AUTORITEIT
PERSOONSGEGEVENS

Datum
9-5-2023

Ambtsbericht

Onderwerp
Informatievoorziening voor de beantwoording van Kamervragen van het lid Van Raan (PvdD) over het aan banden leggen van ChatGPT in Italië vanwege privacyzorgen en de consequenties hiervan voor Nederland

Het lid Van Raan (PvdD) heeft Kamervragen gesteld aan de Staatssecretaris van Koninkrijksrelaties en Digitalisering over het aan banden leggen van ChatGPT in Italië vanwege privacyzorgen en de consequenties hiervan voor Nederland. Dit ambtsbericht dient ter verschaffing van informatie aan het Ministerie van Justitie en Veiligheid voor de beantwoording van de vragen 3, 9, 10, 11, 17 en 18.

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?

Informatie voor beantwoording van vraag 3:
Op 13 april heeft het samenwerkingsverband van Europese privacytoezichthouders (de European Data Protection Board, ook wel EDPB) naar aanleiding van het Italiaanse optreden tegen OpenAI inzake ChatGPT besloten om een taskforce in te stellen. De Taskforce ChatGPT heeft tot doel de samenwerking en informatie-uitwisseling over mogelijke handhavingsmaatregelen te bevorderen. Alle Europese privacytoezichthouders zijn in dit samenwerkingsverband vertegenwoordigd, dus ook de Autoriteit Persoonsgegevens (AP). Generatieve AI, zoals het *large language model* kunstmatige intelligentie (AI) systeem ChatGPT, zijn een grensoverschrijdend fenomeen die vragen om een geharmoniseerde aanpak. Daarom hecht de AP grote waarde aan effectief gezamenlijk optreden van de Europese privacytoezichthouders.

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

Informatie voor beantwoording van vragen 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. Er is bij de AP geen melding 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 EU-lidstaat, 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 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?

Informatie voor beantwoording van vraag 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 Artificial Intelligence Act (AI Act). Regulering, en bijbehorend toezicht, zal gepaard moeten gaan met een uitbreiding van de personele capaciteit van de digitale toezichthouders.

Daarnaast is binnen de AP begin 2023 een nieuw organisatieonderdeel opgericht: de directie Coördinatie Algoritmes (DCA). In 2023 pakt de AP een drietal concrete activiteiten op, namelijk:

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. Het is van belang dat we als samenleving meer 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. De algoritmes en AI Kamer zal bijdragen aan de activiteiten van de DCA.

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?

Datum
9-5-2023

Informatie voor beantwoording van vraag 18:
Het kabinet investeert van 2022 tot en met 2026 steeds meer in de AP. Hierdoor kan de AP een aantal mooie stappen zetten. De AP is echter ook bezorgd. De financiering van het toezicht op persoonsgegevens blijft nog altijd ver achter bij de hoge mate van digitalisering van Nederland. Nieuwe ontwikkelingen, zoals rond generatieve AI, gaan bovendien razendsnel. Om haar opgave goed te kunnen vervullen, moet het budget van de AP daarom groeien naar een structurele financiering van ongeveer 100 miljoen euro per jaar.