EUROPESE
COMMISSIE

Brussel, 19.2.2020
COM(2020) 64 final

VERSLAG VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT, DE RAAD EN HET EUROPEES ECONOMISCH EN SOCIAAL COMITÉ

Verslag over de gevolgen van kunstmatige intelligentie, het internet der dingen en robotica op het gebied van veiligheid en aansprakelijkheid

VERSLAG OVER DE GEVOLGEN VAN KUNSTMATIGE INTELLIGENTIE, HET INTERNET DER DINGEN EN ROBOTICA OP HET GEBIED VAN VEILIGHEID EN AANSPRAKELIJKHEID

1. Inleiding

Kunstmatige intelligentie (KI)[1], het internet der dingen (IoT)[2] en robotica scheppen nieuwe kansen en voordelen voor onze samenleving. De Commissie erkent het belang en het potentieel van deze technologieën en de noodzaak om aanzienlijke investeringen te doen op deze gebieden[3]. Zij is vastbesloten om van Europa een wereldleider te maken op het gebied van KI, IoT en robotica. Willen we dit doel bereiken, dan is een duidelijk en voorspelbaar rechtskader vereist om de technologische uitdagingen aan te pakken.

1.1. Bestaand kader voor veiligheid en aansprakelijkheid

Het algemene doel van de rechtskaders inzake veiligheid en aansprakelijkheid is ervoor te zorgen dat alle producten en diensten, ook die waarin opkomende digitale technologieën zijn geïntegreerd, veilig, betrouwbaar en consistent werken en dat eventuele schade efficiënt wordt vergoed. Een hoog niveau van veiligheid voor producten en systemen waarin nieuwe digitale technologieën zijn geïntegreerd, en robuuste mechanismen voor het vergoeden van schade (d.w.z. het aansprakelijkheidskader) dragen bij tot een betere bescherming van de consument. Ook wordt daardoor vertrouwen gewekt in deze technologieën, wat een voorwaarde is voor de aanvaarding ervan door bedrijven en gebruikers. Dit zal dan weer het concurrentievermogen van onze industrie versterken en bijdragen tot de verwezenlijking van de doelstellingen van de Unie[4]. Een duidelijk kader voor veiligheid en aansprakelijkheid is met name van belang wanneer nieuwe technologieën zoals KI, IoT en robotica ontstaan, zowel voor de bescherming van de consument als voor de rechtszekerheid voor bedrijven.

De Unie beschikt over een robuust en betrouwbaar regelgevingskader voor veiligheid en productaansprakelijkheid en een robuust stelsel van veiligheidsnormen, aangevuld door nationale, niet-geharmoniseerde aansprakelijkheidswetgeving. Samen garanderen deze het welzijn van onze burgers op de eengemaakte markt en moedigen zij innovatie en technologische acceptatie aan. KI, IoT en robotica leiden er echter toe dat de kenmerken van veel producten en diensten veranderen.

In de mededeling "Kunstmatige intelligentie voor Europa"[5] , die op 25 april 2018 is aangenomen, meldt de Commissie dat zij een verslag zal indienen met een beoordeling van

---

1 De deskundigengroep op hoog niveau (AI HLEG) heeft een definitie van kunstmatige intelligentie opgesteld, die te vinden is op https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines.

2 Een definitie van het internet der dingen is te vinden in de aanbeveling van ITU-T Y.2060, die beschikbaar is op https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060.

3 SWD(2016) 110, COM(2017) 9, COM(2018) 237 en COM(2018) 795.

4 https://ec.europa.eu/growth/industry/policy_nl

5 https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:52018DC0237
In het begeleidende werkdocument van de diensten van de Commissie SWD(2018) 137 (https://eur-lex.europa.eu/legal-content/nl/ALL/?uri=CELEX:52018SC0137) is een eerste overzicht gegeven van de aansprakelijkheidsproblemen die zich voordoen in verband met opkomende digitale technologieën.

de implicaties van de opkomende digitale technologieën voor de bestaande kaders inzake veiligheid en aansprakelijkheid. Dit verslag benoemt en beschrijft de bredere gevolgen voor en potentiële lacunes in die kaders op het gebied van KI, IoT en robotica. De oriëntaties die in dit verslag bij het witboek over kunstmatige intelligentie zijn opgenomen, dienen als input voor discussie en maken deel uit van het bredere proces van de raadpleging van belanghebbenden. Het deel over veiligheid is gebaseerd op de evaluatie[6] van de machinerichtlijn[7] en de werkzaamheden in verband met de desbetreffende deskundigengroepen[8]. Het deel over aansprakelijkheid is gebaseerd op de evaluatie[9] van de richtlijn productaansprakelijkheid[10], de input van de relevante deskundigengroepen[11] en de contacten met belanghebbenden. Het is niet de bedoeling om met dit verslag een volledig overzicht te geven van de bestaande regelgeving inzake veiligheid en aansprakelijkheid, maar wel om aandacht te geven aan de belangrijkste problemen die tot nu toe zijn vastgesteld.

1.2. Eigenschappen van technologieën op het gebied van KI, IoT en robotica

KI, IoT en robotica hebben veel eigenschappen gemeen. Zij kunnen **connectiviteit**, **autonomie** en **data-afhankelijkheid** combineren en zo taken uitvoeren met weinig of geen menselijke controle of supervisie. Met KI uitgeruste systemen kunnen ook hun eigen prestaties verbeteren door te leren van hun ervaringen. Hun **complexiteit** wordt weerspiegeld in zowel de veelheid aan economische actoren die betrokken zijn bij de **toeleveringsketen** als de veelheid aan componenten, onderdelen, software, systemen en diensten die samen de nieuwe technologische ecosystemen vormen. Daarbij komt ook nog het feit dat producten die reeds op de markt zijn gebracht, **openstaan voor updates en upgrades**. De enorme hoeveelheden gegevens, de afhankelijkheid van algoritmen en het **gebrek aan transparantie** waarmee beslissingen bij KI tot stand komen, maken het moeilijker om het gedrag van een met KI uitgerust product te voorspellen en inzicht te krijgen in de mogelijke oorzaken van schade. Tot slot kunnen connectiviteit en openheid er ook toe leiden dat KI- en IoT-producten aan **cyberdreigingen** blootstaan.

---

6 SWD(2018) 161 final.

7 Richtlijn 2006/42/EG.

8 Consumer Safety Network, opgezet krachtens Richtlijn 2001/95/EG inzake algemene productveiligheid, Richtlijn 2006/42/EG betreffende machines en Richtlijn 2014/53/EU betreffende radioapparatuur, groepen van deskundigen uit de lidstaten, het bedrijfsleven en andere belanghebbenden, zoals consumentenorganisaties.

9 COM(2018) 246 final.

10 Richtlijn 85/374/EEG.

11 De deskundigengroep inzake aansprakelijkheid en nieuwe technologieën is opgericht om de Commissie expertise te verschaffen over de toepasselijkheid van de richtlijn productaansprakelijkheid en de nationale regelgeving op het gebied van wettelijke aansprakelijkheid, en haar te ondersteunen bij de ontwikkeling van richtsnoeren voor mogelijke aanpassingen van de toepasselijke wetgeving in verband met nieuwe technologieën. De deskundigengroep kent twee formaties, namelijk de formatie productaansprakelijkheid en de formatie nieuwe technologieën; zie ook: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3592&Lang=NL.
Zie voor het verslag van de formatie nieuwe technologieën over aansprakelijkheid voor kunstmatige intelligentie en andere opkomende technologieën: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199.

1.3. Kansen die worden geboden door KI, IoT en robotica

Versterking van het vertrouwen van gebruikers in en de maatschappelijke acceptatie van opkomende technologieën, verbetering van producten, processen en bedrijfsmodellen en ondersteuning van het streven van Europese fabrikanten naar grotere efficiëntie zijn slechts enkele van de mogelijkheden die KI, IoT en robotica kunnen bieden.

Naast productiviteits- en efficiëntiewinst belooft KI mensen in staat te stellen een hoger intelligentieniveau te bereiken, de weg te banen voor nieuwe ontdekkingen en enkele van de grootste uitdagingen van de wereld op te lossen, van het behandelen van chronische ziekten, het voorspellen van de uitbraak van ziekten en het terugdringen van het aantal verkeersdoden tot het bestrijden van klimaatverandering en het anticiperen op cyberdreigingen.

Deze technologieën kunnen vele voordelen opleveren door de veiligheid van producten te verbeteren, waardoor deze minder gevoelig worden voor bepaalde risico's. Geconnecteerde en geautomatiseerde voertuigen zouden bijvoorbeeld de verkeersveiligheid kunnen verhogen, aangezien de meeste verkeersongevallen momenteel het gevolg zijn van menselijke fouten[12]. IoT-systemen zijn bovendien ontworpen om grote hoeveelheden gegevens uit verschillende bronnen te ontvangen en te verwerken. Dit verhoogde informatieniveau kan worden gebruikt om ervoor te zorgen dat de producten zichzelf kunnen aanpassen en daardoor veiliger kunnen worden. Nieuwe technologieën kunnen bijdragen tot doeltreffender terugroepacties, aangezien producten de gebruiker bijvoorbeeld kunnen waarschuwen dat er een veiligheidsprobleem is[13]. Als zich een veiligheidsprobleem voordoet bij het gebruik van een geconnecteerd product, kan de producent rechtstreeks met de gebruikers communiceren, enerzijds om hen te waarschuwen voor de risico's en anderzijds om, als dat kan, het probleem rechtstreeks te verhelpen door bijvoorbeeld een veiligheidsupdate aan te bieden. Zo heeft een producent van smartphones bij het terugroepen van een van zijn apparaten in 2017 een software-update uitgevoerd om de batterijcapaciteit van de teruggeroepen telefoons tot nul te reduceren[14], zodat de gebruikers de gevaarlijke apparaten niet langer konden gebruiken.

