

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

981

Vragen van het lid **Ergin** (DENK) aan de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties over *het gebruik van AI-systemen door de overheid en de risico's daarvan waar niet naar wordt gekeken* (ingezonden 30 oktober 2024).

Antwoord van Staatssecretaris **Szabó** (Binnenlandse Zaken en Koninkrijksrelaties) (ontvangen 8 januari 2025)

Vraag 1

Bent u bekend met het bericht van de NOS getiteld «Overheid maakt volop gebruik van AI, maar kijkt vaak niet naar risico's»?¹

Antwoord 1

Ja, hier ben ik mee bekend.

Vraag 2

Hoe beoordeelt u het feit dat bij meer dan de helft van de systemen die gebruikmaken van kunstmatige intelligentie (AI) binnen de overheid geen gedegen risicoanalyse wordt uitgevoerd, zoals blijkt uit het onderzoek van de Algemene Rekenkamer (ARK)?

Antwoord 2

Het is belangrijk dat er voor dit soort systemen een gedegen risicoanalyse wordt gemaakt. Het is straks verplicht om voor hoog-risico AI-systemen de risico's af te wegen onder de AI-verordening. Vooruitlopend op de AI-verordening en ook voor AI-systemen die niet als hoog risico worden gecategoriseerd bestaan er al verschillende instrumenten om een dergelijke risicoafweging te maken, bijvoorbeeld de Impact Assessment Mensenrechten en Algoritmen (IAMA).

Vraag 3

Welke stappen neemt u om ervoor te zorgen dat alle overheidsinstanties de risico's van AI-gebruik adequaat in kaart brengen volgens de geldende wet- en regelgeving, met bijzondere aandacht voor mensenrechten en privacy?

¹ NOS, 16 oktober 2024, «Overheid maakt volop gebruik van AI, maar kijkt vaak niet naar risico's» (nos.nl/artikel/2540979-overheid-maakt-volop-gebruik-van-ai-maar-kijkt-vaak-niet-naar-risico-s).

Antwoord 3

Alle AI-systemen moeten voldoen aan geldende wet- en regelgeving, ook de systemen met beperkte risico's. Hiertoe bestaan vele instrumenten. In het algoritmekader wordt een overzicht geboden van de bestaande wettelijke verplichtingen, waaronder de AI-verordening. Ook wordt daarin verwezen naar maatregelen en worden verschillende instrumenten samengebracht om organisaties binnen de overheid te ondersteunen. Mensenrechtentoetsen, de AVG en het verbod op discriminatie zijn daar onderdeel van.

Vraag 4

Kunt u uitleggen waarom slechts vijf procent van de AI-systemen is opgenomen in het openbare algoritmeregister, terwijl dit register juist werd opgezet naar aanleiding van de Toeslagenmisdaad? Zo nee, waarom niet?

Antwoord 4

Niet alle AI-systemen hoeven in het Algoritmeregister te worden geregistreerd. Bijvoorbeeld als het gaat om een experiment dat geen impact heeft (gehad) op burgers of bedrijven, of als de impact van een AI-systeem met name indirect is.

Mij is bekend dat veel overheden, zowel binnen het Rijk als daarbuiten, bezig zijn met de vulling van het register, maar dat het inventariseren, beoordelen en registreren van AI-systemen tijd en capaciteit vraagt. Alle departementen hebben toegezegd ten minste de hoog-risico AI-systemen eind 2025 geregistreerd te hebben. In de Jaarrapportage Bedrijfsvoering Rijk zullen departementen inzicht verschaffen in de precieze voortgang.

Ik stimuleer overheden, zowel binnen de rijksoverheid als medeoverheden, om te publiceren in het algoritmeregister. Daarvoor neemt het Ministerie van BZK proactief contact op met overheden en wordt er ondersteund met verschillende instrumenten, zoals de handreiking algoritmeregister, templates van leveranciers, ondersteuning van een implementatieteam, zogenoemde aansluitsessies, een regiotour, een nieuwsbrief en artikelen met tips van organisaties die al gepubliceerd hebben.

Vraag 5

Hoe gaat u ervoor zorgen dat alle hoogrisico-AI-systemen voor de deadline van 2026 in het register zijn opgenomen, zoals vereist door Europese regelgeving?

Antwoord 5

Voor registratie in het algoritmeregister verwijs ik u naar vraag 4. Voor wat betreft de Europese databank, verplicht de AI-verordening de registratie van hoog risico AI-systemen door aanbieders en gebruiksverantwoordelijken van deze systemen in een EU-databank. Deze verplichting geldt per 2 augustus 2026 voor nieuwe hoog risico AI-systemen. Het is nog niet precies bekend hoe de EU-databank vormgegeven wordt.

