Data Foundations

Hoofdstuk 6

Lab data ethics

Hassan Haddouchi

In deze opdracht kijken we naar het ethische vraagstuk in de wereld van data-collectie en leren uit data.

Jullie wordt gevraagd om, gegeven de theorieles en de bijkomende kennis rond GDPR alsook de achtergrondkennis beschreven in de opdracht, een verslag te schrijven dat componenten van een framework nader bekijkt voor een specifieke case, namelijk de ontwikkeling van een beveiligingsrobot.

Zorg dat je verslag duidelijk gestructureerd is. Dien je verslag in PDF formaat in op Digitap.

Tip: benader de use-case vanuit uw perspectief als software ontwikkelaar gespecialiseerd in data.

Achtergrond

De wereld is aan het veranderen en momenteel versnelt AI dit proces. Zowel de behoeften alsook de eisen van de markt veranderen. Maar we merken ook dat de eisen en ervaringen van gebruikers aan het evolueren zijn. Dit allemaal in een context waarin technologie en technologische ontwikkeling steeds beschikbaar en toegankelijk moet blijven.

Het doel van veel producten is steeds om een betere dienst te leveren die persoonlijk en duidelijk is. De persoonlijke ervaring van de gebruiker staat steeds centraal.

Het is zo dat onze relatie met machines gebaseerd is op dezelfde elementen waarop de relatie van mens tot mens is gebaseerd. Dit komt voort uit het doel van AI, namelijk intelligente systemen creëren die in staat zijn om taken uit te voeren die gemakkelijk of zelfs triviaal zijn voor mensen, terwijl de efficiëntie en nauwkeurigheid worden verbeterd.

De hamvraag is: waar ontmoeten data, AI en ethiek elkaar?

Een prangende ethische kwestie is het zogeheten ‘Trolley Problem’ uit de theorieles.

Welke keuze is de meest ethische? (deze vraag hoef je niet te beantwoorden. Het is enkel om aan te duiden dat ethische vraagstukken heel complex kunnen zijn).

Stel dat het karretje door AI zelf kan rijden en dat er niemand aan de hendel staat. Bovendien kan het karretje, ook door middel van AI, vanop afstand de hendel besturen. Het vraagstuk wordt nu nog complexer.

Dit voorbeeld illustreert keuzes die in feite morele oordelen zijn. Analisten argumenteren bijgevolg dat zulke keuzes niet kunnen worden gedegradeerd tot ongevoelige machines.

De kracht van data en AI ligt in samenwerking met mensen, zoals robots in fabrieken, zelfrijdende auto's, operatierobots en navigatiesystemen.

Momenteel focust zich de discussie rond mogelijk problematische aspecten van data & AI op de volgende kwesties:

- Privacy en veiligheid. AI draait op data, dus kwetsbaarheden in de cyberbeveiliging kunnen een bedreiging vormen voor individuen en organisaties.
- Transparantie. Hoe worden de gegevens verwerkt en hoe worden ze gebruikt? Welke gegevens worden in patroonherkenning geselecteerd en hoe wordt de kwalitiet ervan bepaald?
- Vooroordelen (bias). Bias kan op verschillende manieren een algoritme beïnvloeden.

Nu kunnen we spreken van een framework om een focus te leggen op ethische implementaties bij werken met data.

Dit framework bevat 4 componenten: **vertrouwen**, **transparantie**, **eerlijkheid** en **privacy**.

Opdracht: een robot als beveiligingsagent

De robots die vandaag zijn ontwikkeld, maken gebruik van kunstmatige intelligentie, langeafstandssensoren, high-definition camera's en snelle computerverwerking. Dit allemaal zorgt voor een behoorlijk beveiligingssysteem voor verschillende behoeften. Een robot kan in feite gemakkelijk een aangewezen gebied bewaken. Ze zijn ontworpen om het terrein en de binnenkant van een gebouw te bewaken. Deze beveiligingsrobots zijn intelligent ontworpen en maken gebruik van complexe GPS systemen die gemakkelijk objecten binnen enkele centimeters kunnen vinden. M.a.w.: wanneer de robot beweegt, weet hij precies waar hij staat. Met een beveiligingscamera kan de robot dagelijks gegevens vastleggen en opslaan. De nieuwste AI-aangedreven beveiligingsrobots gebruiken gezichtsherkenning om de identiteit op te slaan van mensen die een bepaald huis of gebouw bezoeken en om een database aan te maken van personen die regelmatige bezoekers zijn of bijvoorbeeld bekende personen zijn. Stel nu dat we een door AI-aangedreven beveiligingsrobot willen ontwikkelen.

Schrijf een uitgebreid verslag over bovenstaande case, waarbij je een focus legt op het etische vraagstuk door middel van het voorgestelde framework. Er is geen template voor het verslag, wel een maximum van 2 pagina's. Bronnen vermelden is verplicht (achteraan het document). Volgende criteria dien je in acht te nemen:

- Een analyse van het probleem.
- Een uiteenzetting van het ethische vraagstuk in verhouding tot het probleem. Wat zijn mogelijke ethische valkuilen bij de ontwikkeling van intelligente robots? Wat is van minder belang? Wat is de rol van data in dit verhaal? Welke rol speel jij als data-engineer of software-ontwikkelaar?
- Gegeven het framework dat hierboven werd beschreven, geef voor elke component een duidelijke en uitgebreide aanbeveling bij de ontwikkeling van AI robots.

Inleveren

Dien je rapport als PDF in op Digitap.