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

2735

Vragen van het lid **Van Raan** (PvdD) aan de Staatssecretaris van Binnenlandse Zake en Koninkrijksrelaties over *het aan banden leggen van ChatGPT in Italië vanwege privacyzorgen en de consequenties hiervan voor Nederland* (ingezonden 1 mei 2023).

Antwoord van Minister **Weerwind** (Rechtsbescherming) mede namens de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties (ontvangen 30 mei 2023).

Vraag 1
Kent u het bericht «ChatGPT banned in Italy over privacy concerns»?[1]

Antwoord 1
Ja.

Vraag 2
Klopt het dat de Italiaanse toezichthouder besloten heeft tot het aan banden leggen van ChatGPT omdat het bedrijf erachter (OpenAI) mogelijk de Europese privacywetgeving overtreedt?

Antwoord 2
Voor informatie over het handelen van de Italiaanse privacytoezichthouder ben ik aangewezen op openbare bronnen. Blijkens de website van deze toezichthouder, de «Garante per la Protezione dei Dati Personali» (hierna: de Garante) heeft zij aan OpenAI laten weten dat ChatGPT voorlopig geen gegevens van Italiaanse gebruikers mocht verwerken, vanwege zorgen over de naleving van de privacyregels.[2] Deze zorgen zagen op de informatie die aan betrokkenen wordt verstrekt wanneer hun persoonsgegevens worden verwerkt, welk mechanisme voor leeftijdsverificatie wordt toegepast, of de door ChatGPT verwerkte persoonsgegevens voldoen aan het beginsel van juistheid en actualiteit (artikel 5, lid 1, onder d van de AVG) en tot slot op basis van welke rechtsgrondslag persoonsgegevens worden verzameld en verwerkt ten behoeve van het trainen van het onderliggende algoritme. ChatGPT is sinds 28 april jl. weer beschikbaar in Italië. De Garante heeft daarover op haar website geschreven dat OpenAI maatregelen en verbeterin-

[1] https://www.bbc.com/news/technology-65139406
[2] https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9881490

ah-tk-20222023-2735
ISSN 0921 - 7398
's-Gravenhage 2023

gen heeft getroffen in het licht waarvan het verbod is opgeheven voor Italiaanse gebruikers. De Garante spreekt de hoop uit dat OpenAI de komende weken zal voldoen aan de verdere verzoeken van de Garante. Dat ziet op de implementatie van een leeftijdsverificatiesysteem en het verzorgen van een communicatiecampagne om alle Italianen te informeren over wat er is gebeurd en over de mogelijkheid om zich te verzetten tegen het gebruik van hun persoonlijke gegevens om een algoritme te trainen. De Garante schrijft dat zij zal doorgaan met het vooronderzoek dat is gestart tegen OpenAI en met het werk dat zal worden uitgevoerd door de taskforce die is opgericht binnen het Europees Comité voor gegevensbescherming (European Data Protection Board, (EDPB)). Zie hierover het antwoord op vraag 3.

Vraag 3
Klopt het dat er een Europese taskforce is opgericht? Wat is de status en bevoegdheid van zo'n taskforce? Is de Nederlandse toezichthouder daar ook bij betrokken? Zo nee, waarom niet?

Antwoord 3
De Autoriteit Persoonsgegevens (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.

Vraag 4
Hoe worden de beide Kamers geïnformeerd over de werkzaamheden en uitkomsten van de taskforce?

Antwoord 4
De EDPB publiceert nieuwsberichten op haar website, zo ook in dit geval.[3] Wanneer er op het gebied van de taskforce (beleids)ontwikkelingen zijn, zullen deze daar worden geplaatst. Daarnaast zal de AP hierover bij gelegenheid berichten laten uitgaan.

Vraag 5
Weet u welke persoonsgegevens worden verzameld en verwerkt door ChatGPT (OpenAI) in Nederland? Is dat ook bekend voor de gebruikers?

Antwoord 5
Dat is mij niet bekend. Op de website van OpenAI wordt voor gebruikers en niet-gebruikers, zowel binnen als buiten Europa, gemeld welke persoonsgegevens met welke methoden worden verwerkt.[4]

Vraag 6
Indien persoonsgegevens verzameld en verwerkt worden door ChatGPT (OpenAI) in Nederland, op welke wettelijke basis gebeurt dat dan?

