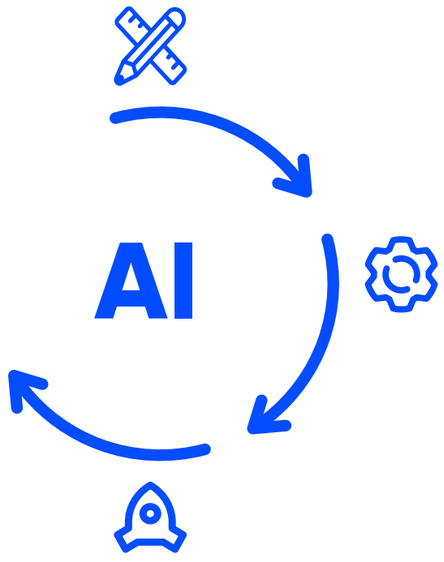
HOE IS DE AI-LEVENSCYCLUS GEREGULEERD ?

Verscheidene juridische regimes zijn van toepassing op ontwikkelaars tijdens de levenscyclus van een AI-systeem. In deze brAInfood bekijken we verschillende van deze regimes tijdens verschillende fasen in de AI-levenscyclus. We bespreken de meest relevante regimes, zonder exhaustief te zijn.

Kenniscentrum Data & Maatschappij (januari 2024). Hoe is de AI-levenscyclus gereguleerd? Brussel: Kenniscentrum Data & Maatschappij.



Kenniscentrum Data & Maatschappij

Artificiële Intelligentie Vlaanderen

ONTWERP

Tijdens de ontwerpfase wordt het probleem gedefinieerd waarvoor het AI-systeem een oplossing biedt. Data wordt verzameld, verwerkt en verdeeld in trainings-, validatie- en testdata.

CONTRACTENRECHT

Trainingsdata, bestaande modellen en andere tools zoals computerkracht kunnen onderworpen zijn aan licenties of andere contractuele voorwaarden. Ontwikkelaars moeten de voorwaarden van hun overeenkomsten goed controleren en volgen wanneer ze deze tools gebruiken.

AI VERORDENING

De Verordening hanteert een risico-gebaseerde aanpak om AI-systemen op te delen in vier categorieën: verboden, hoog-risico, beperkt risico en minimaal risico. Data gebruikt in de ontwikkeling van een hoog-risico AI-systeem moeten voldoen aan bepaalde kwaliteitscriteria (zoals relevantie, volledigheid, etc.).

GEGEVENSBESCHERMING

De **AVG** is van toepassing op de verzameling, het gebruik en andere verwerkingen van persoonsgegevens. Als persoonsgegevens nodig zijn voor de training van een AI-systeem, dan moeten ontwikkelaars de AVG-verplichtingen respecteren. Deze verplichtingen zijn breed en omvatten onder meer minimale gegevensverwerking, een rechtmatige verwerkingsgrond en doelbinding (met uitzonderingen voor algemeen belang en statistische doeleinden).

ANDERE

Auteursrecht: Als de data waarmee een AI-systeem wordt getraind literaire of artistieke werken bevat dan zijn deze beschermd door het auteursrecht. De reproductie van deze data vereist de toestemming van de houder van het auteursrecht, behalve wanneer uitzonderingen voor tekst- en datamining toepasselijk zijn.

Data Verordening: Deze Verordening bevat rechten voor de eerlijke toegang tot en het eerlijk gebruik van data. Hieronder vallen toegangsrechten op data uit verbonden producten en regels voor oneerlijke bedingen rond toegang tot en gebruik van data. Ontwikkelaars moeten zich bewust zijn van deze mechanismen en van oneerlijke bedingen die ze niet moeten aanvaarden.

Deontologische of professionele geheimhoudingsplichten: Als trainingsdata ontstaan of gebruikt worden bij een gereguleerd beroep, dan kunnen bepaalde geheimhoudingsplichten van toepassing zijn die het (her)-gebruik van de data verhinderen.

ONTWIKKELING

In de ontwikkelingsfase wordt het AI-systeem gemaakt. Het AI-systeem wordt getraind met data en verbeterd door herhaaldelijke aanpassingen. Het wordt verder getest en scherp gesteld zodat het geschikt is voor haar doel.

CONTRACTENRECHT

Overeenkomsten moeten worden opgesteld voor de ontwikkeling, de eigendom, het gebruik, en het delen van het AI-systeem en haar outputs. De eigendomsrechten op de algoritmen, software, datasets en andere intellectuele eigendommen die in deze fase worden ontwikkeld moeten duidelijk zijn, met inbegrip van ontwikkelingen door onderaannemers en werknemers. Andere contractuele beschermingen (bv. geheimhouding) kunnen ook nodig zijn.

AI VERORDENING

Ontwikkelaars van hoog-risico AI-systemen moeten voldoen aan verplichtingen rond risicobeheer, technische documentatie, transparantie, registratie, menselijk toezicht etc. Bepaalde hoog-risico AI-systemen zullen ook onderhevig zijn aan een grondrechteneffectbeoordeling voor gebruik.

