

AI-forordningen i trilogforhandlinger

Trilogforhandlingerne mellem Europa-Parlamentet, Europa-Kommissionen og Ministerrådet om AI-forordningen er i gang. De har hver deres ønsker til den nye lovgivning, fx en udvidet liste over forbudte AI-systemer og strenge krav til transparens for udbydere af ChatGPT og lignende modeller.

Kunstig intelligens er en teknologi, som har taget verden med storm. Den hastige udvikling og de mange muligheder, som den fører med sig, har fundamentalt ændret menneskets forhold til teknologi. Den nok største teknologiske milepæl i mange år er tilgængeliggørelsen af kunstig intelligens baseret på avancerede sprogmodeller i forbindelse med chatbotter, herunder "ChatGPT" fra OpenAI og "Bard" fra Google.

Mulighederne med denne type kunstig intelligens lader til kun at begrænses af menneskets egen fantasi. Lovgivning på området er på vej, men indtil EU's kommende forordning om kunstig intelligens ("AI-forordningen")

er på plads, må vi bruge den regulering og de juridiske værktøjer, vi allerede har, til at guide os igennem de mange problemstillinger, som anvendelsen af kunstig intelligens giver anledning til.

Status på AI-forordningen

Rådet i EU vedtog oplæg til forhandling af AI-forordningen 25. november 2022. Europa-Parlamentet vedtog sin forhandlingsposition til forordningen om kunstig intelligens med hele 499 stemmer for, 28 imod og 93 hverken for eller imod 14. juni 2023. Forordningen er således videre til trilogforhandlingerne mellem Europa-Parlamentet, Europa-Kommissionen og Ministerrådet, hvor målet er at nå til

enighed om en endelig tekst for AI-forordningen i slutningen af 2023.

Udvidelse af listen over forbudte AI-systemer

Rådet ønsker at udvide listen over forbudte AI-systemer til at omfatte private aktørers brug af AI til social scoring. Rådet har også ønsket at udvide det allerede eksisterende forbud mod at bruge AI-systemer, der udnytter sårbarhederne hos en bestemt gruppe af personer, til også at omfatte personer, der er sårbare på grund af deres sociale eller økonomiske situation.

Parlamentet vil forbyde brugen af biometriske identifikationssystemer i EU. Dette gælder både for brugen af disse systemer i realtid - hvilket også fremgik af Kommissionens udspil - og også efterfølgende brug, dog med enkelte undtagelser.

Parlamentet ønsker derudover at forbyde:

1. alle biometriske kategoriseringssystemer, som anvender følsomme (person)karakteristika,
2. "predictive policing"-systemer (algoritmer, der forudser kriminalitet) baseret på profilering, lokation eller tidligere kriminel adfærd,
3. følelsesgenkendelsessystemer inden for retshåndhævelse, grænsekontrol, arbejdspladser og uddannelsesinstitutioner,
4. AI-systemer, der bruger vilkårlig scraping af biometriske data fra sociale medier eller CCTV-optagelser til at skabe ansigtsgenkendelsesdatabaser.

Højrisiko AI-systemer

Kommissionen foreslog i sit udspil, at visse systemer, der anvendes til formål angivet i bilag III i AI-forordningen, automatisk skal karakteriseres som højrisikosystemer. Parlamentet ønsker i den forbindelse et yderligere krav om, at systemerne også skal udgøre en "significant risk to health, safety and fundamental rights" for at kunne kvalificeres som højrisikosystemer. Rådet ønsker i den forbindelse, at AI-systemer, der sandsynligvis ikke vil resultere i alvorlige krænkelse af grundlæggende rettigheder eller andre væsentlige risici, ikke karakteriseres som højrisikosystemer.

Derudover har både Parlamentet og Rådet slettet, tilføjet og præciseret oversigten over højrisikosystemer i bilag III.

