DataFoundations

Labo6.1: Data ethics

Kobe Vervoort
3ITSOF1

Labo 6.1 – Data ethics

Het ontwikkellen van een AI-gestuurde beveiligingsrobot maakt vele nieuwe concepten, zoals verbeterde veiligheid en efficiënte monitoring, mogelijk. Het gebruik van gezichtsherkenning en de opslag van camerabeelden zorgt echter voor belangrijke bedenkingen omtrent het ethische aspect, privacy en regelgeving. In dit verslag vat ik samen hoe de GDPR en de AI Act deze technologie bepaalde regels opleggen, en hoe een compliant en ethische implementatie kan worden gerealiseerd.

Als software-ontwikkelaar ben ik verantwoordelijk voor het rekening houden met het opvolgen van alle ethische en juridische regels die mij werden opgelegd. Data is enorm belangrijk in dit verhaal, aangezien dit essentieel is om het projectidee te realiseren. Zonder data is er geen sprake van AI-aangestuurde robots. Het blijft natuurlijk erg belangrijk dat deze data op een goede, verantwoordelijke manier behandeld en verwerkt kan worden. Minder belangrijke onderdelen zijn de langeafstandssensoren en de GPS-systemen, aangezien hiermee niet in de fout gegaan wordt.

Gezichtsherkenning en GDPR
De GDPR (General Data Protection Regulation) is de belangrijkste wetgeving binnen de EU en omvat de verwerking van persoonsgegevens, waaronder biometrische gegevens zoals gezichtsherkenning. Volgens de GDPR moet er dus sprake zijn van volgende zaken, voordat men zulke gegevens mag opslaan/verwerken:

1. Het verwerken van biometrische gegevens vereist expliciete **toestemming** van de betrokkenen, tenzij een andere rechtsgrond, zoals gerechtvaardigd belang, van toepassing is. Bijvoorbeeld:
    - Voor bewaking van een privégebouw kan een eigenaar toestemming van bezoekers vragen.
    - In openbare ruimtes is toestemming vaak moeilijk haalbaar, waardoor gezichtsherkenning hier onrealistisch wordt.
2. Alleen **strikt noodzakelijke gegevens** mogen worden opgeslagen. Voor gezichtsherkenning betekent dit dat bijvoorbeeld unieke gezichtskenmerken in hash-vorm worden opgeslagen in plaats van volledige gezichtsafbeeldingen.
3. De verzamelde gegevens mogen alleen worden gebruikt voor **beveiligingsdoeleinden** en niet voor andere doelen, zoals marketing of commerciële toepassingen.
4. Camerabeelden en bijbehorende biometrische gegevens moeten worden **verwijderd** zodra ze niet meer nodig zijn.
5. De gegevens moeten worden beschermd door encryptie en strenge toegangscontroles om ongeautoriseerde toegang te voorkomen.

AI Act en gezichtsherkenning
De AI Act beschrijft aanvullende regels voor het gebruik van AI-systemen, waaronder gezichtsherkenning. Deze wetgeving bevat specifieke eisen voor “hoog risico”-toepassingen zoals beveiligingsrobots:

1. De AI Act **verbiedt** real-time gezichtsherkenning in openbare ruimtes, tenzij noodzakelijk voor bijvoorbeeld nationale veiligheid.

2. Beveiligingsrobots vallen in de categorie **"hoog risico",** wat betekent dat ze moeten voldoen aan strenge eisen zoals:
    - Risico impact analyses voor privacy en ethiek.
    - Het systeem moet voldoen aan EU-standaarden en gecertificeerd zijn.
    - Gebruikers moeten transparant geïnformeerd worden over de werking en impact van de gezichtsherkenning.

Uitdagingen en praktische oplossingen

1. Gegevensverzameling en -opslag
    - **Edge computing**: Analyseer gezichtsherkenning lokaal op de robot, zodat de gegevens niet naar een centrale server worden verzonden.
    - **Anonimisering**: Gebruik hashing om biometrische gegevens onherkenbaar te maken, wat het risico op datalekken vermindert.
2. Toestemming en transparantie
    - Plaats duidelijke waarschuwingsborden waarin wordt aangegeven dat gezichtsherkenningstechnologie wordt gebruikt.
    - Maak gebruik van een transparant dashboard voor gebouwbeheerders om inzicht te geven in welke gegevens zijn verzameld en hoe ze worden gebruikt.
3. Voorkomen van bias
    - Gebruik diverse datasets om te voorkomen dat gezichtsherkenning discriminerend is tegenover bepaalde demografische groepen.
    - Voer regelmatig tests uit om systematische fouten in de AI-modellen te identificeren.
4. Beveiliging en controle
    - Beveilig de verzamelde gegevens met sterke encryptie.
    - Implementeer logboeken voor datatoegang en voer audits uit om naleving van de regelgeving te garanderen.
5. Menselijke tussenkomst
    - Laat de robot potentiële verdachte situaties markeren, maar geef de eindbeslissing aan menselijke operators.

Het gebruik van gezichtsherkenning en de opslag van beveiligingscamerabeelden biedt grote voordelen, maar roept ook ethische en juridische vragen op. De GDPR stelt strikte eisen bij het verwerken van biometrische gegevens. Ook de AI Act beschrijft aanvullende richtlijnen om de risico's van AI-systemen te beperken. Door technologie te ontwikkelen die voldoet aan deze wetten, kan een beveiligingsrobot niet alleen effectief, maar ook ethisch verantwoord functioneren.

Bronnen

AI Act. (2024, oktober 14). Opgehaald van European Commission: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

Algemene verordening gegevensbescherming. (2024, november 22). Opgehaald van Wikipedia: https://nl.wikipedia.org/wiki/Algemene_verordening_gegevensbescherming

How do we process biometric data lawfully? (2024, december 5). Opgehaald van Information Commissioner's Office: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-process-biometric-data-lawfully/

Verordening Kunstmatige Intelligentie. (2024, november 13). Opgehaald van Wikipedia: https://nl.wikipedia.org/wiki/Verordening_Kunstmatige_Intelligentie

Video Recording. (2019, februari 4). Opgehaald van Data Protection Commission: https://www.dataprotection.ie/en/dpc-guidance/video-recording