Vraag 6

Welke maatregelen neemt u, gezien de Toeslagenmisdaad en de waarschuwing van de ARK over mogelijke discriminatie door AI-systemen, om te garanderen dat AI-systemen van bijvoorbeeld de Belastingdienst en het Uitvoeringsinstituut Werknemersverzekeringen (UWV) voldoen aan de vereisten van nauwkeurigheid en non-discriminatie?

Antwoord 6

Het Ministerie van Binnenlandse Zaken investeert in de kennis over biastoesing binnen de overheid, zodat overheden- die daar zelf verantwoordelijk voor zijn – tijdig de juiste maatregelen nemen om dit te voorkomen. Het Ministerie van BZK heeft in 2021 een handreiking non-discriminatie laten opstellen. Recent is mede op basis van deze handreiking een e-learning module non-discriminatie uitgebracht.² Daarnaast zijn er ook buiten het ministerie initiatieven die erop gericht zijn om nauwkeuriger aan de vereisten van non-discriminatie te voldoen, denk aan bias detectie tools of een gestandaardiseerde werkwijze voor profileringsalgoritmes. Door algoritmes te

² <https://leerplatform.it-academieoverheid.nl/login/index.php>

controleren aan de hand van deze standaard kunnen (indirecte) discriminatie en andere ongewenste effecten van profilering worden bestreden.³ Verschillende van deze hulpmiddelen komen samen in het algoritmekader, waarin ook de aanbeveling van het Rathenau-instituut⁴ is meegenomen om de manier waarop biastoetsing plaatsvindt te versterken.

Vraag 7

Deelt u de zorg van de ARK dat er een prikkel bestaat om AI-systemen niet als hoogrisico in te schatten, zodat men niet hoeft te voldoen de strengere Europese regelgeving?

Antwoord 7

Nee, die zorg deel ik niet. Alle AI-systemen die de overheid gebruikt moeten voldoen aan geldende wet- en regelgeving, waaronder de bepalingen van de AI-verordening die in fases van kracht wordt. Binnen de overheid zijn organisaties momenteel bezig met het inventariseren van de bestaande AI-systemen om vervolgens een inschatting te maken van de classificatie onder de AI-verordening. Op nationaal niveau zal voor deze EU-wetgeving toezicht worden ingericht op hoog-risico AI-systemen, bijvoorbeeld op de verplichting om hoog-risico AI-systemen te registreren in een EU-databank. Voor het niet registreren van deze AI-systemen kunnen sancties worden opgelegd door de toezichthouder. Ook het verkeerd inschatten van AI-systemen die onder de hoog-risico AI-toepassingsgebieden van de AI-verordening vallen, kan leiden tot sancties. Daarnaast spelen ook de Auditdienst Rijk (ADR) en de ARK door onder meer audits en onderzoeken een rol bij het in kaart brengen van risico's op de inzet van AI bij de rijksoverheid.

Vraag 8

Hoe wordt bij de inzet van AI-toepassingen, zoals de inzet van robohonden voor celinspecties bij de Dienst Justitiële Inrichtingen (DJI), gewaarborgd dat de privacy en rechten van gedetineerden worden beschermd en worden er risicoanalyses uitgevoerd?

Antwoord 8

DJI verkent de mogelijkheden van innovaties om de maatschappelijke opgave van DJI verder te kunnen verbeteren. Het is belangrijk dat er voor dit soort systemen een gedegen risicoanalyse wordt gemaakt (zie ook antwoord op vraag 2). In het geval van de robohond onderzoekt DJI in hoeverre een robohond de effectiviteit en efficiëntie van een celinspectie kan vergroten met inachtneming van waarborgen van gedetineerden, zoals privacy. De innovatiepilot loopt nog en duurt waarschijnlijk nog 2 jaar.

Vraag 9

Hoe wordt ervoor gezorgd dat er een duidelijke standaard is voor het testen en monitoren van AI-systemen, met betrekking tot nauwkeurigheid en non-discriminatie, gezien het groeiende gebruik van AI in overheidsdiensten?

Antwoord 9

Aanbieders van hoog-risico AI-systemen moeten ervoor zorgen dat die systemen aan de eisen uit de AI-verordening voldoen. Dit houdt o.a. in dat systemen nauwkeurig werken en niet discrimineren. Deze (abstracte) eisen worden op Europees niveau nader uitgewerkt in concrete technische specificaties. Deze specificaties worden ook wel geharmoniseerde standaarden genoemd. Deze standaarden zijn er nog niet, maar worden momenteel op Europees niveau door o.a. Europese normalisatie-instituten ontwikkeld. Nederland en het kabinet zijn via het Nederlandse normalisatie-instituut (NEN) betrokken bij de uitwerking van deze standaarden.

