Q&A – Webinar AI Act

Definitie van AI

Q Wat is het verschil tussen algoritmen en AI?

A AI staat voor Artificiële Intelligentie, ook wel kunstmatige intelligentie genoemd. Dit is een verzamelnaam voor algoritmen waaronder Machine Learning (incl. Neurale Netwerken en Deep Learning). Een algoritme is niets anders dan een berekening of model die door een computer wordt uitgevoerd waarmee input wordt vertaald richting een output.

A Niet elk algoritme is AI. Wel bevat elke AI-systeem minstens één of meerdere algoritmen.

A Het voorstel van de van de Europese Commissie voor een AI Act hanteert zo'n brede definitie van AI-systemen dat ook ander typen algoritmen onder deze definitie vallen. In andere voorstellen wordt een andere definitie gehanteerd. Dit is de reden dat we met name praatten over algoritmen en algoritmetoepassingen in onze webinar.

Q Als een systeem 'enige mate van autonomie' heeft, dan valt het onder de AI Act. Dan zouden toch ook systemen die niet per sé ML bevatten eronder vallen; zoals 'gewone' algoritmische besluitvorming?

A Dat klopt. Ook een beslisboom die regelgebaseerd is – vaak een directe vertaling van wet- en regelgeving en/of beleid - kan autonoom worden ingezet.

Q Ook relatief eenvoudige computersystemen kunnen vergaande consequenties hebben voor een individu. Als AI act geen bescherming hiervoor biedt, welke EU wetgeving zou dan wel kunnen beschermen? Of is dat dan een 'blinde vlek'?

A Dat hangt erg van de context af. Onder meer de AVG, maar ook maar algemene basisbeginselen kunnen in zo'n geval bescherming bieden. De AI Act beoogt enkele AI-specifieke risico's te adresseren, zoals autonome karakter en gebrek aan transparantie.

Q Wordt met 'generieke AI' 'generatieve AI' bedoeld?

A Nee, generatieve AI kan wel een vorm zijn van generieke AI. Het maken van bepaalde content kan namelijk voor meerdere doeleinden worden toegepast (generiek). Op het moment dat je generatieve AI in een bepaald proces gebruikt voor een specifiek doel wordt het een toepassing. Andere vormen van een generieke AI zijn bijvoorbeeld modellen waarmee je eenvoudig een tijdsreeks kan voorspellen of classificeren.

Q Wat is het verschil tussen foundation models en general purpose AI?

A Een 'foundation model' is een basis om op verder te bouwen (structuur) en 'general purpose AI' een systeem dat voor meerdere doeleinden direct inzetbaar is. Beiden worden genoemd in het voorstel van het Europese Parlement voor de AI Act.

Q Wordt open source uitgezonderd van de AI Act? En wat zou een reden kunnen zijn om open source uit te zonderen van de AI act?

A In het voorstel voor een AI Act van het Europees Parlement wordt een uitzondering gemaakt voor free and open-source AI. De vraag is of dat voorstel standhoudt. De reden daarvoor is dat in ieder het geval het Europees Parlement lijkt te willen

voorkomen dat initiatieven waarin ontwikkelaars zonder commercieel oogmerk samen werken aan AI en die op openbare repositories plaatsen aan alle voorwaarden van de AI Act hoeven te voldoen. Het Parlement lijkt te vrezen dat dat er toe zou leiden dat dergelijke initiatieven niet meer zullen plaatsvinden, en acht dat onwenselijk.

Q Wat is de huidige stand van de "uitzondering" voor toepassingen voor militaire doelen en nationale veiligheid?

A Het gebruik van AI voor militaire doeleinden valt in beginsel buiten de AI Act. Dat zal vermoedelijk niet veranderen.

Q Als een call center vooraf zegt "dit gesprek wordt opgenomen voor trainingsdoeleinden" dan zou dat ook kunnen betekenen dat de opnames automatisch worden verwerkt met behulp van spraakherkenning en tekst mining evenals input voor de 'training van een AI systeem'. Deze opnamen bevatten biometrische gegevens. Mogen deze cases onder de AI Act?

