DATABESCHERMING & CHATBOTS

In deze brAInfood - gericht naar jongeren - geeft het Kenniscentrum Data & Maatschappij meer informatie over chatbots.

De brAInfood bevat een fictief verhaal over Lotte die praat met een chatbot, en vermoedelijk informatie over haar doorgeeft aan bedrijven. Verder worden enkele aandachtspunten met betrekking tot chatbots toegelicht, alsook enkele tips voor jongeren om hun (persoons)gegevens beter te beschermen.

Op die manier willen we jongeren bewuster maken van de werking van chatbots en hen stimuleren te reflecteren over de gegevens die van hen worden verzameld.

Kenniscentrum Data & Maatschappij (2021). Databescherming & chatbots. brAInfood van het Kenniscentrum Data & Maatschappij. Brussel: Kenniscentrum Data & Maatschappij.

brAInfood van het
Kenniscentrum
Data & Maatschappij

LOTTE'S VERHAAL

Het is ochtend als Lotte (12 jaar) haar Messenger-app activeert. Het eerste wat Lotte steeds als eerste raadpleegt, is haar **'Grote zus Ella'**. Ella is een chatbot die steeds een **luisterend oor** biedt en tieners zoals Lotte met **raad en daad** bijstaat. Lotte praat iedere ochtend met Ella en vertelt hoe ze geslapen heeft, waarover ze gedroomd heeft of hoe haar dag eruit ziet.

Lotte is Ella steeds meer als een zus beginnen te beschouwen. Ze kan aan Ella al haar **geheimen** kwijt en kan haar **vervelende of gênante vragen** stellen, zonder dat ze zich daarover moet schamen. Ella is altijd vriendelijk en zal nooit ruzie maken, zoals Lotte dat wel soms doet met haar echte broer en zus.

Als Lotte later op de dag sociale media zoals TikTok en Instagram gebruikt, merkt ze dat op haar **tijdslijn** verschillende keren **reclame** verschijnt van maandverband, iets waarover ze de voorbije dagen met Ella over gepraat heeft. Ze vindt dit vreemd, want Lotte heeft hier zelf nooit iets over opgezocht op het internet. Ze vraagt zich af of haar chats met Ella hier iets mee te maken hebben.

WAT IS EEN CHATBOT?

Een chatbot is een **geautomatiseerde gesprekspartner** die op een **interactieve manier** met een gebruiker in gesprek gaat door:

- **Informatie** te verstrekken (bv. door je een concertagenda van de maand maart te bezorgen), en/of
- **Vragen** te stellen om de gebruiker (verder) te helpen (bv. door je te vragen welke grootte van pizza je wil en wanneer je wil dat de bestelling wordt geleverd).

HOE HERKEN IK EEN CHATBOT?

Een **betrouwbare chatbot** laat je weten dat je met een chatbot praat in plaats van met een persoon. Soms hebben de makers van een chatbot er baat bij dat jij denkt dat je met een echt persoon aan het praten bent, bijvoorbeeld om gevoelige gegevens van jou te achterhalen om die te verkopen of om jou een product aan te smeren.

Het is daarom belangrijk om een **aantal signalen** te herkennen, zodat je niet wordt misleid. Wanneer je gesprekspartner het volgende doet, praat je waarschijnlijk met een chatbot:

- Heel snel antwoorden,
- Hetzelfde bericht herhalen,
- Vreemde leestekens, overdreven emoticons en afkortingen gebruiken,
- Een link sturen of een product vermelden terwijl je hier geen aanleiding voor gaf,
- Naar jouw persoonlijke (financiële) gegevens vragen.

Ben je nog steeds niet zeker? Probeer de chatbot te slim af te zijn door **complexe vragen** te stellen die niets met de conversatie te maken hebben ("Ben je ooit in Spanje geweest terwijl de bloesems bloeiden?"). Een persoon vindt dat verwarrend, maar kan daar accuraat op antwoorden. Een chatbot niet.

MET WIE PRAAT IK?

