgegevens zullen worden verwerkt.[83] Waar in de AI-verordening op enkele punten specifiek aandacht wordt besteed aan de relatie met de Algemene Verordening Gegevensbescherming[84], ontbreekt die in de VRPA ten enenmale. Ik zou verwachten dat de wetgever tenminste verduidelijkt dat de verplichtingen meebrengen dat persoonsgegevens verwerkt mogen c.q. moeten worden, en dat daarvoor een grondslag wordt gecreëerd alsmede, voor zover het bijzondere persoonsgegevens betreft, een uitzondering wordt gemaakt op het principeverbod om dat soort gegevens te verwerken.

76. Dit relateert aan de factor *trust* (i.e. vertrouwen), die samen met *risk* het consumentenperspectief van het in mijn proefschrift ontwikkelde toetsingskader vormen: De Bruin 2022, hoofdstuk 3.4.3. Ik denk dat dat vertrouwen zal toenemen onder de voorgestelde regels, ten opzichte van de huidige.
77. Zie De Bruin 2022, hoofdstuk 7.2; en in dit blad De Bruin 2022, p. 11-14.
78. Zie voor de factor *risk* (i.e. risico) hoofdstuk 3.4.3.2 van het hiervoor aangehaalde proefschrift.
79. Ibidem, hoofdstuk 3.4.2 aangaande het innovatorenperspectief, en meer met name *legal certainty* (rechtszekerheid), onderdeel 3.4.2.2.
80. Ibidem, onderdeel 3.4.2.4 aangaande *flexibility*.
81. Dit is van invloed op de factor *stringency* (onderdeel 3.4.2.3), die zal toenemen.
82. Zie bijvoorbeeld M. Schellekens., "Self-driving cars and the chilling effect of liability law", *Computer Law & Security Review* 2015, vol. 31, pp. 506-517.
83. Zie De Bruin 2022, hoofdstuk 5.
84. Zie bijvoorbeeld artikel 10 lid 5 AI-verordening.