A Het gebruik van biometrische gegevens is niet in algemene zin verboden op grond van de AI Act. Wel in beginsel verboden is het gebruik van biometrische systemen voor de identificatie op afstand in real time in openbare ruimten met het oog op de rechtshandhaving.

Q Is er een algemene longlist/shortlist al ergens beschreven waarmee AI-toepassingen geïnventariseerd kunnen worden?

A Dit is sector en domein afhankelijk. Je kunt inspiratie opdoen in het landelijke algoritmeregister. Hier kun je zien wat overheidsinstanties tot nu toe geïdentificeerd, geregistreerd en gepubliceerd is. Dit is nog niet volledig.

Termijn

Q Is bekend wanneer de trialoogsessie plaatsvinden over de AI Act? Is er al planning?

A Uit de trialoogsessies volgt een definitieve versie. Deze sessies vinden op dit moment plaats. De verwachting is dat dit jaar een definitieve versie van de AI ACT naar het parlement gaat voor goedkeuring in q1 2024. De inwerkingtreding is dan 2 jaar later in 2026.

Betrokken Partijen

Q Wie moet aan de basisbeginselen van AI systeem voldoen? De aanbieder? of ook de gebruiker die het gebruikt in zijn communicatie/processen met burgers?

A De AI Act bevat zowel verplichtingen voor de aanbieder als de gebruiker. In welke mate er verplichtingen op deze partijen rusten, hangt af van of sprake is van een AI-systeem met een hoog risico of niet.

Q Over AI-productieketen: die wordt ontwikkeld voor sommige AI producten, als één bedrijf de data verzamelt, een ander het model traint en beschikbaar stelt (bijv. open source) en iemand anders bouwt daar weer iets boven op. Wie is dan verantwoordelijk?

A Dat hangt uiteraard sterk af van de precieze omstandigheden van het geval. In beginsel rusten op grond van de AI Act de meeste verplichtingen op de partij die een AI Systeem op de markt brengt. Ook op de gebruiker rusten verplichtingen. Het kan ook zo zijn dat één partij beide rollen vervult.

Q Maakt het bij de AI-systemen nog uit wie het gebruikt? Wordt daarbij onderscheid gemaakt of je een systeem dan wel of niet mag gebruiken?

A Of een AI-systeem op grond van de AI Act als hoog risico wordt aangemerkt, hangt af van de toepassing. Sommige toepassingen, bijvoorbeeld de opsporing, kunnen alleen door specifieke partijen worden uitgevoerd. In zoverre maakt het dus uit wie het systeem gebruikt.

Q Wie stelt de handleiding op die de gebruiker moet volgen?

A Deze verplichting rust op grond van de AI Act op de partij die het systeem op de markt brengt.

Q Wie beoordeelt binnen een organisatie of een systeem aan de voorwaarden voldoet?

A Beoordeling vindt plaats op meerdere niveaus naar eigen voorwaarden en wet-regelgeving:

- Werken volgens standaarden / Vier-ogen principes
- Interne en externe toetsing
- Extern toezichthouder (nationaal)

Q Wie wordt de formele toezichthouder op de AI Act

A Voor nu ligt het toezicht op algoritmen waarbij persoonsgegevens worden verwerkt bij Autoriteit Persoonsgegevens. Het is nog onzeker wie de toezichthouder zal worden op grond van de AI Act.

Q Kun je 3 slimme vragen formuleren die een gebruiker aan een aanbieder kan stellen als het gaat om prestatie AI-systeem?

A Laten we beginnen met maar liefst 4 vragen:

1. Zijn er benchmarktests of onafhankelijke evaluaties beschikbaar die de nauwkeurigheid van het systeem hebben gemeten? Zo ja, wat waren de resultaten van deze tests?
2. Zijn er specifieke doelgroepen of contexten waarin het systeem minder nauwkeurig is, waar blinde vlekken zijn of waar de kans op overrepresentatie groot is?
3. Hoe en hoe vaak worden de prestaties van het AI-systeem gemonitord?
4. Hoe kan ik melding maken van fouten in de uitkomst?

Uiteraard belangrijk om meer vragen te stellen. Neem contact op met Sabine als je meer wilt weten over de 68 punten om een AI-systeem op te toetsen.

Q AI heeft zoveel verschillende facetten, is een algoritme expert dan niet een te eenzijdige kijk op AI toezicht?