Daarnaast kunnen nieuwe technologieën de traceerbaarheid van producten helpen verbeteren. Zo kan de connectiviteitsfunctie van IoT-producten bedrijven en markttoezichtautoriteiten in staat stellen gevaarlijke producten te traceren en risico's in alle toeleveringsketens vast te stellen[15].

Naast de kansen die KI, IoT en robotica kunnen bieden voor de economie en de samenleving, bestaat er ook een risico dat wettelijk beschermde (materiële en immateriële) belangen schade wordt toegebracht. Het risico dat dergelijke schade zich voordoet, zal toenemen naarmate het aantal toepassingen stijgt. Het is dan ook essentieel om na te gaan of en in hoeverre het

---

[12] Volgens ramingen wordt ca. 90% van de verkeersongevallen veroorzaakt door menselijke fouten. Zie het verslag van de Commissie "Mensenlevens redden: Verbeteren van de veiligheid van voertuigen in de EU", COM(2016) 787 final.

[13] De bestuurder van een auto kan bijvoorbeeld worden gewaarschuwd dat hij moet vertragen omdat er verderop een ongeluk is gebeurd.

[14] OESO (2018), "Measuring and maximising the impact of product recalls globally: OECD workshop report", *OECD Science, Technology and Industry Policy Papers*, No. 56, OECD Publishing, Paris, https://doi.org/10.1787/ab757416-en.

[15] OESO (2018), "Enhancing product recall effectiveness globally: OECD background report", *OECD Science, Technology and Industry Policy Papers*, No. 58, OECD Publishing, Paris, https://doi.org/10.1787/ef71935c-en.

huidige rechtskader inzake veiligheid en aansprakelijkheid nog geschikt is om de gebruikers te beschermen.

2. Veiligheid

In de mededeling van de Commissie "Vertrouwen kweken in mensgerichte kunstmatige intelligentie" wordt gesteld dat ***in KI-systemen mechanismen voor veiligheid en beveiliging door ontwerp [moeten] worden geïntegreerd om ervoor te zorgen dat ze bij elke stap aantoonbaar veilig zijn***, *met oog voor de* ***fysieke en mentale veiligheid*** *van alle betrokkenen*[16].

Bij de beoordeling van de EU-wetgeving inzake productveiligheid in dit deel wordt bekeken of het huidige wetgevingskader van de Unie de nodige elementen bevat die ervoor kunnen zorgen dat bij opkomende technologieën, en in KI-systemen in het bijzonder, veiligheid en beveiliging door ontwerp zijn geïntegreerd.

Dit verslag kijkt met name naar de richtlijn algemene productveiligheid[17]en de geharmoniseerde productwetgeving die voortvloeit uit de horizontale regels van de "nieuwe aanpak"[18] en/of het "nieuwe wetgevingskader" (hierna Uniewetgeving of Uniekader voor productveiligheid genoemd)[19]. De horizontale regels zorgen voor de samenhang tussen de sectorale voorschriften inzake productveiligheid.

De Uniewetgeving inzake productveiligheid moet ervoor zorgen dat producten die in de Unie in de handel worden gebracht, voldoen aan strenge gezondheids-, veiligheids- en milieueisen en dat dergelijke producten vrij kunnen circuleren in de hele Unie. De sectorale wetgeving[20] wordt aangevuld door de richtlijn algemene productveiligheid[21], die voorschrijft dat alle consumentenproducten veilig moeten zijn, ook als zij niet onder de sectorale wetgeving van de Unie vallen. Naast de veiligheidsvoorschriften wordt markttoezicht gehouden en zijn bevoegdheden verleend aan de nationale autoriteiten op grond van de verordening inzake markttoezicht[22] en de richtlijn algemene productveiligheid[23]. Op het gebied van vervoer gelden er aanvullende Unievoorschriften en nationale voorschriften voor het in gebruik

---

16 Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's: Vertrouwen kweken in mensgerichte kunstmatige intelligentie, Brussel 8.4.2019 (COM(2019) 168 final).

17 Richtlijn 2001/95/EG van het Europees Parlement en de Raad van 3 december 2001 inzake algemene productveiligheid (PB L 11 van 15.1.2002, blz. 4).

18 PB C 136 van 4.6.1985, blz. 1.

19 Verordening (EG) nr. 2008/765 en Besluit nr. 768/2008/EG.

20 Deze regeling omvat niet de Uniewetgeving inzake vervoer en automobielen.

21 Richtlijn 2001/95/EG van het Europees Parlement en de Raad van 3 december 2001 inzake algemene productveiligheid (PB L 11 van 15.1.2002, blz. 4).

22 Verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad van 9 juli 2008 tot vaststelling van de eisen inzake accreditatie en markttoezicht betreffende het verhandelen van producten en tot intrekking van Verordening (EEG) nr. 339/93 (PB L 218 van 13.8.2008, blz. 30, ELI: https://eur-lex.europa.eu/eli/reg/2008/765/oj), en vanaf 2021 Verordening (EU) 2019/1020 van het Europees Parlement en de Raad van 20 juni 2019 betreffende markttoezicht en conformiteit van producten en tot wijziging van Richtlijn 2004/42/EG en de Verordeningen (EG) nr. 765/2008 en (EU) nr. 305/2011 (PB L 169 van 25 juni 2019, blz. 1, ELI: https://eur-lex.europa.eu/eli/reg/2019/1020/oj)

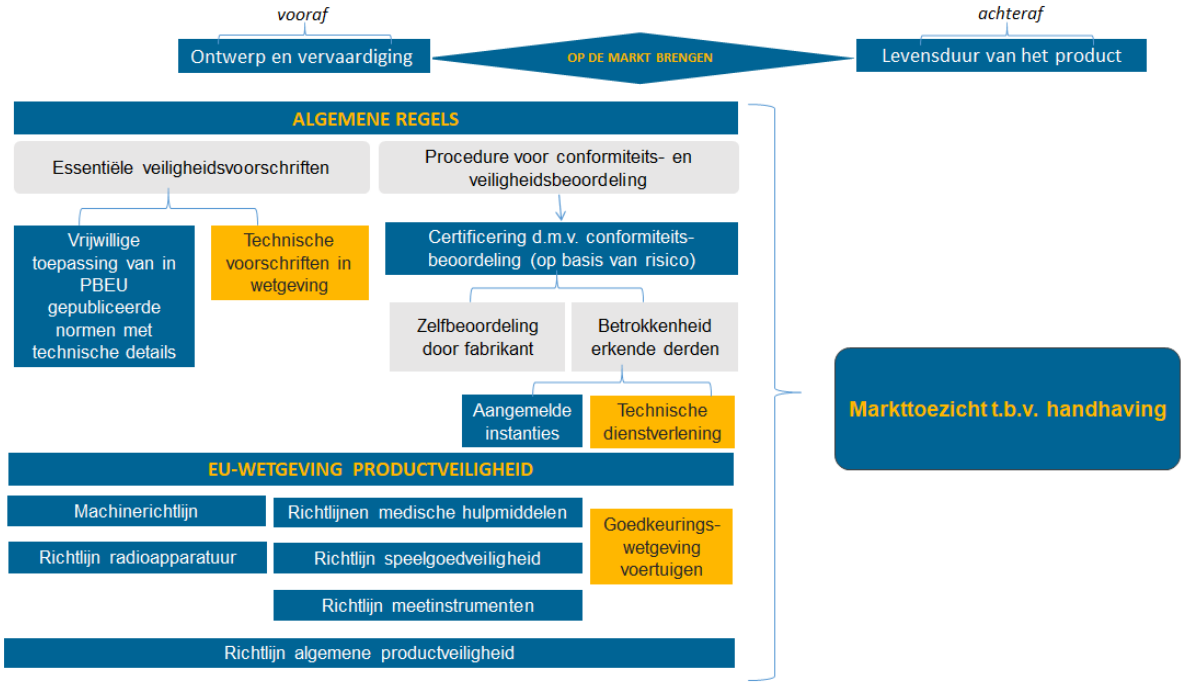
23 Artikel 8, lid 1, onder b), en lid 3, van de richtlijn algemene productveiligheid.

nemen van een motorvoertuig[24], een luchtvaartuig of een schip en duidelijke voorschriften inzake de veiligheid tijdens het gebruik, met inbegrip van de taken van de gebruiker en de toezichttaken van de autoriteiten.

Ook normalisatie op Europees niveau is een wezenlijk onderdeel van de wetgeving inzake productveiligheid van de Unie. Gezien de mondiale aard van de digitalisering en de opkomende digitale technologieën is internationale samenwerking op het gebied van normalisatie van bijzonder belang voor het concurrentievermogen van de Europese industrie.

