

Data Foundations

Hoofdstuk 6

Data ethics

Hassan Haddouchi



Waaraan denken jullie bij data ethics?

Inhoud

- Het morele doolhof van data en ML
- Balanceren tussen informatie en integriteit
- Bias in algoritmen
- Transparantie en uitlegbaarheid
- Autonome ethiek en verantwoordelijkheid
- Veiligheid en potentiëel misbruik
- Best practices voor ethische ontwikkeling
- Discussie en casestudy's

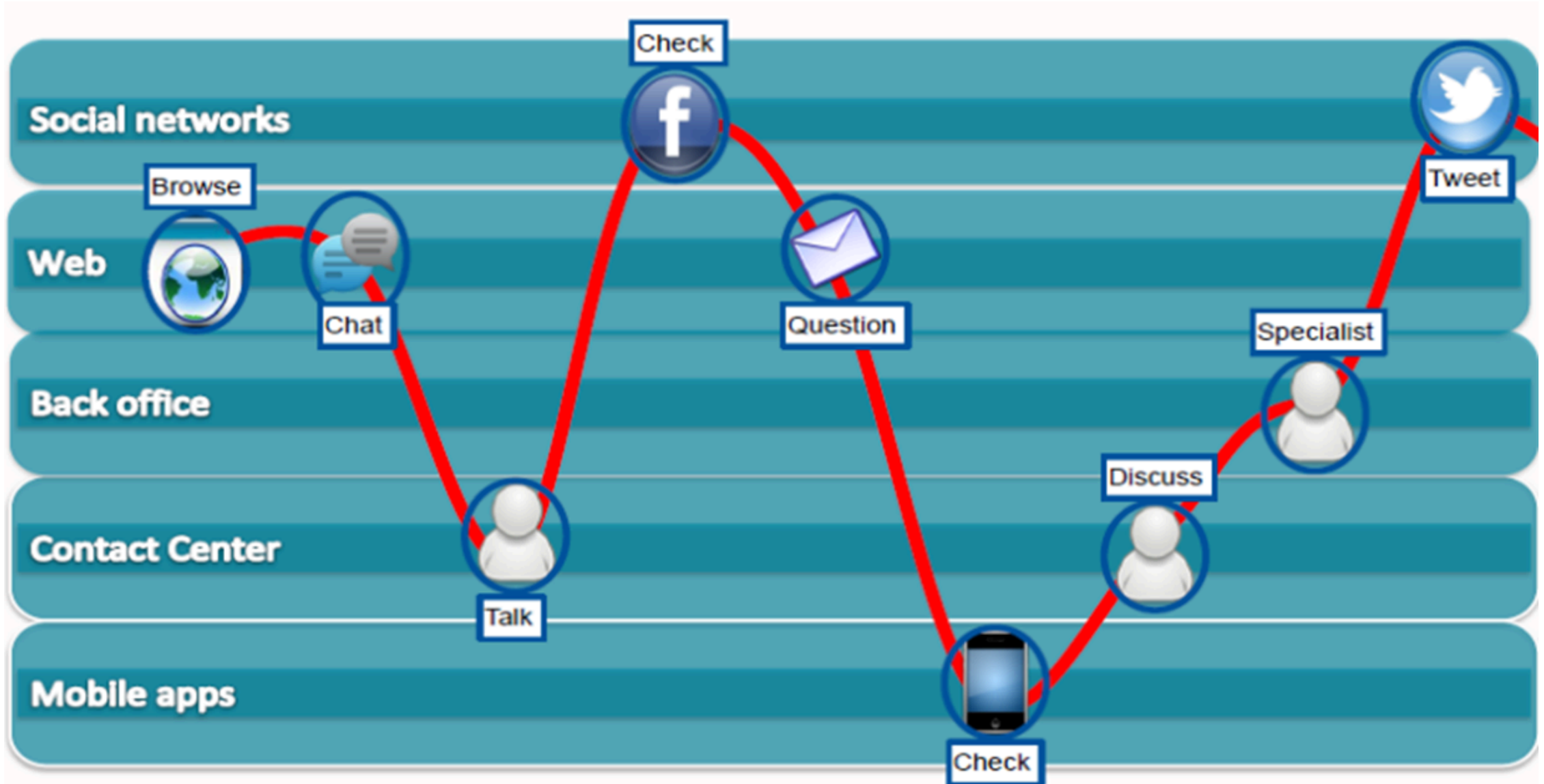
Veranderingen in de wereld

- Markt-benodigdheden
- Ontwikkeling van technologieën

Gebruikservaring verbeteren:

- Intelligente systemen
- Interactieve systemen
- Multimodaal: door verschillende kanalen

De lijn van digitale diensten



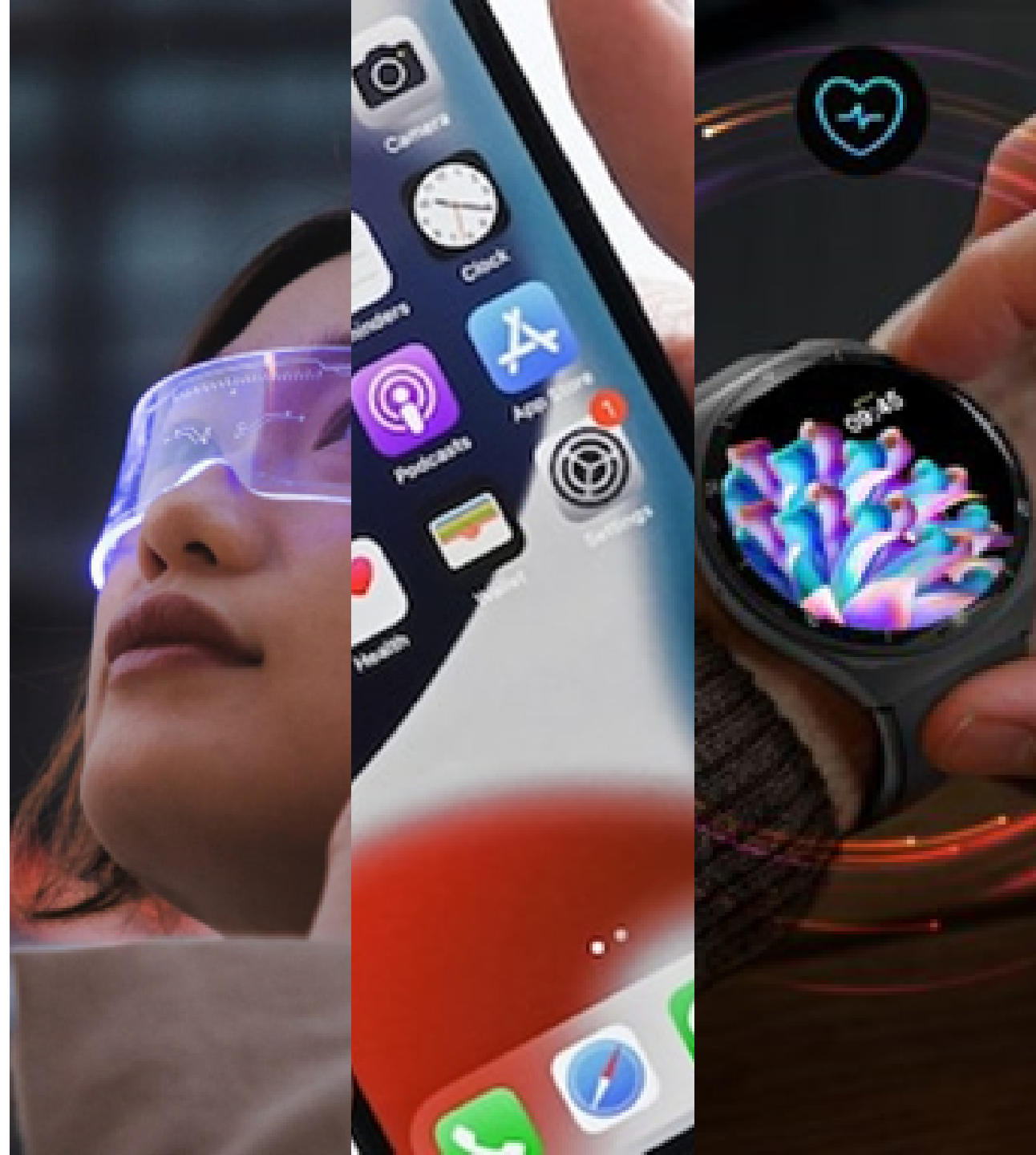
Het belang van ethische overwegingen

- Morele leidraad
- Bescherming van gebruikers
- Maatschappelijke verantwoordelijkheid
- Betrokkenheid van belanghebbenden

Wat willen gebruikers zien?

- Consistentie in klantendiensten
- Snelle oplossingen
- Herkenning
- Op de hoogte blijven
- Problemen oplossen

Het digitale tijdperk



Het digitale tijdperk

In het moderne tijdperk doordringen digitale technologieën elk facet van ons dagelijks bestaan.