Krav til udbydere af foundation models og generative AI

Parlamentets udkast inkluderer som det eneste en definition på og regler for anvendelse af "foundation models" (modeller, der er trænet på store mængder af data, og som bruges som fundament til at bygge AI-systemer), herunder generative models (algoritmer, der kan skabe nyt indhold) såsom GPT-4 (ChatGPT).

Foundation models defineres som "an AI model that is trained on broad data at scale, is designed for generality of output, and can be adapted to a wide range of distinctive tasks". Ved anvendelse af disse modeller følger en række nye forpligtelser for udbydere, som bl.a. skal identificere og håndtere de risici, som modellen indebærer, overholde visse særlige design-, informati-

ons- og miljøkrav samt registrere modellen i en EU-database.

Udbydere af generative foundation models såsom ChatGPT vil være underlagt strenge krav til transparens, herunder at skulle oplyse, at indholdet er genereret af AI og ikke af et menneske, træne og designe modellen, så man forhindrer generering af ulovligt indhold, samt dokumentere og offentliggøre et tilstrækkeligt detaljeret overblik over brugen af træningsdata.

Nationale myndigheder og håndhævelse

Parlamentet ønsker at give nationale myndigheder beføjelse til at anmode om adgang til både AI-systemer og de modeller, som de benytter, herunder foundation models. Parlamentet foreslår også at oprette et såkaldt "AI Office", hvis formål er at understøtte en harmoniseret anvendelse af AI-forordningen, yde vejledning og koordinere fælles grænseoverskridende undersøgelser.

Mens vi venter - tre gode råd

Nedenfor er tre gode råd, hvis du allerede nu arbejder med kunstig intelligens, herunder "foundation models", eller skal i gang med det.

1. Udarbejd retningslinjer for brug af kunstig intelligens. Lav interne retningslinjer for brug af AI, der understøtter, at medarbejdere ikke ved en fejl behandler personoplysninger i strid med databeskyttelsesforordningen, at ophavsrettigheder ikke krænkes, at forretningshemmeligheder ikke uforvarende afsløres, og at tavshedspligten ikke brydes.

2. Brug redskaber fra Dataetisk Råd. Dataetik handler grundlæggende om at tage velovervejede beslutninger i forbindelse med anvendelse af data og teknologi og dermed tage højde for de konsekvenser, som en sådan anvendelse vil have. Som hjælp til at afklare dataetiske dilemmaer har Dataetisk Råd udviklet et vurderingsskema, konsekvensanalyse og værktøjer, som kan findes på Rådets hjemmeside.

Indtil de mere konkrete lovgivningsmæssige rammer er på plads, kan dataetikken være kompasset i junglen af teknologi og data, der guider dig igennem de mange problemstillinger, som anvendelsen af kunstig intelligens giver anledning til.

3. Udarbejd relevant dokumentation. Dokumentér, hvilke værktøjer og

løsninger med kunstig intelligens I bruger, og hvilke potentielle udfordringer der kan være ved brugen af disse. Undersøg, om og i hvilket omfang leverandøren af de pågældende AI-systemer har dokumenteret udviklingen og brugen af AI-systemet.

Genbesøg eller udarbejd en artikel 30-fortegnelse efter databeskyttelsesforordningen, lav risikovurderinger, og overvej at udarbejde en konsekvensanalyse. Udarbejdelse af disse dokumentationsformer vil gøre brugen af kunstig intelligens mindre risikofyldt.

Definitionen af "system med kunstig intelligens"

Både Parlamentets og Rådets udkast til en definition af "system med kunstig intelligens" (AI-systemer) forenkler Kommissionens definition. Rådet indsnævrer definitionen til systemer, der er udviklet gennem maskinlæring og logik- og vidensbaserede tilgange, mens Parlamentets definition lyder:

"A machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations, or decisions that influence physical or virtual environments."

Parlamentets definition svarer til OECD's definition af et AI-system.



Jens Grønkjær Sjølander Pihl
Partner, advokat
jisp@horten.dk



Emilie Loiborg
Advokat
elo@horten.dk