Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2023–2024

Aanhangsel van de Handelingen

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

2481

Vragen van het lid **Valize** (PVV) aan de Ministers van Economische Zaken en Klimaat en de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties over *het bericht van Elon Musk op X waarin hij stelt alle apparaten van Apple te zullen weren uit zijn bedrijven wanneer OpenAI geïntegreerd wordt op OS-niveau* (ingezonden 13 juni 2024).

Antwoord van Minister **Beljaarts** (Economische Zaken), mede namens de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties (ontvangen 9 september 2024). Zie ook Aanhangsel Handelingen, vergaderjaar 2023–2024, nr. 2098.

Vraag 1
Bent u bekend met het volgende bericht van de heer Musk?[1]

Antwoord 1
Ja, ik heb kennisgenomen van dit bericht.

Vraag 2
Bent u bekend met het vijf dagen eerder verschenen artikel «*Het rommelt bij OpenAI, de maker van ChatGPT: kritiek op veilig gebruik van artificial intelligence komt van binnen en buiten*» gepubliceerd door Business Insiders Nederland op 5 juni 2024?[2]

Antwoord 2
Ja, ik heb kennisgenomen van dit bericht.

Vraag 3
Deelt u de opvatting van de heer Musk dat de integratie van OpenAI op OS-niveau van Apple producten, zoals verkondigd door Apple op de WWDC (Worldwide Developers Conference), een potentieel veiligheidsrisico kan vormen voor deze apparaten? Zo nee, waarom niet?

[1] Elon Musk op X: «If Apple integrates OpenAI at the OS level, then Apple devices will be banned at my companies. That is an unacceptable security violation.» / X
[2] Het rommelt bij ChatGPT-maker OpenAI (alweer) (businessinsider.nl)

ah-tk-20232024-2481
ISSN 0921 - 7398
's-Gravenhage 2024

Antwoord 3
Het integreren van producten van derde partijen in Apple producten, maar ook producten van vergelijkbare partijen, is een veel voorkomend proces. Dit integratieproces kan veiligheidsrisico's met zich mee brengen, waarbij de potentiële kwetsbaarheden over het algemeen toenemen naarmate de integratie diepgaander wordt. In het specifieke geval van AI-integratie binnen een besturingssysteem, zoals de integratie van OpenAI op OS-niveau, worden deze risico's verder geïntensiveerd. Deze vorm van integratie vereist namelijk toegang tot gevoelige gegevens en kerncomponenten van het OS, wat verder gaat dan conventionele integraties. Apple heeft aangegeven in openbare berichtgeving dat er in dit proces data wordt uitgewisseld met externe partijen. Ook heeft Apple in openbare berichtgeving aangegeven maatregelen te hebben getroffen om de cybersecurity en dataprivacy te borgen. Daar zijn geen technische details over openbaar gemaakt. Uiteraard moeten dergelijke integraties voldoen aan de relevante wet- en regelgeving, zoals verder staat toegelicht in de beantwoording van vragen 7 en 8.
Apple heeft overigens de uitrol van de integratie van ChatGTP van OpenAI binnen de EU uitgesteld (zie hiervoor ook de beantwoording van vraag 6, 7 en 8).

Vraag 4
Deelt u de mening dat de scheidingslijn tussen «lokaal opgeslagen» en «opgehaald/gedeeld middels geautoriseerde apps» geen heldere barrière kent en derhalve flinterdun genoemd mag worden? Graag een onderbouwing van uw beantwoording.

Antwoord 4
De scheidingslijn tussen lokaal opgeslagen gegevens en gedeelde gegevens is technisch gezien duidelijk, namelijk dat lokaal opgeslagen gegevens zich bevinden op het apparaat van de gebruiker, terwijl gedeelde gegevens worden overgedragen naar externe servers. Tegelijkertijd is voor gebruikers niet altijd duidelijk wat er wel of niet gebeurt met hun gegevens. Dit komt door de complexiteit van moderne besturingssystemen en de voortdurende balans tussen gebruiksgemak en beveiliging. Hierdoor kan lokale informatie op verschillende manieren, zowel actief (aangevinkt door de gebruiker) als automatisch (bijvoorbeeld via virusscans, en spellingcheckers), met externen worden gedeeld zonder dat de gebruiker zich hiervan bewust is.

