

Artificial Intelligence

(en de mythes erover)

&

Artificial Intelligence Act

Mr. Nico J. Mookhoek CIPP/E

Inhoudsopgave

Na de introductie van het spraakmakende chatprogramma ChatGPT en de daaropvolgende hype groeit de belangstelling voor Artificial Intelligence (AI), kunstmatige intelligentie.

De Europese Unie heeft al geruime tijd wetgeving voor AI in voorbereiding: de AI Act. In juni 2023 heeft het Europees Parlement deze Act goed gekeurd. Het doel is om hiermee de ontwikkeling en het gebruik van AI te reguleren maar zeker ook te stimuleren.

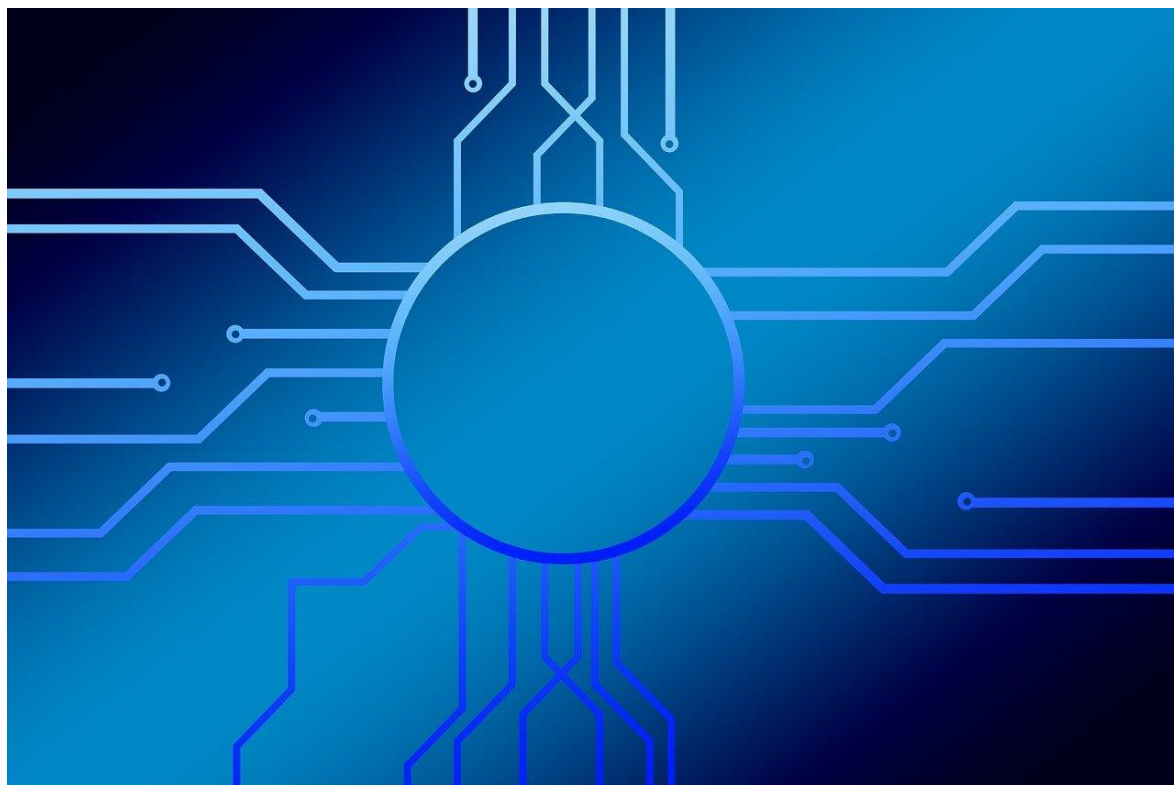
In deze White paper leggen we uit wat AI inhoudt, welke mythes er over bestaan, waar het al wordt toegepast en welke risico's er zijn.

Daarna behandelen we de AI Act op hoofdlijnen en bespreken hoe in Nederland het toezicht en de controle zijn geregeld.