Van slimme thermostaten tot spraakgestuurde assistenten

- Huizen worden slimmer
- Virtuele vergaderingen, cloud computing en samenwerkingstools.
- E-healthplatforms, wearables en gezondheidsapps
- Streamingdiensten, online gaming en VR
- Slimme steden, zelfrijdende auto's en mobiliteitsapps
- Sociale media, instant messaging en videoconferenties

Data Privacy:

Cambridge Analytica



Cambridge Analytica

Cambridge Analytica was een Brits politiek adviesbureau dat gebruik maakt van data analytics.

Bij verkiezingen maken ze profielen van kiezers en om gepersonaliseerde campagne-advertenties te sturen.

Zo verzorgden ze de digitale campagne van Donald Trump in 2016.

Hiervoor werd facebook data gebruikt van meer dan 50 miljoen facebook gebruikers die hier niet mee instemden.

In 2018 ging het bedrijf failliet na een onderzoek van het Britse hooggerechtshof.

Juridisch kader

Er zijn 2 kaders:

- Algemene Verordening Gegevensbescherming (AVG)
- CCPA



GDPR

GDPR is de Europese wetgeving (sinds 2018) over het verwerken van persoonsgegevens en die geldig is in de hele EU, onafhankelijk van waar de data wordt opgeslagen en verwerkt.

Verwerkingsverantwoordelijke: degene die het doel en de manier van data verwerking bepaalt

Gegevensverwerker: degene die de data verwerkt in opdracht van de verwerkingsverantwoordelijke

Een DPA (Data Processing Agreement) is een verplicht contract tussen data beheerder en data verwerker dat vastlegt hoe de data verwerkt wordt.

GDPR

Een voorbeeld

Een brouwerij heeft veel medewerkers in dienst en tekent een overeenkomst met een payrollbedrijf om de lonen uit te betalen. De brouwerij vertelt aan het payrollbedrijf wanneer het loon moet worden uitbetaald, wanneer een werknemer vertrekt of een loonsverhoging krijgt en verstrekt allerlei andere details voor de loonstrook en de betaling. Het payrollbedrijf levert het IT-systeem en slaat de gegevens van de medewerkers op.

De brouwerij is de **verwerkingsverantwoordelijke** van de gegevens en het payrollbedrijf is de **gegevensverwerker**.

Hoe gaan we om met machines?

Onze relaties met machines zijn gebaseerd op dezelfde elementen waarop relaties van mens tot mens zijn gebaseerd.

Toepassing van ethische overwegingen vergelijkbaar met menselijke relaties

Mogelijke conclusie:

Belangrijke ethische principes, zoals respect, eerlijkheid en verantwoordelijkheid, moeten worden toegepast in de ontwikkeling en inzet van AI-systemen.

Doel: menselijke waarden en rechten respecteren en behouden in technologieën.

De evolutie van AI

Computing > Cognitive Computing > Predictive Computing

- Machine learning (ML)
- Rule based learning (RBML)
- Data analytics
- Storage & processing power
- Deep learning (DL)

Interactie

Interactie met virtuele systemen legt de nadruk op het belang van ethische overwegingen in AI ontwikkeling.



Waar Data, AI en ethiek elkaar ontmoeten

Een harmonieuze samensmelting van Data, AI en ethiek is cruciaal om technologische vooruitgang te omarmen met respect voor menselijke waarden en rechten.

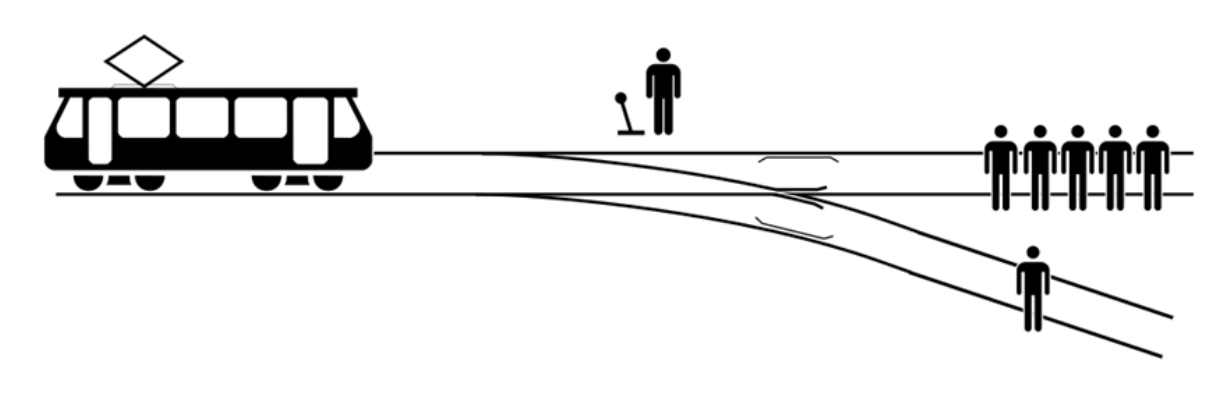
- Privacy & gegevensgebruik
- Bias (vooroordelen) en eerlijkheid
- Transparantie en uitlegbaarheid (explainability)
- Autonome systemen en verantwoordelijkheid
- Sociale impact en werkgelegenheid
- Veiligheid en misbruik