Vraag 5
Vindt u dat dergelijk potentieel veiligheidsrisico voor een overheidsorgaan onwenselijk is? Zo nee, waarom niet?

Antwoord 5
In algemene zin kunnen veiligheidsrisico's die ontstaan door integraties van producten van derde partijen in een besturingssysteem onwenselijk zijn voor de overheid. Zo is een risico van oneigenlijk delen en verwerken van gegevens van smartphonegebruikers onwenselijk. Tegelijkertijd zijn er maatregelen mogelijk om deze risico's te mitigeren. Ook moeten dergelijke integraties voldoen aan de relevante wet- en regelgeving, zoals verder staat toegelicht in de beantwoording van vragen 7 en 8. Apple geeft aan te werken aan uitgebreide bescherming van persoonsgegevens voor hun AI-toepassingen, bijvoorbeeld middels «Private Cloud Compute (PCC)»[3]. De PCC ontvangt gegevens van het toestel van de gebruiker voor het uitvoeren van een AI-toepassing wanneer deze niet op het toestel zelf kunnen worden uitgevoerd. Na ontvangst worden de gegevens gebruikt voor het uitvoeren en worden deze na gebruik gelijk verwijderd. Gegevens in de PCC worden volgens Apple niet gedeeld met derden en zouden ook niet door Apple verder worden verwerkt.

Vraag 6
Wat bent u voornemens te gaan doen om hieraan gerelateerde potentiële veiligheidsrisico's in kaart te brengen en tevens in te perken?

[3] Apple sets a new standard for privacy in AI - Apple (EE)

Antwoord 6
Voor het inzetten van AI-toepassing binnen de Rijksoverheid gelden verschillende risico mitigerende maatregelen. Deze maatregelen zijn verwerkt in zowel (EU) wet- en regelgeving alsook de inkoopvoorwaarden voor ICT. Dit betekent enerzijds dat Apple zelf verantwoordelijk is voor het naleven van de inkoopvoorwaarden en anderzijds zij op wet- en regelgeving getoetst en gecontroleerd worden door Rijksoverheidsorganisaties en toezichthouders. Voor het gebruik van generatieve AI-toepassingen, zoals die van Apple, geldt nog steeds het voorlopige standpunt generatieve AI over het gebruik door Rijksorganisaties van generatieve AI.[4] Hierin staat dat voor het inzetten van een AI-toepassing, deze onderworpen moet worden aan een Impact Assessment Mensenrechten Algoritme (IAMA) en een Data Protection Impact Assessment (DPIA). De uitkomsten van de DPIA en IAMA dienen voor inzet van de toepassing ter advies aan de (departementale) Chief Information Officer (CIO) en de Functionaris Gegevensbescherming (FG) te worden voorgelegd. Door middel van deze maatregelen worden potentiële veiligheidsrisico's op tijd gesignaleerd en kan er doelmatig ingegrepen worden. Leveranciers hebben ook een eigen verantwoordelijkheid om te voldoen aan wetgeving en inkoopvoorwaarden. Zoals in antwoord op vraag 3 benoemd, heeft Apple vooralsnog de uitrol van de AI integratie binnen de EU uitgesteld.

Vraag 7
In hoeverre past een integratie van AI op OS-niveau binnen de kaders van de DMA, DSA, AI-Act en andere relevante wetten, regels en verordeningen?