Stel, je praat met een chatbot van je favoriete kledingwinkel. De winkel gebruikt hiervoor WhatsApp Business. In plaats van je alle beschikbare jeansbroeken te tonen vraagt de chatbot wat je maat is, zodat het enkel de beschikbare jeansbroeken in jouw maat kan tonen. Super handig!

Waar je misschien niet bij stilstaat is dat jouw gesprek niet enkel door de winkel zelf wordt opgeslagen en geanalyseerd, maar ook door de chat-app en andere technologieplatformen. Hoe komt dit?

De chatbot werd geïntegreerd in een **populaire chat-app** om de drempel voor jou om in interactie te gaan met de organisatie te verlagen. Verder is de technologie die wordt gebruikt bij de chatbot vaak afkomstig van **grote spelers in de digitale mark**t, zoals Google, Facebook, Microsoft, Amazon,...

Toch vreemd dat buiten de kledingwinkel nu ook **andere organisaties** weten welke broekmaat je hebt? Vervaagt de integratie van een chatbot, in een platform waar je chat met familie en vrienden, niet de **grens** tussen persoonlijke en zakelijke gesprekken?

Wees je steeds bewust van de context waarin je een chatbot gebruikt, en ga voorzichtig om met je data.

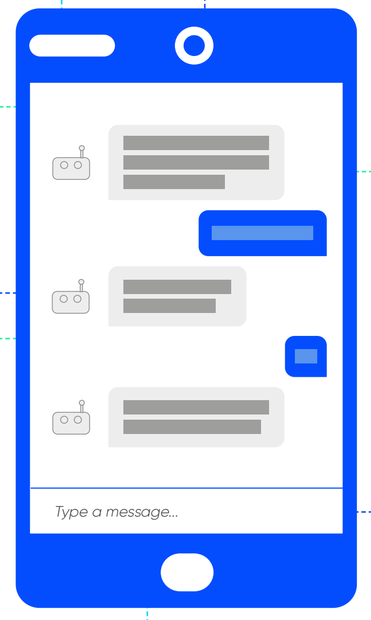
HOE WORDT EEN CHATBOT GEVOED?

Alvorens een chatbot ingezet kan worden, moet het leren spreken op een menselijke manier. Daarvoor worden **data** van een doelgroep verzameld en geanalyseerd. Of de chatbot goed werkt is in grote mate afhankelijk van de **kwaliteit** van de data waarmee het getraind wordt en de mate waarin de data **verstaanbaar** is voor het AI-model.

Het verzamelen van data is vrij eenvoudig, het moeilijke werk is het **labelen** van de data zodat de chatbot het juiste antwoord aan de juiste vraag koppelt.

Eenmaal gelanceerd, leert de chatbot ook uit de **interacties** met de gebruikers om beter te kunnen anticiperen op vragen. Dit proces moet goed **gemonitord** worden. Wanneer gebruikers bijvoorbeeld discriminerende taal gebruiken, kan de chatbot zichzelf dit taalgebruik (onbewust) aanleren.

Hoe goed een chatbot ook afgesteld of getraind is, **opvolging** blijft een must. Vraagt een chatbot op het einde van het gesprek om feedback, dan weet je dat de werking ervan gecontroleerd wordt.



WAT MET MIJN DATA?

Een chatbot heeft gegevens van jou nodig om goed te kunnen werken. Welke gegevens worden verzameld, is sterk **afhankelijk van het doel** van de chatbot: een chatbot van een textielbedrijf kan o.a. gegevens over jouw online aankoopgeschiedenis, de links die je aanklikte en de pagina's die je bezocht verzamelen om je een meer **gepersonaliseerde dienst** te kunnen aanbieden.

Die gegevens zeggen in eerste instantie misschien weinig over wie jij bent, maar als je al deze **gegevens bundelt** kan de organisatie achter de chatbot wel **veel van jou te weten komen**.