Een groot deel van het productveiligheidskader van de Unie is opgesteld vóór de opkomst van digitale technologieën zoals KI, IoT of robotica. Het bevat daarom niet altijd bepalingen die uitdrukkelijk ingaan op de nieuwe uitdagingen en risico's van deze opkomende technologieën. Aangezien het geldende productveiligheidskader technologieneutraal is, betekent dit echter niet dat het niet van toepassing is op producten waarin deze technologieën zijn verwerkt. Bovendien is in latere wetgevingshandelingen die deel uitmaken van dat kader, zoals die betreffende medische hulpmiddelen of automobielen, reeds expliciet rekening gehouden met een aantal aspecten van de opkomst van digitale technologieën, zoals geautomatiseerde besluitvorming, software als afzonderlijk product en connectiviteit.

Basis van de huidige productveiligheidswetgeving van de Unie[25]



[24] Bijvoorbeeld Richtlijn 2007/46/EG (goedkeuring van motorvoertuigen en aanhangwagens daarvan en van systemen, onderdelen en technische eenheden die voor dergelijke voertuigen zijn bestemd) en Verordening (EU) 2018/858 van het Europees Parlement en de Raad van 30 mei 2018 betreffende de goedkeuring van en het markttoezicht op motorvoertuigen en aanhangwagens daarvan en systemen, onderdelen en technische eenheden die voor dergelijke voertuigen zijn bestemd, tot wijziging van Verordeningen (EG) nr. 715/2007 en (EG) nr. 595/2009 en tot intrekking van Richtlijn 2007/46/EG.

[25] Deze afbeelding geeft niet de eisen met betrekking tot de productlevenscyclus weer (d.w.z. gebruik en onderhoud) en dient uitsluitend ter illustratie.

De uitdagingen waarvoor de digitale technologieën in opkomst het productveiligheidskader van de Unie stellen, worden hierna beschreven.

Connectiviteit is een centraal kenmerk van een toenemend aantal producten en diensten. Dit is een uitdaging voor het traditionele concept van veiligheid, aangezien connectiviteit de veiligheid van het product direct en indirect in gevaar kan brengen, indien de connectiviteitsfunctie kan worden gehackt, en daarmee tot veiligheidsdreigingen kan leiden en de veiligheid van de gebruikers kan aantasten.

Een voorbeeld hiervan is een smartwatch voor kinderen waarvan IJsland kennisgeving heeft gedaan aan het Rapid Alert System van de EU[26]. Dit product zou geen rechtstreekse schade toebrengen aan het kind dat het draagt, maar omdat het niet aan minimale veiligheidseisen voldoet, kan het gemakkelijk worden gebruikt als instrument om toegang tot het kind te krijgen. Aangezien een van de beoogde functies van het product is om de veiligheid van kinderen te bevorderen door het mogelijk te maken hun locatie te volgen, verwacht de consument niet dat het product een veiligheidsdreiging voor het kind inhoudt, doordat iedereen het kind kan traceren en/of benaderen.

Een ander voorbeeld is te vinden in een kennisgeving van Duitsland over een personenauto[27]. In de software van de in het voertuig ingebouwde radio kunnen beveiligingslekken zitten waardoor onbevoegden toegang kunnen krijgen tot de ermee verbonden controlesystemen van het voertuig. Als de leemten in de beveiliging van de software door een derde worden misbruikt, zou er een verkeersongeval kunnen gebeuren.

Industriële toepassingen kunnen ook worden blootgesteld aan cyberdreigingen die de veiligheid van personen op grotere schaal aantasten, wanneer bij dergelijke toepassingen de nodige beveiligingsniveaus ontbreken. Dit kan bijvoorbeeld het geval zijn bij een cyberaanval op een kritisch controlesysteem van een industrieel bedrijf, die bedoeld is om een explosie te veroorzaken die mensenlevens zou kunnen kosten.

De EU-wetgeving inzake productveiligheid voorziet in het algemeen niet in specifieke verplichte essentiële vereisten tegen cyberbedreigingen die de veiligheid van de gebruikers kunnen aantasten. Bepalingen over veiligheidsaspecten komen wel voor in de verordening medische hulpmiddelen[28], de richtlijn meetinstrumenten[29], de richtlijn radioapparatuur[30] en de wetgeving betreffende de typegoedkeuring van voertuigen[31]. De cyberbeveiligingsverordening[32] voorziet in vrijwillige kaders voor cyberbeveiligingscertificering met betrekking tot producten, diensten en processen op het gebied van informatie- en communicatietechnologie (ICT), terwijl de toepasselijke wetgeving inzake productveiligheid van de Unie bindende voorschriften bevat.

---

[26] Rapex-kennisgeving van IJsland, gepubliceerd op de website van EU Safety Gate (A12/0157/19).

[27] Rapex-kennisgeving van Duitsland, gepubliceerd op de website van EU Safety Gate (A12/1671/15).

[28] Verordening (EU) 2017/745 betreffende medische hulpmiddelen.

[29] Richtlijn 2014/32/EU betreffende het op de markt aanbieden van meetinstrumenten.

[30] Richtlijn 2014/53/EU betreffende het op de markt aanbieden van radioapparatuur.

[31] Richtlijn 2007/46/EG betreffende de goedkeuring van motorvoertuigen en aanhangwagens daarvan en van systemen, onderdelen en technische eenheden die voor dergelijke voertuigen zijn bestemd. Deze richtlijn wordt per 1 september 2020 ingetrokken en vervangen door Verordening (EU) 2018/858 betreffende de goedkeuring van en het markttoezicht op motorvoertuigen en aanhangwagens daarvan en systemen, onderdelen en technische eenheden die voor dergelijke voertuigen zijn bestemd, tot wijziging van Verordeningen (EG) nr. 715/2007 en (EG) nr. 595/2009 en tot intrekking van Richtlijn 2007/46/EG.

[32] Verordening (EU) 2019/881.

Bovendien kan het risico op verlies van de connectiviteit van opkomende digitale technologieën ook risico's in verband met de veiligheid met zich meebrengen. Indien bijvoorbeeld de netwerkverbinding van een geconnecteerd brandalarm wegvalt, kan het product de gebruiker bij brand niet waarschuwen.

Veiligheid is in de huidige productveiligheidswetgeving van de Unie een van de doelstellingen van het overheidsbeleid. Het veiligheidsconcept hangt samen met het gebruik van het product en met de (bijvoorbeeld mechanische of elektrische) risico's die moeten worden aangepakt om het product veilig te maken. Onder het gebruik van het product wordt, afhankelijk van de EU-productveiligheidswetgeving die op het product van toepassing is, niet alleen het beoogde gebruik verstaan, maar ook voorzienbaar gebruik en in sommige gevallen, zoals in de machinerichtlijn[33], ook redelijkerwijs voorzienbaar verkeerd gebruik.

Het veiligheidsconcept waarop de huidige productveiligheidswetgeving van de Unie is gebaseerd, past bij een uitgebreid veiligheidsconcept dat de veiligheid van consumenten en gebruikers tot doel heeft. Het begrip productveiligheid omvat dus bescherming tegen alle soorten risico's die door het product ontstaan, dat wil zeggen niet alleen mechanische, chemische en elektrische risico's, maar ook cyberrisico's en risico's die verband houden met verlies van connectiviteit van een apparaat.

Voor het toepassingsgebied van de relevante wetgevingshandelingen van de Unie zouden uitdrukkelijke bepalingen op dit gebied kunnen worden overwogen om de gebruikers betere bescherming en meer rechtszekerheid te bieden.

Autonomie[34] is een van de belangrijkste kenmerken van KI. Uit kunstmatige intelligentie voortvloeiende onbedoelde gevolgen zouden gebruikers en eraan blootgestelde personen schade kunnen berokkenen.

Voor zover het toekomstige "gedrag" van KI-producten vooraf kan worden bepaald door de risicobeoordeling die de fabrikant uitvoert voordat de producten in de handel worden gebracht, bevat het productveiligheidskader van de Unie reeds verplichtingen voor producenten om bij de risicobeoordeling rekening te houden met het "gebruik"[35] van de producten gedurende hun levensduur. Het productveiligheidskader bepaalt ook dat fabrikanten instructies en veiligheidsinformatie of waarschuwingen voor de gebruikers moeten verstrekken[36]. In dit verband vereist de richtlijn radioapparatuur[37] bijvoorbeeld dat de fabrikant instructies verstrekt over hoe de radioapparatuur moet worden gebruikt in overeenstemming met het beoogde gebruik ervan.

---

[33] Richtlijn 2006/42/EG betreffende machines.

[34] Hoewel op KI gebaseerde producten autonoom kunnen handelen door hun omgeving waar te nemen, zonder een reeks vooraf vastgestelde instructies te volgen, wordt hun gedrag beperkt door het doel dat voor de werking ervan is vastgesteld en andere relevante ontwerpkeuzen die de ontwikkelaars van die producten hebben gemaakt.

[35] Volgens de productveiligheidswetgeving van de Unie verrichten de producenten de risicobeoordeling op basis van het beoogde gebruik van het product, voorzienbaar gebruik en/of redelijkerwijs voorzienbaar verkeerd gebruik.

[36] Besluit nr. 768/2008/EG van het Europees Parlement en de Raad van 9 juli 2008 betreffende een gemeenschappelijk kader voor het verhandelen van producten en tot intrekking van Besluit 93/465/EEG van de Raad (PB L 218 van 13.8.2008, blz. 82). Artikel R2, lid 7, van bijlage I luidt als volgt: *"De fabrikanten zien erop toe dat het product vergezeld gaat van instructies en informatie aangaande de veiligheid, in een taal die de consumenten en andere eindgebruikers, zoals bepaald door de betrokken lidstaat, gemakkelijk kunnen begrijpen."*

[37] Artikel 10, lid 8, betreffende de instructies voor de eindgebruiker en bijlage VI betreffende de EU-conformiteitsverklaring.