Antwoord 7
Het is aan de toezichthouders en uiteindelijk aan de rechters op Europees en nationaal niveau om te bepalen in hoeverre een integratie van AI op OS-niveau binnen de bestaande kaders van relevante wet- en regelgeving past. In de Digital Markets Act (DMA) en de AI-verordening staan bepalingen die ingaan op onder andere interoperabiliteitsverplichtingen en de verantwoordelijkheden binnen de waardeketen van AI. Besturingssystemen vallen niet binnen de reikwijdte van de Digital Services Act (DSA).
Apple is door de Europese Commissie aangewezen als poortwachter onder de DMA voor verschillende kernplatformdiensten. De iOS-diensten van Apple vallen onder het toepassingsgebied van de DMA en zijn door de Commissie aangewezen als kernplatformdienst in de categorie besturingssysteem (artikel 2, tweede lid, onder f). Dit betekent dat Apple moet zorgen voor effectieve naleving van de maatregelen in de DMA die van toepassing zijn op besturingssystemen, zoals het verbod op het combineren van data of de interoperabiliteitsverplichtingen. Op basis van artikel 5, tweede lid, van de DMA mag Apple bijvoorbeeld niet zonder toestemming persoonsgegevens gebruiken in andere diensten die Apple afzonderlijk aanbiedt.
Onder de DMA zijn diensten die gebruikmaken van AI niet opgenomen als afzonderlijke kernplatformdienst. Uit overweging 14 van de DMA volgt echter dat de definitie van kernplatformdiensten voor de toepassing van deze verordening technologieneutraal is en ook diensten omvat die langs verschillende wegen worden aangeboden. De onderliggende technologie waar het besturingssysteem op leunt, kan op deze wijze dus ook onder het toepassingsgebied van de DMA komen te vallen. Dat betekent echter niet dat de DMA zich verzet tegen een integratie van AI op OS-niveau, mits Apple zich voor haar iOS-diensten houdt aan de verplichtingen en verboden die volgen uit de DMA.
Onder de AI-verordening zijn aanbieders van AI-modellen voor algemene doeleinden met ingang van 2 augustus 2025 verplicht om informatie en documentatie op te stellen, up-to-date te houden en beschikbaar te stellen voor toezichthouders en aanbieders die dat AI-model in hun AI-systemen willen integreren. De bedoeling is dat deze informatie en documentatie inzicht geeft in de capaciteiten en beperkingen van het AI-model voor algemene doeleinden en daarmee aanbieders verderop in de waardeketen die met dit model verder bouwen aan specifiekere AI-modellen of -systemen in staat stelt aan hun verplichtingen uit de AI-verordening te voldoen.

[4] Voorlopig standpunt generatieve AI Kabinet | Nieuwsbericht | Rijksoverheid.nl

Als AI-modellen voor algemene doeleinden voor systeemrisico's kunnen zorgen, dan moeten ze volgens de AI-verordening aan extra eisen voldoen. Dit kan het geval zijn als er zeer veel computerkracht gebruikt is bij het trainen van het model, maar ook het aantal eindgebruikers kan een relevante factor zijn bij de beoordeling of een AI-model voor systeemrisico's kan zorgen. Modellen met systeemrisico's moeten onder andere modelevaluaties uitvoeren, risico's beoordelen en beperken en zorgen voor een passend niveau van cybersecurity. Ook moeten incidenten zo snel mogelijk gemeld worden bij het Europese AI-bureau, dat toezicht houdt op deze modellen.

Vraag 8
Wat gaat u doen om de privacy van onze burgers te borgen?

Antwoord 8
De privacy van burgers binnen het digitale domein wordt op verschillende manieren geborgd. Binnen de EU wordt het grondrecht op gegevensbescherming wettelijk beschermd via de Algemene Verordening Gegevensbescherming (AVG). Toezicht en handhaving op de rechtmatigheid van gegevensverwerking in de publiek en private sector wordt in Nederland gedaan door de Autoriteit Persoonsgegevens (AP).
De AP is een onafhankelijke toezichthouder en heeft ruim mandaat en uitgebreide bevoegdheden om te onderzoeken of partijen voldoen aan hun verplichtingen uit de AVG. Zo heeft de AP als toezichthoudend autoriteit de bevoegdheid om organisaties te gelasten alle informatie voor hun onderzoek te verstrekken (art. 58, AVG). Ook is de AP bevoegd om sancties op te leggen als een organisatie de privacywetgeving overtreedt. Sancties die de AP kan opleggen zijn: waarschuwingen, berispingen, last onder dwangsom, boetes (maximaal 20 miljoen of 4% van de wereldwijde jaaromzet) of een verwerkingsverbod.
In de casus van Apple wordt het toezicht niet door de AP opgepakt, maar door de Ierse privacyautoriteit. Het Europese hoofdkantoor van Apple is namelijk gevestigd in Cork, Ierland. Dit houdt in dat, aangezien de hoofdvestiging zich in Ierland bevindt, de leidende toezichthoudende autoriteit conform artikel 56 uit de AVG de Ierse toezichthouder is. De Ierse toezichthouder heeft eenzelfde mandaat en bevoegdheden als de Nederlandse AP en zij werken bij grensoverschrijdende gegevensverwerkingen nauw samen. Deze samenwerking vindt plaats middels de European Data Protection Board (EDPB).