Wat is Artificial Intelligence? Mythes over AI.....	2
Risico's van AI.....	5
De nieuwe Artificial Intelligence Act.....	7
Toezicht & controle	10



Wat is Artificial Intelligence (AI)?



Het begrip Artificial Intelligence is lastig te definiëren omdat het inmiddels een containerbegrip is geworden. Veel IT toepassingen krijgen, soms ten onrechte, het stempel AI. De definitie van de nationale AI-cursus geeft het meeste duidelijkheid: “AI zijn intelligente systemen die zelfstandig taken kunnen uitvoeren in complexe omgevingen en eigen prestaties kunnen verbeteren door te leren van ervaringen.”

In het kort werkt dat als volgt. De computer ontvangt grote hoeveelheden data met behulp van algoritmen maakt het daar een model van. Dat model analyseert de acties die er mee worden uitgevoerd en past zichzelf op basis van die analyse voortdurend autonoom aan. Het model verbetert dus zichzelf.

Artificial Intelligence komt in 2 vormen voor. Allereerst als software: virtuele assistentie, zoekmachines, systemen voor spraak- en gezichtsherkenning zijn

daar voorbeelden van. Daarnaast is er de zogenaamde "Belichaamde" AI: robots, zelfrijdende wagens, drones, het internet der dingen vallen onder die tweede categorie.

Mede door ChatGPT is AI enorm in de belangstelling komen te staan. Deze Chatrobot geeft vliegensvlug antwoord op jouw vragen en schrijft in een mum van tijd een tekst over elk opgegeven onderwerp, van vrije tijd tot en met professionele onderwerpen en programmeertaal. Daarmee is ChatGPT een vorm van Artificial Intelligence die razendsnel tot de grote massa is doorgedrongen.

Mythes over AI

Over AI bestaan nogal wat mythes. De meest hardnekkige is dat het Science Fiction is, dat het om futuristische toepassingen gaat. Niets is minder waar. Sommige AI-technologieën dateren al uit de jaren 50 van de vorige eeuw. In diverse sectoren wordt AI al langere tijd toegepast. Het zorgt er nu al voor dat je na het online winkelen gepersonaliseerde advertenties gebaseerd op je koopgedrag ontvangt, het schotelt je nu al op basis van je kijkgedrag nieuwe videootjes en films voor op YouTube en Netflix, het leest röntgenfoto's en herkent bij kankeronderzoek patronen in kankercellen.

Wel kent de technologie de laatste jaren grote doorbraken waardoor de toepassingen in een stroomversnelling zijn gekomen. Dit komt omdat de hoeveelheden beschikbare data waarmee AI getraind wordt gigantisch zijn toegenomen, de rekenkracht van computers exponentieel is gegroeid en er veel nieuwe algoritmes zijn ontwikkeld.

Een tweede mythe is dat AI slimmer dan de mens is. AI heeft weliswaar veel potentie en wordt ook steeds geavanceerder. Maar het kan, volgens de heersende opinie, nog steeds niet vergeleken worden met de menselijke intelligentie. In de basis is AI gebaseerd op heel geavanceerde wiskunde en statistiek. Dat betekent dat de techniek geen empathie kan tonen of gevoel kan uiten zoals de (meeste) mensen dat kunnen. Met dit laatste is overigens niet iedereen het eens. Elon Musk stelt: "robots zullen alles beter kunnen dan mensen".

Als laatste wordt AI nogal eens gezien als een bedreiging voor het werk van mensen. Inderdaad zal de inzet van AI bepaalde soorten mensenwerk overbodig maken.

Uit onderstaande toepassingen blijkt dat AI vooral ingezet wordt ter ondersteuning van medewerkers en voor repetitieve werkzaamheden, waar het vaak ook nog beter in is.

Om bij ChatGPT te blijven: grote delen tekst kunnen prima geschreven worden door die chatrobot. Echter: menselijke controle en aanpassing op die teksten is op dit moment nog nodig.