Antwoord 6
Over die informatie beschik ik niet. Op de in antwoord 5 genoemde website noemt OpenAI als rechtsgronden voor het verwerken van persoonsgegevens[5] de uitvoering van een overeenkomst (artikel 6, eerste lid onder b AVG),[6] het gerechtvaardigde belang (artikel 6, eerste lid onder f AVG) van het tegengaan van misbruik, fraude of veiligheidsrisico's of van het ontwikkelen, verbeteren

[3] https://edpb.europa.eu/news/news/2023/edpb-resolves-dispute-transfers-meta-and-creates-task-force-chat-gpt_en
[4] https://openai.com/policies/privacy-policy
[5] https://www.bbc.com/news/technology-65139406
[6] https://www.rtlnieuws.nl/tech/artikel/5375256/chatgpt-chatbot-privacy-datalek

of promoten van haar diensten of[7] toestemming (artikel 6, eerste lid onder a AVG) voor een specifiek doel dat aan de betrokkene wordt meegedeeld.

Vraag 7
Bent u het met ons eens dat verzameling en verwerking van persoonsgegevens altijd een wettelijke basis moet hebben? Zo nee, op welke gronden zou die wettelijke basis afwezig mogen zijn?

Antwoord 7
Voor een rechtmatige verwerking van persoonsgegevens moet een grondslag bestaan. Dit zijn de zes limitatieve grondslagen zoals opgesomd in artikel 6, eerste lid, van de AVG. Wanneer een verwerking niet op een van die grondslagen gebaseerd kan worden, is zij onrechtmatig.

Vraag 8
Indien de wettelijke basis voor verzameling en verwerking van persoonsgegevens afwezig mag zijn (en de wettelijke basis is aanwezig), op welke manier voldoet (het werken met) ChatGPT daaraan?

Antwoord 8
Het is niet aan mij om daarover te oordelen. Dat is veeleer een vraag die door de toezichthouder zal worden beoordeeld.

Vraag 9, 10 en 11
Klopt het dat er bij ChatGPT ook sprake is geweest van een datalek waarbij gesprekken en betaalgegevens zijn gelekt?[8]
Zo ja, zijn hierbij ook gegevens van Nederlandse gebruikers gelekt?
Zo ja, is dit datalek gemeld bij de Autoriteit Persoonsgegevens, conform de Algemene Verordening Gegevensbescherming (AVG)? Zo nee, waarom niet?

Antwoord 9, 10 en 11
Van een datalek is sprake wanneer er ongeoorloofde of onbedoelde toegang tot persoonsgegevens heeft plaatsgevonden, maar ook als deze gegevens ongewenst zijn vernietigd, verloren, gewijzigd of verstrekt. Desgevraagd heeft de AP mij laten weten dat bij haar geen melding is gedaan van het lekken van gegevens van Nederlandse gebruikers.
Of een dergelijke melding aan de AP verplicht zou zijn geweest onder de meldplicht datalekken, is afhankelijk van de vraag waar een hoofdvestiging is gevestigd. Wanneer een hoofdvestiging niet in Nederland is gevestigd, maar in een andere lidstaat van de Europese Unie, dan is de toezichthouder in die lidstaat leidend. Een datalek moet dan verplicht bij de leidende toezichthouder worden gemeld, ook al zijn er Nederlandse gebruikers betrokken bij het datalek. Melding aan de AP is vervolgens optioneel en alleen verplicht wanneer de verwerkingsverantwoordelijke twijfelt bij welke toezichthouder gemeld moet worden. In het geval van OpenAI, de verwerkingsverantwoordelijke van ChatGPT, is er geen sprake van een hoofdvestiging in de Europese Unie. Dan zijn alle Europese privacytoezichthouders gelijkelijk bevoegd. Dit betekent dat er alleen bij de AP gemeld moet worden als er Nederlandse ingezetenen bij het datalek betrokken zijn.

Vraag 12
Bent u bereid de Autoriteit Persoonsgegevens om een spoedadvies te vragen over het blokkeren van ChatGPT? Zo nee, waarom niet?

Antwoord 12
Onder verwijzing naar antwoord 3 en de daarin genoemde taskforce van de EDPB, waarin ook de AP vertegenwoordigd is, moet ik hierop ontkennend antwoorden omdat de kwestie reeds door de AP mede beoordeeld wordt. Ik vertrouw er bovendien op dat de AP in het kader van haar voorlichtende taak naar buiten zal treden over ChatGPT wanneer daartoe aanleiding bestaat.