Er kunnen zich in de toekomst ook situaties voordoen waarin de resultaten van KI-systemen vooraf niet volledig kunnen worden vastgesteld. In een dergelijke situatie kan het zijn dat de risicobeoordeling die wordt uitgevoerd voordat het product in de handel wordt gebracht, niet langer in overeenstemming is met het gebruik, de werking of het gedrag van het product. In die gevallen kan, voor zover het beoogde gebruik zoals de fabrikant dat oorspronkelijk heeft voorzien, is gewijzigd[38] als gevolg van het autonome gedrag en de naleving van de veiligheidsvoorschriften, worden overwogen een herbeoordeling van het zelflerende product te vereisen[39].

Wanneer producenten beseffen dat een product tijdens de levensduur ervan risico's met zich meebrengt die gevolgen hebben voor de veiligheid, zijn zij overeenkomstig het geldende kader reeds verplicht de bevoegde autoriteiten daarvan onmiddellijk in kennis te stellen en actie te ondernemen om de risico's voor de gebruikers te voorkomen[40].

Naast de risicobeoordeling die wordt uitgevoerd voordat een product in de handel wordt gebracht, kan een nieuwe risicobeoordelingsprocedure worden ingesteld wanneer het product tijdens de levensduur ervan belangrijke veranderingen ondergaat, bijvoorbeeld een andere productfunctie krijgt, die de fabrikant bij de aanvankelijke risicobeoordeling niet heeft voorzien. Bij deze nieuwe risicobeoordelingsprocedure moet de nadruk liggen op de gevolgen voor de veiligheid van het autonome gedrag dat het product gedurende zijn gehele levensduur vertoont. De risicobeoordeling moet worden uitgevoerd door de betrokken marktdeelnemer. Daarnaast zouden in de relevante Uniewetgeving strengere eisen voor de fabrikanten kunnen worden opgenomen inzake de instructies en waarschuwingen voor de gebruikers.

In de vervoerswetgeving zijn reeds vergelijkbare risicobeoordelingen vereist[41]; zo wordt in de wetgeving inzake het spoorwegvervoer bepaald dat wanneer een spoorvoertuig na de certificering wordt gewijzigd, de uitvoerder van de wijziging een specifieke procedure en duidelijke criteria moet volgen om te bepalen of de autoriteit er al dan niet bij moet worden betrokken.

---

[38] Tot dusver wordt in de context van KI het begrip "zelflerend" doorgaans gebruikt om aan te geven dat machines in staat zijn om tijdens hun training te leren; het is nog geen vereiste dat KI-machines na hun ingebruikneming blijven leren; het is integendeel met name in de gezondheidszorg gewoonlijk zo dat het leerproces van KI-machines na de succesvolle afronding van hun training stopt. In dit stadium betekent het autonome gedrag dat KI-systemen vertonen, niet dat het product taken uitvoert die door de ontwikkelaars niet zijn voorzien.

[39] Dit is in overeenstemming met punt 2.1 van de "Blauwe Gids": richtlijnen voor de uitvoering van de productvoorschriften van de EU, 2016.

[40] Artikel 5 van Richtlijn 2001/95/EG van het Europees Parlement en de Raad van 3 december 2001 inzake algemene productveiligheid.

[41] In geval van een wijziging van het spoorwegsysteem die gevolgen kan hebben voor de veiligheid (bv. een technische of operationele wijziging of ook wel een organisatorische verandering die van invloed kan zijn op het operationele of onderhoudsproces), wordt het te volgen proces beschreven in bijlage I bij Uitvoeringsverordening (EU) 2015/1136 (PB L 185 van 14.7.2015, blz. 6).
In geval van een "belangrijke wijziging" moet aan de initiatiefnemer van de wijziging een veiligheidsbeoordelingsverslag worden overgelegd door een onafhankelijke "beoordelingsinstantie" (de nationale veiligheidsinstantie of een andere technisch bekwame instantie zou deze rol kunnen vervullen).
Na de risicoanalyse neemt de initiatiefnemer van de wijziging gepaste maatregelen om de risico's te beperken (indien de initiatiefnemer een spoorwegonderneming of een infrastructuurbeheerder is, is de toepassing van de verordening onderdeel van het veiligheidsbeheersysteem, waarvan de toepassing onder toezicht staat van de nationale veiligheidsautoriteit).

Het zelflerende karakter van KI-producten en -systemen kan ertoe leiden dat de machine beslissingen neemt die afwijken van de aanvankelijke bedoelingen van de makers ervan en derhalve van de verwachtingen van de gebruikers. Dit roept vragen op over menselijke controle, die inhoudt dat de mens kan kiezen of de beslissingsbevoegdheid ter verwezenlijking van een door de mens gekozen doelstelling kan worden overgedragen aan KI-producten of -systemen, en op welke wijze dat moet gebeuren[42]. De bestaande Uniewetgeving inzake productveiligheid regelt niet uitdrukkelijk het menselijk toezicht in de context van zelflerende KI-producten en -systemen[43].

De desbetreffende rechtshandelingen van de Unie kunnen voorzien in specifieke vereisten voor menselijk toezicht bij wijze van waarborg, vanaf het ontwerp van het product en gedurende de hele levensduur van KI-producten en -systemen.

Het toekomstige "gedrag" van de KI-toepassingen kan tot **risico's voor de geestelijke gezondheid**[44] van gebruikers leiden, bijvoorbeeld als gevolg van de samenwerking met humanoïde KI-robots en -systemen, thuis of in de werkomgeving. In dit verband wordt met de term veiligheid momenteel in het algemeen verwezen naar de bij de gebruiker bestaande perceptie van de dreiging van fysiek letsel dat door de opkomende digitale technologie kan worden veroorzaakt. Tegelijkertijd worden veilige producten in het rechtskader van de Unie gedefinieerd als producten die geen of slechts minimale risico's inhouden voor de veiligheid en gezondheid van personen. Algemeen is men het erover eens dat de definitie van gezondheid op zowel lichamelijk als geestelijk welzijn doelt. Risico's voor de geestelijke gezondheid zouden in het rechtskader uitdrukkelijk onder het begrip productveiligheid moeten vallen.

De autonomie mag bijvoorbeeld niet gedurende langere tijd buitensporige stress of ongemak veroorzaken en mag de geestelijke gezondheid niet schaden. In dit verband worden als factoren die het gevoel van veiligheid voor ouderen[45] positief beïnvloeden, beschouwd: een veilige relatie hebben met het zorgpersoneel, controle hebben over de dagelijkse routines en ervan op de hoogte zijn. Producenten van robots die met ouderen in contact komen, moeten deze factoren in aanmerking nemen om risico's voor de geestelijke gezondheid te voorkomen.

Wat het toepassingsgebied van de relevante EU-wetgeving betreft, kan worden overwogen er voor producenten van onder meer KI-robots de uitdrukkelijke verplichting in op te nemen om uitdrukkelijk rekening te houden met de immateriële schade die hun producten zouden kunnen toebrengen aan gebruikers, in het bijzonder kwetsbare gebruikers zoals ouderen in een zorgomgeving.

---

[42] Policy and Investment Recommendations for Trustworthy AI, Deskundigengroep op hoog niveau inzake kunstmatige intelligentie, juni 2019.

[43] Dit sluit echter niet uit dat in een bepaalde situatie in toezicht moet worden voorzien als uitvloeisel van een of meer van de bestaande meer algemene verplichtingen betreffende het in de handel brengen van het product.

[44] Statuut van de Wereldgezondheidsorganisatie, eerste streepje: "Gezondheid is een toestand van volledig lichamelijk, geestelijk en sociaal welzijn en niet slechts de afwezigheid van ziekte of zwakheid." (https://www.who.int/about/who-we-are/constitution).

[45] Neziha Akalin, Annica Kristoffersson and Amy Loutfi: "Evaluating the Sense of Safety and Security in Human–Robot Interaction with Older People", in *Social Robots: Technological, Societal and Ethical Aspects of Human-Robot Interaction*, blz. 237-264, juli 2019.

Ook **data-afhankelijkheid** is een essentiële eigenschap van op KI gebaseerde producten en systemen. Nauwkeurigheid en relevantie van data is van essentieel belang om ervoor te zorgen dat op KI gebaseerde systemen en producten beslissingen nemen op de door de producent beoogde wijze.

In de EU-wetgeving inzake productveiligheid wordt niet uitdrukkelijk ingegaan op veiligheidsrisico's die voortvloeien uit onjuiste data. Naargelang het "gebruik" dat van het product wordt gemaakt, moeten de producenten echter tijdens de ontwerp- en testfase al rekening houden met de nauwkeurigheid van de data en de relevantie daarvan voor de beveiligingsfuncties.

Zo kan een op KI gebaseerd systeem dat ontworpen is om specifieke objecten te detecteren, problemen ondervinden met de herkenning van voorwerpen bij slechte verlichting; de ontwerpers ervan moeten dus data gebruiken die afkomstig zijn van producttesten in zowel typische als slecht verlichte omgevingen.

