Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

3381

Vragen van het lid **Van Raan** (PvdD) aan de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties en de Minister voor Rechtsbescherming over *het aan banden leggen van ChatGPT vanwege privacyzorgen* (ingezonden 8 juni 2023).

Antwoord van Minister **Weerwind** (Rechtsbescherming), mede namens de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties (ontvangen 21 augustus 2023).

Vraag 1
Kent u het artikel «Dat zijn toch gewoon ál onze artikelen?»[1]

Antwoord 1
Ja.

Vraag 2 en 3
Kunt u bevestigen dat ChatGPT zijn taalmodel traint op basis van miljoenen onrechtmatig verkregen documenten van Docplayer.nl?
Klopt het dat die documenten vol staan met onder andere BSN-nummers, persoonlijke belastingaangiftes, curricula vitae en andere persoonsgegevens?

Antwoord 2 en 3
Ik beschik niet over informatie over de manier waarop ChatGPT gegevens verwerkt. Ik deel de zorg of gegevensverwerking door ChatGPT in overeenstemming met de regels van het gegevensbeschermingsrecht plaatsvindt. Ik vind het dan ook een goede zaak dat de Autoriteit Persoonsgegevens (AP), als toezichthouder op de naleving van de Algemene Verordening Gegevensbescherming (AVG), op 7 juni jl. bekend heeft gemaakt dat zij OpenAI per brief om opheldering heeft gevraagd over ChatGPT.[2] De AP schrijft op haar website dat zij van OpenAI wil weten welke data worden gebruikt om het algoritme te trainen op welke manier dat gebeurt. Verder schrijft de AP zorgen te hebben omtrent informatie over mensen die GPT gebruikt. De gegenereerde inhoud kan onnauwkeurig zijn, verouderd, onjuist, ongepast, beledigend, of aanstootgevend en kan een eigen leven gaan leiden. Of en zo

[1] https://www.groene.nl/artikel/dat-zijn-toch-gewoon-al-onze-artikelen; De Groene Amsterdammer d.d. 7 juni 2023.
[2] https://www.autoriteitpersoonsgegevens.nl/actueel/ap-vraagt-om-opheldering-over-chatgpt.

ah-tk-20222023-3381
ISSN 0921 - 7398
's-Gravenhage 2023

ja hoe OpenAI die gegevens kan rectificeren of verwijderen, vindt de AP nog onduidelijk, zo volgt uit haar bericht.

Vraag 4
Deelt u de stelling uit het artikel: «De persoonlijke informatie van docplayer.nl was op de website zélf al in strijd met de wet, laat staan wanneer die ook nog eens in chatbots wordt verwerkt»? Zo nee, waarom niet?

Antwoord 4
Er is mij onvoldoende bekend over docplayer.nl om hierover stelling in te nemen. Dat is ook niet de taak van het kabinet; de toezichthouder op de verwerking van persoonsgegevens dient dat in de eerste plaats te beoordelen, of het Openbaar Ministerie indien wordt vermoed dat sprake is van strafbare feiten.

Vraag 5 en 6
Klopt het dat ChatGPT hiermee onrechtmatig en onwettig persoonsgegevens verwerkt?
Hoe oordeelt u daarover? Wat gaat u er aan doen?

Antwoord 5 en 6
Het kabinet deelt de zorgen van uw Kamer over de risico's die generatieve AI-systemen, zoals ChatGPT, met zich mee kunnen brengen voor onder meer privacy, desinformatie en manipulatie. We zetten ons als kabinet vol in op het nemen van passende stappen op dit onderwerp.
Het kabinet werkt momenteel aan een visietraject over generatieve AI, zoals verzocht door uw Kamer middels de motie van de leden Dekker-Abdulaziz en Rajkowski. Deze visie wordt op een transparante wijze ontwikkeld en getoetst in diverse sectoren. U ontvangt deze visie voor het einde van het jaar. Over de voortgang is uw Kamer op 7 juli jl. al separaat geïnformeerd[3]. In deze visie formuleert het kabinet een standpunt over generatieve AI, waar ook een van de meest gebruikte generatieve AI-tools onder valt: ChatGPT. Ook wordt uiteengezet welk handelingsperspectief de Nederlandse overheid heeft om te waarborgen dat deze technologie op een verantwoorde manier in onze samenleving wordt ingebed.
Nederland speelt daarnaast een actieve rol in de onderhandelingen over zowel de AI-verordening van de EU als het AI-verdrag van de Raad van Europa. De AI-verordening stelt specifieke eisen aan de ontwikkelaars en gebruikers van hoog-risico AI-systemen, bijvoorbeeld als het gaat om transparantie en productveiligheid. Wij vinden het – net als het Europees Parlement – van belang dat er in deze wet speciale aandacht is voor foundation models en generatieve AI, zoals GPT en ChatGPT. Het kabinet zet zich ervoor in dat deze wet zo snel mogelijk wordt aangenomen.
De AP heeft mij geïnformeerd dat het samenwerkingsverband van Europese privacytoezichthouders (EDPB) op 13 april heeft besloten om, naar aanleiding van het Italiaanse optreden tegen OpenAI inzake ChatGPT, een taskforce in te stellen. Deze taskforce heeft tot doel de samenwerking en informatie-uitwisseling over mogelijke handhavingsmaatregelen te bevorderen. Alle Europese privacytoezichthouders zijn in dit samenwerkingsverband vertegenwoordigd, dus ook de AP. Generatieve AI, zoals het grote taalmodel artificiële intelligentie (AI) systeem ChatGPT, is een grensoverschrijdend fenomeen dat vraagt om een geharmoniseerde aanpak. Daarom hecht de AP grote waarde aan een effectief gezamenlijk optreden van de Europese privacytoezichthouders. Of ChatGPT rechtmatig persoonsgegevens verwerkt, is uiteindelijk ter beoordeling van de toezichthouders.