Het Trolley Probleem

Een op hol geslagen wagon dat zich richting vijf vastgebonden mensen beweegt die op het spoor liggen.

1. Doe niets en laat de wagon de vijf mensen op het hoofdspoor doodrijden.
2. Trek aan de hendel en stuur de wagon naar het zijspoor waar één persoon zal doodrijden.

Welke optie is de meest ethische?



Snelle evolutie

Het snel evoluerende landschap van data en machine learning confronteert ons met intrigerende morele vraagstukken.

Ethische dilemma's en vraagstukken.



Ethische vraagstukken: een voorbeeld

Wervingsalgoritme om sollicitaties te analyseren en geschikte kandidaten te selecteren.

- Vertoonde een voorkeur voor kandidaten met kenmerken van de dominante demografie in de trainingset.

Het belang van voortdurende ethische evaluaties.

Navigeren door ethische overwegingen

Case: privacy bij gezondheidsgegevens

Stel: een team van datawetenschappers is betrokken is bij de ontwikkeling van een geavanceerd gezondheidsanalysealgoritme.

Doel: op basis van individuele gezondheidsgegevens persoonlijke gezondheidsvoorspellingen te doen. Echter, tijdens het proces ontstaat er een ethisch dilemma met betrekking tot privacy.

Tijdens het proces ontstaat er een ethisch dilemma met betrekking tot privacy.

Het algoritme heeft toegang tot genetische gegevens, medische geschiedenis en levensstijlkeuzes.

Uitdaging: de voorspellende kracht van het algoritme te maximaliseren zonder de privacy van individuen in gevaar te brengen.

Ethische vraagstukken?

Ethische vraagstukken:

- Hoe kan het team zorgen voor geanonimiseerde gegevens zonder de voorspellende waarde te verminderen?
- Op welke manier moeten individuen worden geïnformeerd en toestemming geven voor het gebruik van hun gezondheidsgegevens?
- Hoe kan het algoritme worden ontworpen om rekening te houden met culturele en ethische diversiteit in gezondheidspraktijken?

Verbondenheid van ethiek, data en ML

Toenemende afhankelijkheid van technologie.

De digitale samenleving brengt een verschuiving in waarden, normen en verwachtingen teweeg.

Data als drijvende kracht

De exponentiële groei van digitale gegevens is de brandstof van innovatie en besluitvorming.

De mogelijkheid om relevante en betrouwbare informatie te extraheren, geeft een concurrentievoordeel.

AI en ML zijn gebaseerd op het solide fundament van data.

Kansen en uitdagingen

Bescherming van persoonlijke gegevens

Vermijden van misbruik

Beschermen tegen datalekken, hacking en het waarborgen van integriteit van informatie.

Compliance en regelgeving

Bias in algoritmen

Algoritmen kunnen inherente bias bevatten door de manier waarop ze zijn getraind en de data die ze gebruiken.

Bias kan leiden tot ongelijkheid en onrechtvaardige beslissingen.

Gevoelige domeinen zoals: werkgelegenheid, kredietverstrekking, juridische procedures, ...

Hoe ontstaat bias?

Historische gegevens, onvolledige datasets, aannames in het model.

Hoe identificeer je bias?

Historische gegevens, onvolledige datasets, aannames in het model.

Data en besluitvorming

Belangrijke principes zijn:

- Transparantie
- Uitlegbaarheid
- Non-discriminatie
- Verantwoordingsplicht
- Menselijke betrokkenheid
- Continue monitoring

Best practices voor ethische ontwikkeling in data

Eigenaarschap over je persoonlijke informatie.

Transparantie in verzamelen, opslaan en gebruik van data.

Privacy: beveiliging, dual-authentication, file encryption, regelgeving.

Intentie: waarom heb je bepaalde data nodig?

Uitkomst van data analyse en bias in algoritmen.