Een ander voorbeeld heeft betrekking op landbouwrobots, zoals fruitplukrobots die afgestemd zijn op het opsporen en lokaliseren van rijpe vruchten aan bomen of op de grond. Hoewel de betrokken algoritmen wat de categorisering betreft nu al succespercentages van meer dan 90% laten zien, kunnen tekortkomingen in de datasets die deze algoritmen voeden, ertoe leiden dat de robots een ongelukkig besluit nemen en daardoor letsel toebrengen aan mensen of dieren.

De vraag rijst of in de Uniewetgeving inzake productveiligheid specifieke vereisten moeten worden opgenomen met betrekking tot veiligheidsrisico's die ontstaan doordat in de ontwerpfase onjuiste data zijn gebruikt. Ook moet worden nagegaan of er mechanismen moeten komen die ervoor zorgen dat de kwaliteit van de data in alle fasen van het gebruik van de KI-producten en -systemen wordt gehandhaafd.

Voor sommige op KI gebaseerde producten en systemen kan het vermogen om prestaties te verbeteren door van ervaringen te leren, ook leiden tot een **gebrek aan transparantie**. Afhankelijk van de wijze van benadering komt gebrek aan transparantie bij op KI gebaseerde producten en systemen in verschillende gradaties voor. Een en ander kan ertoe leiden dat het besluitvormingsproces in het systeem moeilijk te traceren is (het "black box"-effect). Mensen hoeven misschien niet elke stap van het besluitvormingsproces te begrijpen, maar naarmate KI-algoritmen steeds geavanceerder worden en steeds meer op kritieke gebieden worden ingezet, is het van doorslaggevend belang dat mensen kunnen doorgronden hoe de algoritmische besluiten van het systeem tot stand komen. Met name is dat van belang voor het mechanisme voor controle achteraf, aangezien dit de handhavingsautoriteiten de mogelijkheid biedt om de verantwoordelijkheid voor gedragingen en keuzes van KI-systemen vast te stellen. Dit wordt ook erkend in de mededeling van de Commissie "Vertrouwen kweken in mensgerichte kunstmatige intelligentie"[46].

[46] https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top, https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:52019DC0168

In de Uniewetgeving inzake productveiligheid wordt niet uitdrukkelijk ingegaan op de toenemende risico's als gevolg van het gebrek aan transparantie van op algoritmen gebaseerde systemen. Daarom moet erover worden nagedacht welke eisen moeten worden gesteld aan de transparantie van algoritmen, maar ook aan de robuustheid, de verantwoordingsplicht en, waar relevant, menselijk toezicht en vertekening[47]. Dit is met name van belang voor het mechanisme voor controle achteraf en voor het vertrouwen in het gebruik van deze technologieën. Een oplossing zou kunnen zijn de ontwikkelaars van algoritmen te verplichten de ontwerpparameters en metagegevens van de datasets over te leggen voor het geval dat zich een ongeval voordoet.

Andere risico's die gevolgen kunnen hebben voor de veiligheid, vloeien voort uit de **complexiteit van de producten en systemen**, doordat er verschillende componenten, apparaten en producten in kunnen zijn geïntegreerd die elkaars werking kunnen beïnvloeden (bijvoorbeeld producten die deel uitmaken van een smart-home-ecosysteem).

Met deze complexiteit wordt al rekening gehouden door het Unierechtskader voor veiligheid waarnaar in het begin van dit onderdeel wordt verwezen[48]; met name het feit dat wanneer een producent de risicobeoordeling van een product uitvoert, hij rekening moet houden met het beoogde gebruik, voorzienbaar gebruik en in voorkomend geval redelijkerwijs voorzienbaar verkeerd gebruik.

In dit verband geldt: **als de producent voorziet dat het door hem vervaardigde apparaat zal worden verbonden met andere apparaten en er daarmee wisselwerking zal plaatsvinden, moet dit bij de risicobeoordeling in overweging worden genomen.** Gebruik of verkeerd gebruik wordt vastgesteld op basis van bijvoorbeeld ervaring met het gebruik van hetzelfde type product, onderzoek of menselijk gedrag in het verleden.

De complexiteit van systemen komt ook meer specifiek aan de orde in de sectorale veiligheidswetgeving, zoals de verordening betreffende medische hulpmiddelen, en in zekere mate in de wetgeving inzake algemene productveiligheid[49]. Zo moet de producent van een geconnecteerd apparaat dat bedoeld is om deel uit te maken van een smart-home-ecosysteem, redelijkerwijs kunnen voorzien dat zijn producten een effect zullen hebben op de veiligheid van andere producten.

Daarnaast behandelt de vervoerswetgeving deze complexiteit op systeemniveau. Voor auto's, treinen en vliegtuigen vindt typegoedkeuring en certificering plaats voor zowel elk onderdeel apart als voor het gehele voertuig of vliegtuig. Rij- en luchtwaardigheid en spoorweginteroperabiliteit maken deel uit van de veiligheidsbeoordeling. Op het gebied van het vervoer moet voor een "systeem" door een autoriteit een "vergunning " verleend zijn, hetzij op basis van een beoordeling door een derde van de overeenstemming met duidelijke technische vereisten, hetzij na een demonstratie van de wijze waarop de risico's worden

---

[47] Op basis van de belangrijkste vereisten die de deskundigengroep op hoog niveau heeft voorgesteld in de ethische richtsnoeren voor betrouwbare KI: https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines

[48] Verordening (EG) nr. 2008/765 en Besluit (EG) nr. 2008/768 en de geharmoniseerde sectorale productveiligheidswetgeving, bijvoorbeeld de machinerichtlijn (Richtlijn 2006/42/EG).

[49] In artikel 2 van de richtlijn algemene productveiligheid wordt bepaald dat voor een veilig product rekening moet worden gehouden met "het effect ervan op andere producten, ingeval redelijkerwijs kan worden verwacht dat het product in combinatie met die andere producten zal worden gebruikt".

aangepakt. De oplossing is in het algemeen een combinatie van het "product"- en "systeem"-niveau.

De wetgeving van de Unie inzake productveiligheid, met inbegrip van de vervoerswetgeving, houdt reeds in zekere mate rekening met de complexiteit van producten of systemen bij het aanpakken van de risico's die de veiligheid van de gebruikers kunnen beïnvloeden.

Bij complexe systemen wordt vaak gebruikgemaakt van **software**, een essentieel onderdeel van een op KI gebaseerd systeem. In het algemeen is de fabrikant van het eindproduct in het kader van de initiële risicobeoordeling verplicht om de risico's te voorzien van in dat product geïntegreerde software op het moment dat dit in de handel wordt gebracht.

Bepaalde onderdelen van de Uniewetgeving inzake productveiligheid verwijzen uitdrukkelijk naar software die in een product is geïntegreerd. Zo bepaalt de machinerichtlijn[50] dat een storing in de software van het besturingssysteem niet tot gevaarlijke situaties mag leiden.

In het kader van de productveiligheidswetgeving van de Unie kunnen software-updates worden vergeleken met onderhoudsmaatregelen die om veiligheidsredenen worden uitgevoerd, mits zij een reeds op de markt gebracht product niet ingrijpend wijzigen en geen nieuwe risico's introduceren die niet waren voorzien in de initiële risicobeoordeling. Indien de software-update echter het product waarvoor het wordt gedownload, ingrijpend wijzigt, kan het volledige product als een nieuw product worden beschouwd en moet de conformiteit met de relevante wetgeving inzake productveiligheid op het moment van de wijziging opnieuw worden beoordeeld[51].

Voor opzichzelfstaande software die in de handel wordt gebracht of na het in de handel brengen van het product wordt geüpload, bevat de sectorspecifieke geharmoniseerde Uniewetgeving inzake productveiligheid over het algemeen geen specifieke bepalingen. Bepaalde rechtshandelingen van de Unie hebben echter betrekking op opzichzelfstaande software, bijvoorbeeld de verordening medische hulpmiddelen. Bovendien kan opzichzelfstaande software die is geüpload naar geconnecteerde producten die via bepaalde radiomodules[52] communiceren, door middel van gedelegeerde handelingen ook door de richtlijn radioapparatuur worden geregeld. Deze richtlijn vereist dat specifieke klassen of categorieën radioapparatuur mogelijkheden ondersteunen die moeten waarborgen dat de conformiteit van die apparatuur niet in het gedrang komt wanneer software wordt geüpload[53].

De productveiligheidswetgeving van de Unie houdt weliswaar rekening met veiligheidsrisico's die voortvloeien uit software die bij het op de markt brengen van een product daarin is geïntegreerd, alsmede eventuele latere door de fabrikant geplande updates, maar het is mogelijk dat specifieke en/of uitdrukkelijke voorschriften vereist zijn voor opzichzelfstaande software (bijvoorbeeld een "app" die gedownload moet worden). Bijzondere aandacht is nodig ten aanzien van opzichzelfstaande software waarmee veiligheidsfuncties in KI-producten en -systemen worden gewaarborgd.

---

50 Punt 1.2.1 van bijlage I bij de machinerichtlijn.

51 Blauwe Gids, richtlijnen voor de uitvoering van de productvoorschriften van de EU, 2016

52 Radiomodules zijn elektronische apparaten die radiosignalen (Wi-Fi, Bluetooth) uitzenden en/of ontvangen tussen twee apparaten.

53 Artikel 3, lid 3, onder i), van de richtlijn radioapparatuur.

Het is mogelijk dat voor fabrikanten aanvullende verplichtingen moeten gelden om ervoor te zorgen dat zij het mogelijk maken te voorkomen dat tijdens de levensduur van de KI-producten software wordt geüpload die veiligheidsconsequenties heeft.