Het gerenommeerde internationale advocatenkantoor Allen & Overy claimt dat met de inzet van AI de legal professionals beter ondersteund wordt. Zij gebruiken daarvoor een systeem met de naam Harvey. Een innovatief artificial intelligence platform op basis van het Open AI model, dat ook weer de basis voor ChatGPT is.

Bij klantenservice wordt AI ook steeds meer ingezet. Iedereen kent ze wel: de chatbots die in je scherm verschijnen en vragen waar ze je mee kunnen helpen. Deze chatbots kunnen het gros van de klantvragen beantwoorden. Menselijke medewerkers kunnen zich dan richten op de complexere zaken.

Uit een Zweeds onderzoek uit 2023 blijkt dat AI borstkanker zelfs vaker herkent en minder false positieven constateert dan radiologen. Een Nederlandse radioloog die gevraagd werd naar de uitkomsten van het Zweedse borstonderzoek gaf de volgende verklaring. Radiologen bekijken in korte tijd veel mammogrammen, 99% is normaal maar eentje niet, die moet de radioloog er uit halen. "Een mens krijgt behoefte aan koffie of raakt afgeleid, maar AI heeft hier simpelweg geen last van".

Natuurlijk is het onvermijdelijk dat door AI-systemen banen verdwijnen. Uit recente rapporten van onder meer PwC, McKinsey en Deloitte blijkt dat de komende jaren circa 4 procent van de banen daadwerkelijk zal worden vervangen. Maar nog veel interessanter: 96 procent van de banen zal inhoudelijk door toepassing van AI veranderen.

AI-systemen zorgen ook voor nieuwe banen. Een voorbeeld daarvan is de zogenaamde prompt writer, een persoon die de goede opdracht formuleert voor het AI-model.



Risico's van AI



AI kent dus mooie en nuttige toepassingen maar herbergt ook een aantal risico's. Het grootste risico is de zogenaamde Bias, vertekeningen in de data of in het algoritme. De uitkomsten van AI zijn immers afhankelijk van het algoritme en de data waarmee het gevoed wordt. Beiden kunnen onbedoeld of opzettelijk onjuist of manipulatief zijn.

Een AI-systeem dat wordt gevoed met bevooroordeelde data geeft discriminerende uitkomsten. Ofwel "rubbish in, rubbish out". Check daarom de data waarmee het systeem wordt gevoed: zijn ze een goede afspiegeling van de maatschappij of van de klantenkring van de organisatie. Wees transparant over de data waarmee het systeem wordt gevoed. Ook dat helpt om vertekening te voorkomen.

Het risico van vertekening kan naast de data ook liggen in het algoritme. Als sommige belangrijke aspecten van een probleem niet in het algoritme geprogrammeerd zijn, geeft het bevooroordeelde uitkomsten. Of als het algoritme bewust is geprogrammeerd om structurele vooroordelen weer te geven en te herhalen.

Zoals we boven al schreven is een AI systeem niks meer of minder dan een geavanceerd wiskundig systeem en statistieken. Het gebruikt getallen om

bijvoorbeeld een ingewikkelde sociale situatie voor te stellen. Daarmee creëert het een mythe van feitelijkheid en precisie, terwijl de praktijk veel weerbarstiger en genuanceerder is.

Kortom, wanneer AI niet goed wordt uitgevoerd, kan het tot onjuiste of gemanipuleerde beslissingen leiden.

AI heeft ook een aanzienlijke impact op het recht op privacy en de bescherming van persoonsgegevens. Denk daarbij aan systemen voor gezichtsherkenning of AI die gebruikt wordt om personen te traceren en profileren. Het met AI verwerken van persoonsgegevens uit verschillende bronnen tot nieuwe persoonsgegevens is ook een risico. Omdat het systeem gegevens uit verschillende contexten haalt en daarmee een nieuw profiel genereert, kan de uitkomst onverwacht en niet gewenst zijn voor de betreffende persoon. De gegevens die uit de oorspronkelijke context zijn gehaald, krijgen een andere waarde.