A Het gaat hier om een nieuwe rol bovenop bestaande governance. Een algoritme officer is in relatie tot de AI ACT, wat een privacy officer is i.r.t. de AVG. Deze rol kan niet vervuld worden zonder enige kennis van AI, andersom moet kennis van bijvoorbeeld data management, privacy, informatiebeheer en -beveiliging voldoende aanwezig te zijn om als spin in het web te kunnen acteren in samenwerking met bestaande compliance rollen en andere aanvullende disciplines.

Q Begrijp ik het goed dat de commerciële aanbieder van AI systemen verantwoordelijk is voor het uitvoeren van mensenrechtenassessments? Mag je daar dan als gebruiker/gemeente op vertrouwen?

A De laatste versie van de AI Act verplicht de *gebruiker* (deployer) van een AI-systeem met een hoog risico om een mensenrechtenassessment uit te voeren.

Ethiek

Q Komt er ook een ethisch toetsingskader?

A Impact Assessment Mensenrechten en Algoritmen (IAMA) is een voorbeeld van een assessment die ingezet kan worden om ethische afwegingen te maken. Op grond van de laatste concept versie van de AI Act wordt een dergelijke assessment verplicht voor hoog risico AI-systemen. Dit is een instrument om de ethische afweging te ondersteunen en maatregelen te nemen om grondrechten na te leven. Op dit moment is de IAMA een gebruikelijke standaard. Het is niet ondenkbaar dat dit zich verder ontwikkeld (verbetering, light versie) of andere standaarden ontwikkeld gaan worden.

Q Wie bepaalt wat een “juist” gebruik voor een doel is?

A Per systeem stelt de organisatie van tevoren eisen vast: waar moet het aan voldoen (beleid) op basis van het risiconiveau en de kosten van fouten wil en moet je de lat hoger leggen. Of het gebruik voldoende past bij het doel is een afweging die de verantwoordelijke in de organisatie moet maken.

Data

Q Ook al is het AI neutraal, wanneer je de AI met selecte data voedt, kan het behoorlijk mis gaan. Hoe gaat de AI Act in op het gevaar van bias in (trainings)data?

A Data is onlosmakelijk verbonden met de kwaliteit van het AI-systeem. De AI Act schrijft voor dat voorafgaand aan het op de markt brengen van een AI Systeem met een hoog risico, aan bepaalde voorwaarden moet worden voldaan op het gebied van datamanagement, die onder meer ongewenste bias moeten voorkomen.

Q Wat bedoel je in thema's voor toetsing met 'integer' gebruik van data?

A Hoe het model tot stand komt en op welke manier verwerkt het algoritme de data verwerkt tot nieuwe resultaat en vinden hier geen ongewenste aanpassingen plaats die de resultaten beïnvloeden. Dit betekent onder andere: fit-for-purpose data, reproduceerbaarheid van gegevens in zowel training-, test-, validatie- als voorspeldata en passende aannames voor een voldoende goede representatie van de werkelijkheid.

Transparantie

Q Transparantie zit op meer niveaus. Onder andere dat je te maken hebt met AI, hoe een beslissing tot stand is gekomen, welke positie de algoritmische besluitvorming in een proces heeft. Vooral bij transparantie over hoe een besluit tot stand is gekomen kan ik me voorstellen dat daar ook een stukje bedrijfsgeheim in zit. Ook wil je ‘playing the system’ voorkomen. Hoe transparant kan/wil/mag je daar dan over zijn?

A Dat hangt erg af van de situatie. In de standaardvoorwaarden voor de inkoop van algoritmen van de Gemeente Amsterdam, opgesteld door Jeroen, worden drie vormen van transparantie onderscheiden (Technische transparantie, Procedurele transparantie en Uitlegbaarheid) teneinde dit issue te adresseren.

–

Deze antwoorden op de gestelde vragen kunnen niet worden beschouwd als adviezen van VKA en/of Pels Rijcken. Zij zijn gegeven zonder de precieze context van de vraag te kennen en beogen een algemeen beeld te schetsen over AI, algoritmen en de AI Act. Hebt u wel advies nodig over één van deze onderwerpen, neem dan vooral contact op met uw adviseurs.