Tot slot geldt voor opkomende digitale technologieën dat er sprake kan zijn van **complexe waardeketens**. Deze complexiteit is echter niet nieuw, noch is dit uitsluitend een probleem dat wordt veroorzaakt door nieuwe opkomende digitale technologieën zoals KI of IoT. Hetzelfde geldt bijvoorbeeld voor producten als computers, dienstenrobots of vervoerssystemen.

Binnen het productveiligheidskader van de Unie berust de verantwoordelijkheid voor de veiligheid van het product, hoe complex de waardeketen ook is, steeds bij de producent die het product in de handel brengt. De producenten zijn verantwoordelijk voor de veiligheid van het eindproduct, met inbegrip van de onderdelen die in het product zijn geïntegreerd, bijvoorbeeld de software van een computer.

In sommige rechtshandelingen van de Unie inzake productveiligheid zijn al bepalingen opgenomen die uitdrukkelijk verwijzen naar situaties waarin verschillende marktdeelnemers een inbreng hebben in een bepaald product voordat dit product in de handel wordt gebracht. Zo vereist de liftenrichtlijn[54] dat de ondernemer die de lift ontwerpt en vervaardigt, de installateur[55] *"alle nodige documenten en gegevens [verstrekt] zodat de laatste de lift correct en veilig kan installeren en keuren"*. De machinerichtlijn verplicht fabrikanten van apparatuur om de exploitant informatie te verstrekken over de montage van die apparatuur samen met andere machines[56].

De productveiligheidswetgeving van de Unie houdt rekening met de complexiteit van de waardeketens en legt verplichtingen op aan verschillende marktdeelnemers volgens het beginsel van "gedeelde verantwoordelijkheid".

Hoewel voor de huidige complexe waardeketens de verantwoordelijkheid van de producent voor de veiligheid van het eindproduct adequaat is gebleken, zou voor wellicht nog complexere waardeketens rechtszekerheid kunnen worden geboden door middel van uitdrukkelijke bepalingen die specifiek samenwerking vereisen tussen de marktdeelnemers in de toeleveringsketen en de gebruikers. Met name zou elke actor in de waardeketen die een impact heeft op de productveiligheid (bv. softwareproducenten) en gebruikers (door wijziging van het product) zijn verantwoordelijkheid op zich nemen en de volgende actor in de keten de nodige informatie en maatregelen ter beschikking stellen.

---

54 Richtlijn 2014/33/EU, artikel 16, lid 2.

55 De installateur is volgens de liftenrichtlijn (Richtlijn 2014/33/EU) het equivalent van de fabrikant en moet de verantwoordelijkheid op zich nemen voor het ontwerp, de vervaardiging, de installatie en het in de handel brengen van de lift.

56 Machinerichtlijn, bijlage I, punt 1.7.4.2: *"Iedere gebruiksaanwijzing moet, in voorkomend geval, ten minste de volgende informatie bevatten: […] i) instructies voor de montage, installatie en aansluiting van de machine, met inbegrip van tekeningen, schema's en de bevestigingsmiddelen, en aanduiding van het chassis of de installatie waarop de machine moet worden gemonteerd"*.

3. Aansprakelijkheid

Op Unieniveau zijn bepalingen inzake productveiligheid en productaansprakelijkheid twee aanvullende mechanismen voor de verwezenlijking van dezelfde beleidsdoelstelling, namelijk een goed functionerende eengemaakte markt voor goederen die een hoog niveau van veiligheid garandeert, wat wil zeggen dat het risico op schade voor de gebruikers tot een minimum wordt beperkt, en voorziet in een vergoeding voor schade die het gevolg is van gebreken in goederen.

Op nationaal niveau worden deze Unievoorschriften aangevuld door niet-geharmoniseerde stelsels voor wettelijke aansprakelijkheid die vergoeding bieden voor schade door verschillende oorzaken (zoals producten en diensten) en zich richten op verschillende aansprakelijke personen (zoals eigenaren, exploitanten of dienstverleners).

Hoewel optimalisering van de veiligheidsvoorschriften van de Unie op het gebied van KI kan helpen ongevallen te voorkomen, kunnen die toch gebeuren. In dat geval speelt de wettelijke aansprakelijkheid een rol. De regels inzake wettelijke aansprakelijkheid hebben een tweeledige functie in onze samenleving: enerzijds waarborgen zij dat slachtoffers van door anderen veroorzaakte schade een vergoeding krijgen en anderzijds bieden zij de aansprakelijke partij economische prikkels om dergelijke schade te vermijden. De aansprakelijkheidsregels moeten altijd voor een evenwicht zorgen tussen de bescherming van burgers tegen schade, en de mogelijkheid voor bedrijven om te innoveren.

De aansprakelijkheidskaders in de Unie functioneren goed. Zij zijn gebaseerd op de gelijktijdige toepassing van de productaansprakelijkheidsrichtlijn (Richtlijn 85/374/EEG), waarbij de aansprakelijkheid van de producent van producten met gebreken is geharmoniseerd, en andere, niet-geharmoniseerde nationale aansprakelijkheidsregelingen.

De productaansprakelijkheidsrichtlijn voorziet in een beschermingsniveau dat de louter nationale schuldaansprakelijkheid niet biedt. Zij voerde een stelsel in dat berust op de strikte aansprakelijkheid van de producent voor schade die is veroorzaakt door een gebrek in zijn producten. In geval van fysiek letsel of materiële schade heeft de benadeelde recht op vergoeding als hij de schade, het gebrek in het product (dat wil zeggen dat het product niet de veiligheid biedt die het publiek mag verwachten) en het oorzakelijk verband tussen het gebrek en de schade kan aantonen.

De nationale niet-geharmoniseerde regelingen voorzien in regels op het gebied van schuldaansprakelijkheid, waarbij slachtoffers van schade de schuld van de aansprakelijke partij, de schade en het oorzakelijk verband tussen de schuld en de schade moeten bewijzen om met succes een aansprakelijkheidsvordering te kunnen instellen. Zij voorzien ook in risicoaansprakelijkheidsregelingen voor het geval dat de nationale wetgever de aansprakelijkheid voor een risico heeft toegewezen aan een bepaalde persoon, zonder dat een slachtoffer het bewijs hoeft te leveren van een fout/gebrek of van het oorzakelijk verband tussen de fout/het gebrek en de schade.

Nationale aansprakelijkheidsregelingen bieden slachtoffers van schade die door producten en diensten wordt veroorzaakt, een aantal verschillende parallelle schadevorderingen op basis van schuldaansprakelijkheid of risicoaansprakelijkheid. Deze vorderingen zijn vaak gericht tegen verschillende aansprakelijke personen en kennen verschillende voorwaarden.

Zo heeft een slachtoffer dat betrokken is bij een auto-ongeluk, doorgaans een risicoaansprakelijkheidsvordering op de eigenaar van de auto (d.w.z. de persoon die de wettelijke aansprakelijkheidsverzekering voor motorvoertuigen heeft gesloten) en een

schuldaansprakelijkheidsvordering op de bestuurder, beide uit hoofde van het nationale burgerlijk recht, alsmede een vordering op grond van de productaansprakelijkheidsrichtlijn op de producent, indien de auto een gebrek vertoont.

Overeenkomstig de geharmoniseerde voorschriften inzake motorrijtuigenverzekering moet het gebruik van het voertuig verzekerd zijn[57] en is de verzekeraar altijd het eerste aanspreekpunt voor vorderingen tot vergoeding van persoonlijk letsel of materiële schade. Volgens deze regels vergoedt de verplichte verzekering het slachtoffer en beschermt zij de verzekerde die uit hoofde van de nationale civielrechtelijke voorschriften[58] aansprakelijk is voor de vergoeding van financiële schade ten gevolge van het ongeval met het motorvoertuig. Producenten zijn niet onderworpen aan de verzekeringsplicht op grond van de productaansprakelijkheidsrichtlijn. Zelfrijdende voertuigen worden wat de motorrijtuigenverzekeringen betreft in de Uniewetgeving niet anders behandeld dan niet-zelfrijdende voertuigen. Dergelijke voertuigen moeten, net als alle voertuigen, gedekt zijn door de wettelijke aansprakelijkheidsverzekering voor motorrijtuigen, hetgeen voor de benadeelde de gemakkelijkste manier is om schadevergoeding te krijgen.

Het afsluiten van een goede verzekering kan de negatieve gevolgen van ongevallen beperken door te voorzien in soepele schadevergoeding voor het slachtoffer. Duidelijke aansprakelijkheidsregels helpen verzekeringsmaatschappijen om hun risico's te berekenen en terugbetaling te eisen van de partij die uiteindelijk aansprakelijk is voor de schade. Als bijvoorbeeld een ongeval veroorzaakt is door een defect, kan de motorrijtuigenverzekeraar na de schadeloosstelling van het slachtoffer terugbetaling eisen van de fabrikant.