Naast onbedoeld, kan de uitkomst soms ook gewoon foutief zijn. ChatGPT maakte een aantal keren pijnlijke fouten bij het genereren van een persoonlijk profiel. Zo berichtte de Washington Post laatst over een hoogleraar die volgens het door ChatGPT gegenereerde profiel veroordeeld was voor pedofilie. Dit was echter niet het geval, de hoogleraar overweegt nu een rechtszaak tegen ChatGPT.

Kortom, AI kent schitterende toepassingen maar herbergt ook een aantal potentiële risico's. Dit is ook de reden dat de Europese Unie, de AI Act heeft opgetuigd. Enerzijds om de ontwikkeling en toepassing van AI te reguleren, anderzijds om met deze set regels de ontwikkeling te stimuleren.



De nieuwe Artificial Intelligence Act



In juni 2023 stemde het Europees parlement in met de nieuwe AI Act. Dat betekent dat vertegenwoordigers van het EP met de Raad van de EU (de Raad van Ministers) gaan onderhandelen over de definitieve tekst. De verwachting is dat dit geen grote aanpassingen zal opleveren. In deze White paper nemen we daarop vast een voorschotje door de belangrijkste regels op een rijtje te zetten.

Voor wie geldt de Act?

In principe is de reikwijdte van de AI Act heel breed. De regels gelden onder meer voor ontwikkelaars van AI-systemen, importeurs en distributeurs van AI-systemen, partijen die reeds ontwikkelde AI in hun eigen softwarediensten opnemen en gebruikers die dergelijke diensten inzetten. Iedereen die dus op welke wijze dan ook AI gebruikt, moet zelfstandig kunnen aantonen dat aan AI Act wordt voldaan.

Ook de zogenaamde basismodellen vallen onder de reikwijdte van de Act. Basismodellen zijn modellen die niet voor een specifieke toepassing zijn ontwikkeld. Zij bevatten grote hoeveelheden data, maar ondanks hun complexiteit zijn ze vrij eenvoudig te tweaken naar een specifieke toepassing. Vergelijk het met ChatGPT dat als basismodel specifiek geschikt gemaakt wordt voor juridische toepassingen (Harvey).

De AI act op hoofdlijnen: de belangrijkste uitgangspunten.

1. Verantwoordelijkheid: de verantwoordelijkheid wordt bij de ontwikkelaars en gebruikers van AI-systemen gelegd. Zij moeten kunnen aantonen dat hun systemen betrouwbaar, veilig en ethisch zijn. Dat betekent dat de ontwikkelaar van een specifieke toepassing op basis van een basismodel dus ook de werking hiervan moet kennen. In het geval van schade of negatieve gevolgen door AI, kunnen zij aansprakelijk worden gesteld
2. Transparantie: AI-systemen moeten transparant zijn over hun functionaliteit en besluitvormingsprocessen. De gebruikers moeten begrijpen hoe het AI-algoritme tot bepaalde uitkomsten komt en welke data er worden gebruikt.
3. Privacy: Privacybescherming is een essentieel aspect van de wetgeving. AI-systemen moeten voldoen aan strikte regels met betrekking tot het verzamelen, opslaan en gebruiken van persoonlijke gegevens. Dit helpt de privacy van individuen te waarborgen en misbruik van gegevens te voorkomen.
4. Menselijke controle: De Nieuwe AI Act benadrukt het belang van menselijke controle over AI-systemen. Hoewel AI veel taken efficiënter kan uitvoeren dan mensen, moet de uiteindelijke besluitvorming in handen blijven van menselijke operators. Dit voorkomt ongewenste afhankelijkheid van AI en waarborgt menselijke waarden en ethiek.

Risico gestuurde classificatie

De Act is risico gestuurd en onderscheidt verschillende risicocategorieën.

Onacceptabele risico's. Systemen die een onacceptabel risico voor de rechten en vrijheden van het individu vormen, zijn verboden. Voorbeelden daarvan zijn social scoring en zogenaamde manipulatieve AI-systemen.