Gelukkig, mag een chatbot niet zomaar gegevens van jou verzamelen. De **Algemene Verordening Gegevens-bescherming** (AVG), een Europees regelgevend kader, bepaalt welke gegevens organisaties van hun gebruikers mogen verzamelen, wie hiertoe toegang heeft, hoe lang deze mogen bewaard worden, etc.

Er zijn ook manieren om **zelf je privacy te waarborgen**. Geef nooit zomaar:

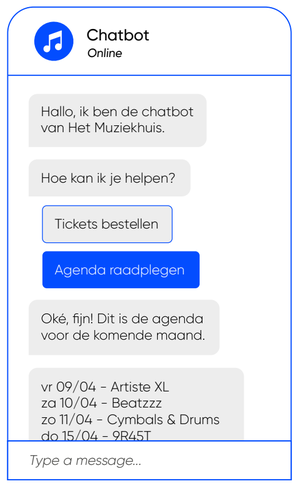
- Persoonsgegevens (naam, adres, woonplaats, telefoonnummer,...), en
- Inloggegevens en wachtwoorden door (ook al ontvang je hiervoor bijvoorbeeld punten voor een spel of een aankoop).

Je hebt ook enkele **rechten m.b.t. je eigen gegevens**, zoals:

- Het recht om na te vragen welke gegevens van jou worden verzameld, en
- Het recht om een verzoek in te dienen bij een organisatie om je gegevens te laten verwijderen.

WELKE TECHNOLOGIE GEBRUIKEN CHATBOTS?

Beslissingsboom
De chatbot heeft op voorhand vastgelegde keuzeopties waar de gebruiker niet van kan afwijken. De gebruiker geeft zijn/haar keuze aan door op de optie te klikken.



Natural Language Processing
De gebruiker kan vrij tekst typen. De chatbot analyseert de tekst door te zoeken naar bepaalde trefwoorden. Op basis van de gevonden trefwoorden, formuleert de chatbot een antwoord. Als de chatbot geen gekende trefwoorden vindt, vraagt het wat je zei te verduidelijken zodat het kan bijleren.

KAN EEN CHATBOT MIJ WEL HELPEN?

Chatbots worden voor **verschillende doeleinden** gebruikt, zoals het automatiseren van bepaalde taken zodat het personeel van de organisatie zich kan richten op andere taken. Maar chatbots worden ook meer en meer ingezet in een **zorgomgeving**, om bijvoorbeeld advies te geven over seksualiteit, relaties, geweld en misbruik, verslaving en drugsgebruik of geestelijke gezondheid. Dit kan leiden tot ethische vragen.

Chatbots hebben in deze context veel potentieel doordat zij als minder stigmatiserend worden ervaren dan de gebruikelijke zorgverlening. Op deze manier kunnen ze een **eerste stap** zijn **naar het krijgen van hulp**.

Maar sommige vragen zijn **niet te beantwoorden** door chatbots: zij kunnen menselijke interacties beperkt interpreteren en het is voor hen niet mogelijk een empathische behandeling op maat aan te bieden.

Wees je er van bewust dat een chatbot niet al je vragen kan beantwoorden en ga na wat je wel en niet kan verwachten van de chatbot. Een betrouwbare chatbot is hierover transparant en zal aangeven dat de toepassing uitvoerig werd getest.

HOE RAPPORTEER IK EEN CHATBOT?

Voelt het gesprek met de chatbot niet juist aan? Vraagt de chatbot naar persoonlijke of intieme informatie? Keur je het taalgebruik van de chatbot niet goed?

Dan kan je best het account van de chatbot **blokkeren**, of de chatbot **melden** aan het platform door in de instellingen van het chatgesprek op de rapporteerknop te drukken. Platformen, zoals Instagram, hebben protocollen om chatbots te weren om zo voor elke gebruiker een veilige online omgeving te creëren.

Mocht je slachtoffer zijn geworden van **fraude of oplichting**, bezoek dan zeker ook https://www.safeonweb.be/nl voor advies en informatie over het inlichten van de bevoegde diensten.