De eigenschappen van opkomende digitale technologieën zoals KI, IoT en robotica, kunnen leiden tot problemen met bepaalde aspecten van de aansprakelijkheidskaders van de Unie en van de lidstaten en kunnen de effectiviteit ervan beperken. Sommige van deze eigenschappen maken het moeilijk om schade terug te voeren op menselijke gedragingen, hetgeen volgens de nationale regels noodzakelijk kan zijn om een vordering op basis van schuld te kunnen indienen. Dit betekent dat het moeilijk of kostbaar kan zijn om aansprakelijkheidsvorderingen op basis van het nationale recht inzake onrechtmatige daad aan te tonen en dat de slachtoffers bijgevolg mogelijk niet voldoende schadeloos worden gesteld. Het is belangrijk dat slachtoffers van ongevallen met producten en diensten, met inbegrip van opkomende digitale technologieën zoals KI, geen lager niveau van bescherming genieten dan slachtoffers van soortgelijke andere producten en diensten, die compensatie zouden krijgen uit hoofde van het nationale aansprakelijkheidsrecht. Dit zou de maatschappelijke acceptatie van deze opkomende technologieën kunnen verminderen en kunnen leiden tot aarzeling om deze technologieën te gebruiken.

Onderzocht moet worden of de uitdagingen die de nieuwe technologieën betekenen voor de bestaande kaders, ook tot rechtsonzekerheid kunnen leiden over de vraag hoe de bestaande rechtsregels moeten worden toegepast (bv. hoe het begrip "schuld" moet worden toegepast op schade die is veroorzaakt door KI). Deze uitdagingen kunnen op hun beurt een ontmoedigende werking hebben op investeringen en de informatie- en verzekeringskosten

[57] Geharmoniseerd voor motorrijtuigen bij Richtlijn 2009/103/EG betreffende de verzekering tegen de wettelijke aansprakelijkheid waartoe de deelneming aan het verkeer van motorrijtuigen aanleiding kan geven en de controle op de verzekering tegen deze aansprakelijkheid.

[58] In de meeste lidstaten geldt risicoaansprakelijkheid voor de persoon op wiens naam het motorrijtuig is geregistreerd.

voor producenten en andere bedrijven in de toeleveringsketen, met name Europese kmo's, opdrijven. Indien de lidstaten de problemen voor de nationale aansprakelijkheidsregelingen uiteindelijk zouden aanpakken, zou dit bovendien kunnen leiden tot verdere fragmentering, en daardoor de kosten van het invoeren van innovatieve KI-oplossingen opdrijven en de grensoverschrijdende handel op de eengemaakte markt belemmeren. Het is van belang dat ondernemingen hun aansprakelijkheidsrisico's in de hele waardeketen kennen en deze risico's kunnen beperken of verhinderen en zich daadwerkelijk tegen deze risico's kunnen verzekeren.

In dit hoofdstuk wordt uitgelegd hoe nieuwe technologieën een uitdaging vormen voor de bestaande kaders en hoe deze uitdagingen kunnen worden aangepakt. Bovendien kunnen specifieke aspecten van bepaalde sectoren, zoals de gezondheidszorg, extra aandacht verdienen.

Complexiteit van producten, diensten en de waardeketen: de afgelopen decennia hebben de technologie en de industrie drastische veranderingen ondergaan. Met name is de scheidslijn tussen producten en diensten wellicht niet meer zo duidelijk als zij vroeger was. Producten en dienstverlening zijn steeds meer met elkaar verweven. Hoewel complexe producten en waardeketens niet nieuw zijn voor de Europese industrie of voor het Europese regelgevingsmodel, vereisen software en ook KI bijzondere aandacht waar het gaat om productaansprakelijkheid. Software is essentieel voor de werking van een groot aantal producten en kan van invloed zijn op de veiligheid ervan. Software is geïntegreerd in de producten, maar kan ook afzonderlijk worden geleverd om het gebruik van het product overeenkomstig de bestemming ervan mogelijk te maken. Met name zouden computers en smartphones zonder software niet echt bruikbaar zijn. Dit betekent dat software een materieel product gebrekkig kan maken en tot fysieke schade kan leiden (zie het kader over software in het deel over veiligheid). Uiteindelijk kan dit ertoe leiden dat de producent van het product aansprakelijk is op grond van de productaansprakelijkheidsrichtlijn.

Aangezien software echter in vele soorten en vormen bestaat, kan het niet altijd eenvoudig zijn antwoorden te geven in verband met de indeling van software als dienst of als product. Hoewel software die de werking van een tastbaar product kan sturen, als een onderdeel of component van dat product kan worden beschouwd, zouden sommige vormen van opzichzelfstaande software moeilijker in te delen zijn.

Hoewel de definitie van product in de richtlijn productaansprakelijkheid ruim is, zou het toepassingsgebied ervan verder kunnen worden verduidelijkt om beter rekening te houden met de complexiteit van opkomende technologieën en ervoor te zorgen dat er altijd vergoeding beschikbaar is voor schade die wordt veroorzaakt door producten die gebreken vertonen vanwege de software of andere digitale kenmerken. Dit zou economische actoren, zoals softwareontwikkelaars, beter in staat stellen te beoordelen of zij volgens de productaansprakelijkheidsrichtlijn als producenten kunnen worden beschouwd.

KI-toepassingen zijn vaak geïntegreerd in **complexe IoT-omgevingen**, waar vele verschillende geconnecteerde apparaten en diensten met elkaar in wisselwerking staan. De combinatie van verschillende digitale componenten in een complex ecosysteem en de veelheid aan betrokken actoren kunnen het moeilijk maken om te beoordelen waar mogelijke schade is ontstaan en wie daarvoor aansprakelijk is. Vanwege de complexiteit van deze technologieën kan het voor de slachtoffers zeer moeilijk zijn om de aansprakelijke partij te identificeren en alle noodzakelijke voorwaarden voor een succesvolle aanvraag aan te tonen, zoals het nationale recht eist. De kosten van deze deskundigheid kunnen economisch onbetaalbaar zijn en de slachtoffers ervan weerhouden om schadevergoeding te eisen.

Daarnaast is er sprake van wisselwerking tussen producten en diensten die op KI zijn gebaseerd en traditionele technologieën, hetgeen eveneens tot complexiteit leidt, ook wat de aansprakelijkheid betreft. Zo zullen bijvoorbeeld zelfrijdende auto's gedurende een bepaalde tijd de weg delen met traditionele auto's. In sommige dienstensectoren (zoals verkeersbeheer en gezondheidszorg), zal een soortgelijke complexiteit ontstaan met interactie tussen verschillende actoren, waarbij gedeeltelijk geautomatiseerde KI-systemen de menselijke besluitvorming ondersteunen.

Volgens het verslag[59] van de formatie nieuwe technologieën van de deskundigengroep inzake aansprakelijkheid en nieuwe technologieën kunnen aanpassingen van de nationale wetgeving ter vergemakkelijking van de bewijslast voor de slachtoffers van KI-gerelateerde schade worden overwogen. Zo zou de bewijslast kunnen worden gekoppeld aan de naleving (door een relevante exploitant) van specifieke verplichtingen inzake cyberbeveiliging of andere bij wet vastgestelde veiligheidsverplichtingen: indien deze regels niet in acht worden genomen, kan dit leiden tot wijziging van de bewijslast met betrekking tot de schuld en het oorzakelijk verband.

De Commissie verzamelt op dit ogenblik meningen over de mate waarin het noodzakelijk is om met een passend EU-initiatief de gevolgen van complexiteit te mitigeren door verlichting of omkering van de bewijslast die uit hoofde van nationale aansprakelijkheidsregels van toepassing is op schade die door het gebruik van KI-toepassingen is veroorzaakt.

Wat de Uniewetgeving betreft, zou volgens de productaansprakelijkheidsrichtlijn een product dat niet aan de verplichte veiligheidsvoorschriften voldoet, als gebrekkig worden beschouwd, ongeacht de schuld van de producenten. Er kunnen echter ook redenen zijn om na te gaan hoe de bewijslast voor de slachtoffers in het kader van de richtlijn kan worden verlicht: de richtlijn berust op de nationale regels inzake het bewijs en de vaststelling van het oorzakelijk verband.

Connectiviteit en openheid: het is momenteel niet geheel duidelijk wat de veiligheidsverwachtingen kunnen zijn met betrekking tot schade die voortvloeit uit inbreuken op de cyberbeveiliging in het product, en of deze schade afdoende zou worden vergoed uit hoofde van de productaansprakelijkheidsrichtlijn.

Er kunnen zich van meet af aan zwakke punten op het gebied van cyberbeveiliging voordoen wanneer een product in omloop wordt gebracht, maar ook in een later stadium, lang nadat het product in omloop is gebracht.

In het kader van schuldaansprakelijkheidsregelingen kan vaststelling van duidelijke verplichtingen inzake cyberbeveiliging het voor de exploitanten mogelijk maken om te bepalen wat zij moeten doen om de gevolgen van aansprakelijkheid te vermijden.

Volgens de productaansprakelijkheidsrichtlijn kan de vraag of een producent bepaalde wijzigingen heeft voorzien, rekening houdend met het redelijkerwijs te verwachten gebruik van het product, een grotere rol gaan spelen. Zo zou het bijvoorbeeld kunnen zijn dat vaker de rechtvaardigingsgrond van het later optredend gebrek wordt toegepast, die inhoudt dat een producent niet aansprakelijk is als het gebrek niet bestond op het moment dat het product in omloop werd gebracht, of de rechtvaardigingsgrond van het ontwikkelingsrisico, die inhoudt

[59] "Liability for Artificial Intelligence and other emerging technologies", verslag, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199

dat met de stand van de kennis op dat moment het gebrek niet kon worden voorzien. Daarnaast zou de aansprakelijkheid kunnen worden verminderd wanneer de benadeelde geen veiligheidsrelevante updates uitvoert. Dit zou kunnen worden beschouwd als medeschuld van de benadeelde en daardoor de aansprakelijkheid van de producent verminderen. Aangezien het begrip redelijkerwijs voorzienbaar gebruik en de kwestie van medeverantwoordelijke nalatigheid, zoals het niet downloaden van een veiligheidsupdate, vaker zouden kunnen voorkomen, kan het voor benadeelde personen moeilijker worden om vergoeding te krijgen voor schade die veroorzaakt is door een gebrek in een product.