---

[7] https://www.ad.nl/tech/nieuwe-functie-snapchat-wil-met-kinderen-afspreken-zie-ik-je-vanavond-ik-ben-een-echt-persoon~a3f9f4bb/

[8] https://www.rtlnieuws.nl/tech/artikel/5375256/chatgpt-chatbot-privacy-datalek

Vraag 13
Klopt het dat Nederlandse en Italiaanse privacywetgeving – vanwege de gedeelde Europese basis – vergelijkbaar zijn? Zo nee, waarin verschillen de Italiaanse en de Nederlandse interpretatie van de Europese privacywetgeving? Zo ja, deelt u de mening dat Nederland net als Italië zou moeten omgaan met ChatGPT?

Antwoord 13
In de gehele Europese Unie is sinds 25 mei 2018 de AVG van kracht. Deze verordening kent lidstaten op onderdelen de bevoegdheden en verplichtingen toe om nadere regels te stellen. In Nederland is die ruimte onder meer ingevuld door de Uitvoeringswet AVG (UAVG). Over kennis inzake de Italiaanse pendant van de UAVG beschik ik niet. De vragen van de Italiaanse toezichthouder met betrekking tot ChatGPT waren evenwel alle rechtstreeks te herleiden tot bepalingen uit de AVG zelf. Ik zie dan ook op voorhand geen verschillen ten aanzien van de regels die Italië en Nederland op ChatGPT worden toegepast.

Vraag 14
Op welke manier bent u bereid in Nederland het gebruik van ChatGPT zodanig aan banden te leggen dat de kans op overtreding van AVG minimaal is?

Antwoord 14
Dit is niet aan mij. De taken en bevoegdheden om op te treden tegen overtredingen van de AVG zijn toegekend aan de toezichthoudende autoriteiten; voor Nederland is dat de AP. Zij kan daartoe handhaven, advies verstrekken, samenwerken met andere toezichthoudende autoriteiten en klachten behandelen over een inbreuk op de bescherming van persoonsgegevens. Op welke wijze de nationale toezichthoudende autoriteiten de taken prioriteren in de uitvoering is aan henzelf. Zij hebben eigen beoordelings- en beleidsvrijheid.

Vraag 15
Welke andere gevaren ziet u, naast het ongeoorloofd verzamelen en verwerken van persoonsgegevens, van het gebruik van ChatGPT of vergelijkbare AI-systemen?

Antwoord 15
Het afgelopen half jaar zijn de capaciteiten van en de aandacht voor generatieve AI sterk toegenomen. Dit was sneller dan verwacht. We hebben het afgelopen half jaar al gezien dat deze AI-systemen zowel kansen bieden als risico's hebben. In de beantwoording van eerdere vragen van uw Kamer is het kabinet al ingegaan op een aantal van deze risico's.[9] Deze effecten kunnen voortkomen uit de werking van de tool, waar het ondanks ingebouwde waarborgen mogelijk is om bevooroordeelde of discriminerende antwoorden te krijgen. Ook kunnen deze systemen gebruikt worden voor schadelijke doeleinden zoals phishing en desinformatie. Verder heeft de introductie van deze AI-systemen impact op onder meer het onderwijs en de arbeidsmarkt.
De snelheid waarmee generatieve AI zich afgelopen half jaar heeft ontwikkeld brengt onzekerheden met zich mee. Er zijn nog veel vraagtekens over de precieze impact en de gevaren. Het is van belang dat we daar meer kennis over opdoen. Het kabinet werkt daarom momenteel aan een kabinetsvisie op nieuwe AI-systemen zoals generatieve AI. In deze visie zal het kabinet nader ingaan op de risico's van deze AI-systemen.

[9] Aanhangsel Handelingen II 2022/23, nr. 1835, 2037 en 2039.

Vraag 16
Zijn er soortgelijke bedrijven en/of vergelijkbare AI-systemen die op eenzelfde of andere manier de wet lijken te overtreden? Bent u bijvoorbeeld bekend met de AI van Snapchat die probeert kinderen tot een fysieke afspraak te bewegen?[10] Voorziet u dat dit mis kan gaan?

Antwoord 16
Het is aan de AP om toezicht te houden op de verwerking van persoonsgegevens door bedrijven en signalen op te pikken wanneer de regels worden overtreden. Het kabinet houdt vanzelfsprekend de ontwikkelingen in de gaten en is bekend met het AI-systeem van Snapchat. In de beantwoording van schriftelijke vragen van het Kamerlid Kathmann en van de Kamerleden Stoffer en Drost gaat het kabinet daar nader op in.[11] Het is van belang dat de AI-verordening waarin in Europa aan gewerkt wordt niet te lang op zich laat wachten. In de AI-verordening zijn AI-systemen onderverdeeld in verschillende categorieën. Afhankelijk van de categorie waarin een AI-systeem valt, gelden zwaardere of minder zware regels. Aanbieders van AI-systemen die voor interactie met natuurlijke personen zijn bedoeld (zoals chatbots), moeten ervoor zorgen dat die systemen zodanig worden ontworpen en ontwikkeld dat natuurlijke personen worden geïnformeerd dat zij met een AI-systeem te maken hebben, tenzij uit de omstandigheden en gebruikscontext al blijkt dat sprake is van een AI-systeem.