GEGEVENSBESCHERMING

Een **gegevensbeschermingseffectbeoordeling (GEB)** kan helpen bij het vinden van gegevensbeschermingsrisico's en gerelateerde oplossingen. Zo kunnen de nodige beschermingsmaatregelen worden genomen en in het AI-systeem worden ingebouwd.

Door ontwerp: Gegevensbeschermingsbeginselen moeten in het ontwerp van het AI-systeem worden ingebouwd door technische middelen (waar mogelijk). Dit gaat onder andere over het inbouwen van minimale gegevensverwerking (door anonieme of pseudonieme data) of opslagbeperkingen (door gegevens automatisch te verwijderen).

Door standaardinstellingen: Het AI-systeem moet worden ontwikkeld zodat het bij gebruik standaardinstellingen heeft die gegevensbescherming waarborgen (bijvoorbeeld enkel persoonsgegevens verzamelen die noodzakelijk zijn voor het doel van het systeem).

ANDERE

Technische normen en standaarden: Deze zijn cruciaal om de kwaliteit en veiligheid van AI-systemen te verzekeren. Bepaalde geharmoniseerde (EU-) standaarden geven de ontwikkelaar ook een vermoeden van conformiteit (bv. Verordening algemene productveiligheid en Cybersecurity verordening) of laten toe om interne conformiteitsbeoordelingen te gebruiken (bv. AI Verordening).

Octrooirecht: Naast hardware kunnen nieuwe software, datastructuren en formaten beschermd worden onder het octrooirecht als ze een technisch karakter hebben en de andere octrooivoorwaarden vervullen. Ontwikkelaars moeten zich bewust zijn dat het gebruik van geoctrooieerde technieken toestemming vereist.

IMPLEMENTATIE

Eens een AI-systeem voldoende getest is en aan haar operationele voorwaarden voldoet, kan het worden ingezet in echte omstandigheden.

CONTRACTENRECHT

De ontwikkelaar moet algemene voorwaarden (B2C en/of B2B) bezorgen aan de gebruikers voor ze het AI-systeem gebruiken om de voorwaarden, beperkingen en verwachtingen voor het gebruik van het systeem te duiden.

AI VERORDENING

Verscheidene hoog-risico AI-systemen moeten een conformiteitsbeoordeling (intern of via derde partij) ondergaan voor ze op de markt worden gebracht of worden gebruikt. Bepaalde hoog-risico AI-systemen moeten ook worden geregistreerd in een EU-database. Sommige AI-systemen moeten aan bepaalde transparantieverplichtingen voldoen. Ontwikkelaars van hoog-risico AI-systemen moeten corrigerende stappen ondernemen als hun AI-systeem op de markt niet conform is met de AI Verordening en moeten zich bewust zijn van mogelijke klachten van personen die door het systeem worden beïnvloed.

GEGEVENSBESCHERMING

AVG: Verwerking van persoonsgegevens in een AI-systeem moet gebeuren op basis van een rechtmatige verwerkingsgrond en op een transparante, eerlijke manier. Een ontwikkelaar moet betrokkenen toelaten hun rechten uit te oefenen. Indien relevant moeten de beperkingen op geautomatiseerde besluitvorming ook in overweging worden genomen.

ANDERE

Consumentenbescherming: Wanneer consumenten betrokken zijn moeten bepaalde informatieverplichtingen, regels rond oneerlijke handelspraktijken en vereisten voor toestemming worden gerespecteerd door de ontwikkelaar, zowel wanneer AI-systemen onderwerp zijn van een overeenkomst als wanneer ze gebruikt worden om een overeenkomst te sluiten.

Auteursrecht: Ontwikkelaars moeten vrijwaringen of garanties bieden voor de resultaten van een AI-systeem. In het bijzonder moeten ze hun positie bepalen rond resultaten die inbreuk maken op de auteursrechten van derden.

Digitaledienstenverordening: Het gebruik van automatische inhoudsmoderatie (inclusief AI-systemen) moet door tussenhandelsdiensten, hostingdiensten en online platformen worden gerapporteerd, samen met andere transparantieverplichtingen.

Aansprakelijkheid

- Contractuele aansprakelijkheid: Ontwikkelaars kunnen contractueel aansprakelijk zijn als hun systeem niet correct presteert of op een andere manier niet voldoet aan hun overeenkomsten.
- Buitencontractuele aansprakelijkheid: Gebruik van een AI-systeem kan leiden tot buitencontractuele aansprakelijkheid. Het voorstel voor een AI-aansprakelijkheidsrichtlijn voegt regels toe voor het ontsluiten van bewijs en vermoedens in het voordeel van de eiser van een schadeclaim door een AI-systeem.
- Productaansprakelijkheid: producenten zijn aansprakelijk voor schade die veroorzaakt wordt door hun producten, onafhankelijk van hun eventuele nalatigheid (EU productaansprakelijkheidsrichtlijn).