Autonomie en gebrek aan transparantie: wanneer KI-toepassingen autonoom kunnen optreden, voeren zij een taak uit zonder dat elke stap vooraf is vastgesteld, en met minder of uiteindelijk helemaal geen directe controle of toezicht door de mens. Algoritmen op basis van machinaal leren kunnen moeilijk, zo niet onmogelijk, te begrijpen zijn ("black box"-effect").

Naast de eerder behandelde complexiteit kan het, wegens het "black box"-effect" van sommige KI, moeilijker worden om vergoeding te krijgen voor de schade die wordt veroorzaakt door autonome KI-toepassingen. De noodzaak om het algoritme en de door de KI gebruikte data te begrijpen, vereist analytische capaciteit en technische expertise die voor slachtoffers buitensporig kostbaar zouden kunnen blijken. Bovendien zou het onmogelijk kunnen blijken om toegang te krijgen tot het algoritme en de data zonder de medewerking van de mogelijk aansprakelijke partij. In de praktijk zou het derhalve zo kunnen zijn dat slachtoffers geen vordering wegens aansprakelijkheid kunnen instellen. Bovendien zou het onduidelijk zijn hoe de fout van een autonoom handelende KI kan worden aangetoond, of wat kan worden beschouwd als de fout van een persoon die gebruik maakt van KI.

In het recht van de lidstaten zijn al verschillende oplossingen ontwikkeld om de bewijslast voor slachtoffers in vergelijkbare situaties te verlichten.

Het blijft een leidend beginsel voor de productveiligheid en productaansprakelijkheid in de Unie dat het aan de producenten is om ervoor te zorgen dat alle op de markt gebrachte producten veilig zijn gedurende hun gehele levenscyclus en voor het redelijkerwijs te voorziene gebruik van het product. Dit betekent dat een fabrikant ervoor moet zorgen dat een product dat gebruikmaakt van KI, bepaalde veiligheidsparameters in acht neemt. De eigenschappen van KI vormen geen beletsel voor het bestaan van een recht op veiligheidsverwachtingen voor producten, of het nu gaat om robotgrasmaaiers of chirurgische robots.

Autonomie kan de veiligheid van het product beïnvloeden, omdat de eigenschappen van een product, met inbegrip van de veiligheidskenmerken, er aanzienlijk door kunnen worden gewijzigd. De vraag is onder welke voorwaarden zelflerende functies de aansprakelijkheid van de producent verlengen en in hoeverre de producent bepaalde wijzigingen had moeten voorzien.

In nauwe coördinatie met de overeenkomstige wijzigingen in het veiligheidskader van de Unie zou het begrip "in het verkeer brengen" dat momenteel in de productaansprakelijkheidsrichtlijn wordt gehanteerd, worden herzien om rekening te houden met het feit dat producten kunnen veranderen en gewijzigd kunnen worden. Dit kan ook helpen verduidelijken wie aansprakelijk is voor eventuele wijzigingen van het product.

Volgens het verslag[60] van de formatie nieuwe technologieën van de deskundigengroep inzake aansprakelijkheid en nieuwe technologieën zou voor de werking van sommige autonome KI-apparaten en -diensten een specifiek risicoprofiel kunnen gelden in termen van aansprakelijkheid, omdat zij aanzienlijke schade kunnen toebrengen aan belangrijke rechten, zoals het recht op leven, gezondheid en eigendom, en het grote publiek kunnen blootstellen aan risico's. Dit kan met name gelden voor KI-apparaten die zich verplaatsen in de openbare ruimte (bijvoorbeeld volledig zelfrijdende voertuigen, drones[61] en robots voor pakketbezorging) of op KI gebaseerde diensten met vergelijkbare risico's (zoals verkeersbeheerdiensten voor het sturen of controleren van voertuigen, of het beheer van elektriciteitsdistributie). Ten aanzien van de uitdagingen die autonomie en gebrek aan transparantie inhouden voor het nationale recht inzake onrechtmatige daad, zou een risicogebaseerde aanpak goed kunnen werken. Door middel van risicoaansprakelijkheidsregelingen zou kunnen worden gewaarborgd dat wanneer een risico werkelijkheid wordt, het slachtoffer een vergoeding krijgt, ongeacht waar de schuld ligt. De gevolgen van de keuze wie bij dergelijke activiteiten aansprakelijk moet zijn voor de risico's van de ontwikkeling en toepassing van KI, moeten zorgvuldig worden beoordeeld en een risicogebaseerde benadering moet worden overwogen.

Voor de werking van KI-toepassingen met een specifiek risicoprofiel peilt de Commissie de standpunten over de vraag in hoeverre risicoaansprakelijkheid, zoals die in het nationale recht is geregeld voor vergelijkbare risico's waaraan het publiek wordt blootgesteld (zoals de exploitatie van motorvoertuigen, luchtvaartuigen of kerncentrales), een noodzakelijke aanpak kan vormen om de effectieve schadevergoeding aan slachtoffers mogelijk te maken. De Commissie peilt ook de standpunten over de vraag of risicoaansprakelijkheid moet worden gekoppeld aan een mogelijke verplichting om een passende verzekering te sluiten, naar het voorbeeld van de richtlijn motorrijtuigenverzekering, om te garanderen dat de schade wordt vergoed, ongeacht de solvabiliteit van de aansprakelijke persoon, en om bij te dragen aan verlaging van de kosten van schade.

Wat betreft de werking van alle andere KI-toepassingen, die de overgrote meerderheid van alle KI-toepassingen uitmaken, gaat de Commissie na of de bewijslast inzake oorzakelijk verband en schuld moet worden aangepast. Een van de kwesties waarop in het verslag[62] van de formatie nieuwe technologieën van de deskundigengroep inzake aansprakelijkheid en nieuwe technologieën wordt gewezen, is in dit verband de situatie waarin de mogelijk aansprakelijke partij de voor de beoordeling van de aansprakelijkheid relevante gegevens niet heeft geregistreerd of niet bereid is deze te delen met het slachtoffer.

---

60 "Liability for Artificial Intelligence and other emerging technologies", verslag, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199

61 Vgl. de onbemande luchtvaartuigsystemen als bedoeld in Uitvoeringsverordening (EU) 2019/947 van de Commissie van 24 mei 2019 inzake de regels en procedures voor de exploitatie van onbemande luchtvaartuigen.

62 "Liability for Artificial Intelligence and other emerging technologies", verslag, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199

4. Conclusie

De opkomst van nieuwe digitale technologieën zoals KI, IoT en robotica, doet nieuwe uitdagingen ontstaan op het gebied van productveiligheid en -aansprakelijkheid, zoals in verband met connectiviteit, autonomie, data-afhankelijkheid, gebrek aan transparantie, complexiteit van producten en systemen, software-updates en grotere complexiteit van veiligheidsbeheer en waardeketens.

De huidige wetgeving inzake productveiligheid kent een aantal leemten die moeten worden weggewerkt, met name in de richtlijn algemene productveiligheid, de machinerichtlijn, de richtlijn radioapparatuur en het nieuwe wetgevingskader. De toekomstige werkzaamheden voor de aanpassing van een aantal wetgevingsinstrumenten in dit kader zullen op consistente en geharmoniseerde wijze plaatsvinden.

Door de nieuwe uitdagingen op het gebied van veiligheid ontstaan ook nieuwe uitdagingen op het gebied van aansprakelijkheid. Deze uitdagingen op het gebied van aansprakelijkheid moeten worden aangepakt om ervoor te zorgen dat benadeelde personen dezelfde bescherming krijgen als zij die benadeeld zijn als gevolg van traditionele technologieën, met behoud van het evenwicht met de noodzaak van technologische innovatie. Hiermee wordt bijgedragen aan het vertrouwen in deze nieuwe opkomende digitale technologieën en wordt voor investeringsstabiliteit gezorgd.

Hoewel de bestaande aansprakelijkheidswetgeving van de Unie en de lidstaten in beginsel het hoofd kan bieden aan nieuwe technologieën, kunnen de omvang en het gecombineerde effect van de uitdagingen op het gebied van KI het moeilijker maken om slachtoffers schadeloos te stellen in alle gevallen waarin dat gerechtvaardigd zou zijn[63]. De huidige regels kunnen er daardoor toe leiden dat de toerekening van kosten wanneer schade optreedt, oneerlijk of inefficiënt kan uitvallen. Om dit recht te zetten en mogelijke onzekerheden in het bestaande kader weg te werken, zou kunnen worden overwogen om door middel van passende EU-initiatieven bepaalde aanpassingen van de richtlijn productaansprakelijkheid en de nationale aansprakelijkheidsregelingen door te voeren op basis van een gerichte risicogebaseerde aanpak, die derhalve rekening houdt met het feit dat verschillende KI-toepassingen verschillende risico's opleveren.

[63] Zie het verslag van de formatie nieuwe technologieën, blz. 3 en beleidsaanbeveling 27.2 van de deskundigengroep op hoog niveau inzake kunstmatige intelligentie.