



Niet zonder risico

De chatbot ChatGPT roept vragen op doordat hij foute informatie kan geven, je zelfs kan manipuleren en een aanslag op je privacy kan plegen. Met onze tips kun je je er tegen beschermen.

Chloé De Smet en Caroline Koelman



ChatGPT is een AI-tool (artificiële intelligentie) die in staat is om geschreven inhoud, teksten of afbeeldingen te genereren. Ontwikkeld door OpenAI, is deze chatbot meer dan alleen een conversatiemachine: het wordt een generatieve AI genoemd. Zijn toepassingen zijn talrijk: het verstrekken van informatie, het schrijven van een scriptie boek of artikel,

programmeerlijnen uitschrijven, lange teksten samenvatten, rangschikkingen opmaken op basis van een spreadsheet, inspiratie opdoen of afbeeldingen genereren (functie voor betalende abonnees). Op basis van een geschreven instructie, ook wel prompt genoemd, voert ChatGPT uit wat er van hem wordt gevraagd. Om je te registreren en de



**ER ZIJN AL KLACHTEN
INGEDIEND, ONDER MEER
WEGENS VERSPREIDING VAN
FOUTE INFORMATIE**

chatbot te kunnen gebruiken, moet je een geldig en authentiek e-mailadres en telefoonnummer opgeven.

Te veel misleidende informatie

Als je ChatGPT al hebt gebruikt, weet je dat hij regelmatig vage of onnauwkeurige informatie geeft. Dit komt doordat ChatGPT nieuwe teksten produceert op basis van informatie die hij op internet heeft gevonden. En deze informatie kan onjuist zijn. Het web staat namelijk vol met propagandamateriaal, lobbywerk en opiniestukken.

Problemen met privacy

De gegevens die door ChatGPT worden verstrekt, kunnen privé zijn. Veel gegevens op internet bevatten persoonlijke informatie over mensen, soms zelfs hun adres of andere privé-informatie die hun identiteit zou kunnen onthullen. Deze informatie is verzameld zonder toestemming van de betrokkenen, wat een duidelijke schending van de privacy inhoudt.

Niet-naleving van auteursrechten

Boeken, artikelen, essays... allemaal informatie die beschikbaar is op het web en wordt gebruikt om de AI te voeden, zonder toestemming van de auteurs. ChatGPT gebruikt alle beschikbare informatie online, of het nu gaat om een blogartikel, een korte opmerking of een uitgebreid artikel. Maar is dat legaal? Wel, volgens de wet is elke reproductie, zelfs gedeeltelijk, van door auteursrecht beschermde inhoud onwettig zonder toestemming van de auteur.

Maar een Europese richtlijn voorziet in een uitzondering voor AI: deze staat toe dat beschermde werken als trainingsbronnen door AI mogen worden gebruikt.

Auteurs kunnen dit gebruik wel weigeren. Maar hoe kan men hier in de praktijk zeker van zijn?

Risico's qua aansprakelijkheid

Een groot risico van het gebruik van ChatGPT is de juridische aansprakelijkheid als gevolg van de soms bevooroordeelde of gevoelige antwoorden. Als de gegeven antwoorden discriminerend of ongepast zouden zijn (bv. aanzetten tot haat, racistische opmerkingen, pedopornografische inhoud enz.), zou de gebruiker kunnen blootstaan aan strafrechtelijke sancties. Als ChatGPT bovendien inhoud genereert die inbreuk maakt op auteursrechten, zou hij zich en/of zijn gebruikers kunnen blootstellen aan gerechtelijke vervolging.

Nakende regelgeving is prima

Om de kunstmatige intelligentie verder te reguleren heeft de Europese Unie gewerkt aan regelgeving rond de verantwoordelijkheid van AI-systemen, inclusief generatieve AI zoals ChatGPT: "wetgevers moeten eisen dat de resultaten van elk generatief AI-systeem veilig, eerlijk en transparant zijn voor consumenten". Die regelgeving voorziet in het reguleren van hoogrisicosystemen zoals ChatGPT of de geavanceerdere nieuwe versie GPT-4.

Wij vinden dit een positieve ontwikkeling omdat consumenten controle moeten kunnen houden over hun privacy en persoonsgegevens zonder hun vertrouwen in technologische innovatie te verliezen.

Dankzij de GDPR kun je al een klacht indienen bij de Gegevensbeschermingsautoriteit GBA. Tal van Europese consumenten hebben dat recent gedaan, onder meer omdat foute informatie werd verspreid en er geen reactie kwam op een vraag om toegang te krijgen tot de gegevens en om die recht te zetten. Het Europees Comité voor Gegevensbescherming heeft al een werkgroep opgericht om ChatGPT te onderzoeken. ■

ONS ADVIES

Bescherm je privéleven

● Gebruik een extern en/of tijdelijk e-mailadres. Maak dus geen ChatGPT-account aan vanuit je Google- of Microsoft-account, maar gebruik liever een account voor privéberichten, in het bijzonder een account die beveiligde en versleutelde berichtendiensten gebruikt.

● Deel zo weinig mogelijk privé-informatie. Beschouw alles wat je in de chatbox deelt als informatie doe je deelt met het grote publiek en niet met een vriend of vertrouweling. Denk dus twee keer na als je ChatGPT vragen begint te stellen.

● Wis je ChatGPT-account en de gedeelde info na gebruik. Op grond van het recht om te worden vergeten zoals voorzien door de GDPR, heb je als gebruiker het recht om te eisen dat jouw persoonlijke informatie wordt verwijderd van de servers van OpenAI.

● Controleer de resultaten die ChatGPT geeft. Wees kritisch en gebruik zeker niet zonder meer de informatie die AI je geeft. Die informatie kan fout of onvolledig zijn.

● Vermeld geen namen van personen of bedrijven. Controleer of je toestemming hebt om ChatGPT te gebruiken voor je werk. Sommige bedrijven verbieden dat namelijk.