[3] Kamerstuk 26 643, nr. 1056.

Vraag 7–9 en 11–13
Klopt het dat ChatGPT voor zijn taalmodel ongeveer net zoveel geleerd heeft van de neonazistische website Stormfront als van de website van RTL Nieuws?[4]
Hoe oordeelt u daarover? Wat gaat u er aan doen?
Klopt het dat ChatGPT gebruik heeft gemaakt van onder andere 594.000 NRC artikelen en 162.000 Volkskrant artikelen?
Hoe oordeelt u daarover? Wat gaat u er aan doen?
Klopt het dat het «kwaliteitsfilter» is gebaseerd op drie bronnen waarvan er twee (Wikipedia en Reddit) een zeer sterke oververtegenwoordiging van mannelijke input kennen?[5]
Hoe oordeelt u daarover? Wat gaat u er aan doen?

Antwoord 7–9 en 11–13
Voor zover u mij vraagt of de bevindingen van het in vraag 1 genoemde artikel van 7 juni jl. correct zijn, moet ik het antwoord schuldig blijven. Ik heb geen informatiepositie die mij in staat stelt om de feitelijke juistheid te verifiëren van onderzoeksjournalistiek die ziet op de handelwijze van een organisatie in de private sector. Indien die handelwijze strijdig blijkt te zijn met het gegevensbeschermingsrecht, dan is het aan de toezichthouder om daarop te reageren. Indien het vermoeden bestaat dat er strafbare feiten worden gepleegd, zoals inbreuk op auteursrechten, dan kan daarvan aangifte worden gedaan.

Vraag 10
Deelt u de mening dat ChatGPT hiermee inbreuk maakt op het auteursrecht?

Antwoord 10
Dat valt niet op voorhand te zeggen. Op grond van artikel 25a, derde lid, van de Auteurswet wordt onder tekst- en datamining verstaan een geautomatiseerde analysetechniek die gericht is op de ontleding van tekst en gegevens in digitale vorm om informatie te genereren zoals, maar niet uitsluitend, patronen, trends en onderlinge verbanden. De definitie is ruim en omspant waarschijnlijk ook het trainen van generatieve artificiële intelligentie zoals ChatGPT. In principe is voor iedere reproductie van een werk van letterkunde, wetenschap of kunst voorafgaande toestemming van de maker of zijn rechtverkrijgende nodig. Zonder die toestemming wordt inbreuk op het auteursrecht gemaakt. Artikel 15o van de Auteurswet voorziet echter in een uitzondering op het reproductierecht voor tekst- en datamining. Aan de inroepbaarheid van die uitzondering zijn twee voorwaarden verbonden. In de eerste plaats moet de degene die zich op de uitzondering beroept rechtmatig toegang hebben tot het werk dat wordt gekopieerd om tekst- en datamining mogelijk te maken. Van rechtmatige toegang tot het werk is uiteraard sprake als het werk voor het publiek online vrijelijk beschikbaar is gesteld. In de tweede plaats moet de maker van het werk of zijn rechtverkrijgende het recht om een reproductie te maken ten behoeve van tekst- en datamining niet op passende wijze hebben voorbehouden. Of daarvan sprake is bij de artikelen waaruit ChatGPT put, is mij niet bekend. Een reproductie mag blijkens het bepaalde in artikel 15o, tweede lid, van de Auteurswet worden bewaard zolang dit nodig is voor tekst- en datamining. Daarna moet de reproductie worden verwijderd. Anders is sprake van inbreuk op het auteursrecht. De regeling is geënt op artikel 4 van richtlijn (EU) 2019/790 van het Europees Parlement en de Raad van 17 april 2019 inzake auteursrechten en naburige rechten in de digitale eengemaakte markt en tot wijziging van Richtlijnen 96/9/EG en 2001/29/EG (PbEU 2019, L130/92). Het geven van een interpretatie is daarmee uiteindelijk aan het Hof van Justitie van de Europese Unie voorbehouden.
In de kabinetsvisie generatieve AI wordt een nadere analyse uitgevoerd van auteursrechtelijke vraagstukken gerelateerd aan generatieve AI, zoals

[4] «In de top-tweehonderd van meest geciteerde websites vonden we Wikipedia en ongeveer elke grote Nederlandse krant, en ook de neonazistische complotwebsite Stormfront. Die laatste staat maar één plek lager in de bronnenlijst dan RTL Nieuws. Van beide websites leert AI dus ongeveer evenveel.»
[5] 90% van de teksten op Wikipedia is geschreven door mannen, 74% van de Reddit gebruikers is man.

ChatGPT. Daarnaast onderzoekt het Rathenau Instituut – in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties – hoe huidig beleid en de bestaande wet- en regelgeving zich verhouden tot generatieve AI. Hierbij zal ook aandacht uitgaan naar (juridische) auteursrechtelijke kwesties betreffende generatieve AI.

Vraag 14
Deelt u de mening dat de Autoriteit Persoonsgegevens zo snel mogelijk met een spoedoordeel moet komen over ChatGPT en het blokkeren ervan geen taboe is? Kunt u de Autoriteit Persoonsgegevens daartoe aansporen?

Antwoord 14
Graag verwijs ik naar het antwoord op de vragen 2 en 3, waaruit volgt dat de AP zelf reeds een stap heeft gezet.

Vraag 15
Kunt u deze vragenset zo snel als mogelijk beantwoorden?

Antwoord 15
De vragen zijn zo spoedig mogelijk beantwoord.