Vraag 17
Is de Autoriteit Persoonsgegevens bereid hier sectorbreed op te handhaven, ook op toekomstige (geavanceerdere) AI-systemen? Zo ja, wanneer kunnen zij hiermee starten? Zo nee, waarom willen zij dat niet?

Antwoord 17
De AP is toezichthouder op de naleving van de bescherming van persoonsgegevens; dus ook als deze gegevens worden verwerkt in algoritmes en AI-systemen in verschillende sectoren. De AP houdt de ontwikkelingen van generatieve AI-systemen, zoals *large language models*, scherp in de gaten. Bovendien ziet de AP dat generatieve AI onderdeel uitmaakt van het wetgevingsproces rond de AI-verordening. Daarnaast is binnen de AP begin 2023 een nieuw organisatieonderdeel opgericht: de directie Coördinatie Algoritmes (DCA). In 2023 pakt de DCA als activiteiten op:
1. (Sector- en domeinoverstijgende) signalen en inzichten over de risico's en effecten van algoritmegebruik verzamelen, analyseren en kennis daarover delen;
2. Bestaande samenwerkingen bij algoritmetoezicht versterken en faciliteren;
3. Gezamenlijke en sectoroverstijgende normuitleg en «guidance» bevorderen.

Deze coördinerende rol is een nieuwe taak voor de AP die de komende jaren nader vorm zal krijgen. Een van de uitgangspunten in de uitvoering van haar activiteiten is dat het bestaande toezicht op algoritmes en AI intact blijft. Dit toezicht, en daarmee de handhavingsbevoegdheid, ligt bij verschillende colleges, markttoezichthouders en rijksinspecties. De AP vindt het van belang om meer te grip krijgen op een verantwoorde ontwikkeling en inzet van algoritmes. Een door de DCA gecoördineerde aanpak draagt bij aan de harmonisatie en effectiviteit van het gedeelde toezicht op algoritmes en AI. Op 24 maart hebben de leden van het Samenwerkingsplatform Digitale Toezichthouders (SDT) besloten om twee zogeheten Kamers op te richten voor het afstemmen van toezicht op online platforms en op algoritmes en AI.[12] De algoritmes en AI Kamer zal bijdragen aan de activiteiten van de DCA.

---

[10] https://www.ad.nl/tech/nieuwe-functie-snapchat-wil-met-kinderen-afspreken-zie-ik-je-vanavond-ik-ben-een-echt-persoon~a3f9f4bb/

[11] Aanhangsel Handelingen II 2022/23, nr. 7266 en 7267.

[12] https://autoriteitpersoonsgegevens.nl/nl/nieuws/toezichthouders-van-sdt-breiden-samenwerking-digitaal-toezicht-uit.

Vraag 18
Op welke manier is de Autoriteit Persoonsgegevens voorbereid op de exponentiële groei van de capaciteit en dus ook de risico's van het gebruik van ChatGPT of vergelijkbare AI-systemen? Beschikt ze naar uw mening over voldoende kennis en capaciteit? Zo nee, hoe gaat u dat oplossen?

Antwoord 18
De AP heeft voldoende expertise om toezicht te houden op de bescherming van persoonsgegevens, ook indien die verwerkt worden door AI-systemen zoals ChatGPT. Daarnaast zet de DCA van de AP zich in om de samenwerking tussen toezichthouders te versterken, domein overstijgende signalen op te vangen en kennis te delen over het toezicht op algoritmes. De wijze waarop de AP de middelen die hen ter beschikking worden gesteld verdeelt over deze afzonderlijke taken is uitsluitend aan de AP, als onafhankelijke toezichthouder. Daarnaast investeert het kabinet in de AP om haar taken uit te voeren, oplopend tot structureel 8 miljoen euro per jaar vanaf 2025. Hierdoor kan de AP verdere stappen zetten, onder andere op het gebied van AI-systemen. In de Kamerbrief over toezicht in het digitale domein van 24 mei 2023 is nader ingegaan op het toezicht op algoritmes en AI.[13] Daarin wordt ook ingegaan op de vraag of de AP over voldoende kennis beschikt.

[13] Kamerstukken II 2023/22 nr 9180.