De Act beschrijft manipulatieve systemen als systemen die bijvoorbeeld gebruik maken van de kwetsbaarheid van een specifieke groep personen zoals leeftijd of handicap om het gedrag op schadelijke wijze te verstoren.

Hoog risico AI-systemen met een hoog risico krijgen een aantal nieuwe verplichtingen. Deze komen naast bestaande verplichtingen uit bijvoorbeeld de Algemene Verordening (AVG). De nieuwe verplichtingen moeten er voor zorgen dat de risico's aantoonbaar beheerst worden. Zo moet onder andere inzichtelijk worden gemaakt met welke data het systeem getraind wordt, waar komen die vandaan komen, hoe biases en discriminatie uitgesloten zijn. In een bijlage bij de AI Act zijn de hoog risico systemen opgesomd.

Laag risico Daarnaast bevat de AI Act transparantieplichtingen voor AI-toepassingen die een beïnvloedend karakter (kunnen) hebben zoals chatbots of deepfakes. Die transparantie moet er voor zorgen dat niemand denkt met een mens van vlees en bloed van doen te hebben.

Invoering

De verwachting is dat er niet veel wijzigingen uit de onderhandelingen komen zou de Act vrij snel ingevoerd kunnen worden. Algemeen wordt verwacht dat de Act begin 2024 in werking zal treden.



Toezicht en controle



AUTORITEIT PERSOONSgegevens

In Nederland is het toezicht en controle op AI neer gelegd bij de Autoriteit Persoonsgegevens (AP).

De AP ziet toe op de ontwikkeling en het gebruik van algoritmes en AI. Het doel hiervan is om het gebruik, discriminatie en willekeur door gebruik van algoritmes beter te controleren en transparantie te bevorderen.

Binnen AP is daarvoor een apart organisatieonderdeel opgericht: de directie Coördinatie Algoritmes (DCA). De werkzaamheden van de DCA staan los van de reguliere toezichtstaken van de AP wanneer algoritmes persoonsgegevens verwerken.

Dit jaar richt de DCA zich op risicosignalering, het versterken van bestaande samenwerkingen bij algoritmetoezicht, en gezamenlijke en sector overstijgende normuitleg. Aan het einde van 2023 verschijnt een gezamenlijk rapport om de ontwikkelingen in het algoritmetoezicht en de risico's van algoritmes inzichtelijk te maken.

In juli 2023 publiceerde het DCA al haar eerste tussentijdse rapport. Daarin signaleert het DCA dat Innovaties zoals intelligente chatbots en gebrekkig inzicht in bestaande algoritmes op dit moment de belangrijkste algoritmerisico's zijn.



Bronnen:

Nieuws Europees Parlement

<https://www.europarl.europa.eu/news/nl/headlines/society/20200827STO85804/wat-is-artificiele-intelligentie-en-hoe-wordt-het-gebruikt>

Kunstmatige intelligentie in 60 minuten- Remy Gieling en Job van den Berg

Nieuws Erasmus Universiteit Rotterdam: <https://www.eur.nl/nieuws/wat-het-verschil-tussen-data-science-machine-learning-en-ai>

AI-cursus: <https://www.ai-cursus.nl>

Website advocatenkantoor Allen & Overy: <https://www.allenoverly.com/en-gb/global/news-and-insights/news/ao-announces-exclusive-launch-partnership-with-harvey>

Website Autoriteit Persoonsgegevens:

<https://www.autoriteitpersoonsgegevens.nl/themas/algoritmes-ai/coordinatie-toezicht-algoritmes-ai>



Heb je hulp nodig bij de juridische aspecten van de ontwikkeling van AI? Wil je een overzicht wat de AI Act voor jouw organisatie betekent? Of wil je Privacy by Design toepassen bij een nieuwe AI toepassing? Wij helpen je graag!

Maak meteen een afspraak voor een online consult [op de website](#)



info@deprivacyguru.nl



085-2223232

DePrivacyGuru: "Privacy zonder gedoe"