³ https://algorithmaudit.eu/nl/knowledge-platform/knowledge-base/public_standard_profiling/

⁴ https://www.rathenau.nl/sites/default/files/2022-07/Algoritmes_afwegen_rapport_Rathenau_Instituut.pdf

Vraag 10

Bent u bereid om extra toezicht of huidige controlemechanismen in te stellen om ervoor te zorgen dat AI-systemen niet alleen efficiënt werken, maar ook rechtvaardig en veilig zijn voor burgers?

Antwoord 10

Op dit moment zijn er al verschillende trajecten die bijdragen aan het borgen van veilige en rechtvaardige AI-systemen.

In het kader van de AI-verordening zal toezicht worden ingericht op de ontwikkeling en het gebruik van AI-systemen. Op AI-systemen met een onaanvaardbaar risico of AI-systemen die een hoog risico vormen voor de veiligheid, gezondheid en grondrechten van burgers, zal onder meer toezicht worden gehouden, waarbij overtredingen kunnen leiden tot hoge boetes. Momenteel werken de betrokken ministeries onder leiding van EZ, BZK en JenV uit hoe het toezicht op de AI-verordening het beste kan worden ingericht. Daarbij wordt het advies van de toezichthouders over deze inrichting betrokken.⁵

Naast de AI-verordening is er voor de inzet van AI en algoritmes ook (mogelijk) andere wet- en regelgeving van toepassing. Zo verwerken veel risicovolle toepassingen op het gebied van AI en algoritmes persoonsgegevens. Dit AVG-toezicht is de afgelopen jaren structureel versterkt.

De Directie Coördinatie Algoritmes (DCA) bij de Autoriteit Persoonsgegevens (AP) heeft daarnaast als coördinerend toezichthouder op algoritmes en AI oog voor belangrijke (publieke) waarden als rechtvaardigheid en veiligheid, bijvoorbeeld door het signaleren van risico's en het delen van kennis op dit gebied met andere (sectorale) toezichthouders.

Vraag 11

Welke stappen gaat u ondernemen om in de toekomst getroffen burgers snel en rechtvaardig te compenseren wanneer de overheid discriminerende beslissingen heeft genomen door het gebruik van AI-systemen?

Antwoord 11

Op verzoek van uw Kamer is een eerste versie van een discriminatieprotocol opgesteld.⁶ Deze is opgenomen in het algoritmekader. In dit protocol zijn de lessen van en ervaringen met de Toeslagenaffaire en DUO verwerkt. Het kabinet investeert in vroegtijdige toetsing, maar mocht het ondanks alle voorzorgsmaatregelen toch misgaan, is het belangrijk om een werkwijze te hebben om de situatie te herstellen. Het discriminatieprotocol is een handvat, dat overheidsorganisaties kunnen gebruiken om hun eigen werkwijze in te richten. Een onderdeel van het protocol is om een noodplan achter de hand te hebben om een algoritme te kunnen stoppen. Ook richt het protocol zich op het herstellen van de schade. Onderdeel is het informeren van betrokkenen en zorgdragen voor adequate herstelprocedures.

Vraag 12

Is er op dit moment een procedure ontwikkeld om burgers die zijn benadeeld door discriminerende AI-beslissingen actief te helpen bij het herstellen van hun rechten?

Antwoord 12

Zie antwoord op vraag 11.

Vraag 13

Bent u bereid meer transparantie te bieden over welke AI-systemen in het algoritmeregister als hoogrisico worden ingeschat, specifiek met betrekking tot het risico op discriminatie?

Antwoord 13

Voor de definitie van hoog-risico AI-systemen wordt gebaseerd op de definitie uit de AI-verordening. In de verordening zijn bepaalde toepassingsgebieden als hoog-risico geclassificeerd, vanwege het risico dat zij vormen

⁵ <https://www.autoriteitpersoonsgegevens.nl/documenten/eindadvies-inrichting-ai-toezicht-ap-rdi>

⁶ Kamerstukken II, 2022–23. 29 279 nr. 759

voor onze gezondheid, veiligheid en grondrechten. Daarbij is het verbod op non-discriminatie een bijzonder relevante factor. De verantwoordelijkheid voor het juist classificeren ligt bij de overheidsorganisaties zelf, waarop toezicht gehouden kan worden door een toezichthouder op basis van de AI-verordening. Het algoritmeregister maakt het mogelijk om te filteren op AI-systemen die door overheidsorganisaties zelf gecategoriseerd zijn als hoog-risico.⁷

Vraag 14

Op welke manieren kunnen burgers worden geïnformeerd over de specifieke risico's van deze AI-systemen en hoe zij zich hiertegen kunnen beschermen?

Antwoord 14

De AI-verordening verplicht gebruikers bij het gebruik van hoog-risico AI-systemen voor besluitvorming, de daardoor geraakte natuurlijke persoon hierover te informeren. Daarnaast heeft de natuurlijke persoon een recht op uitleg bij de inzet van bepaalde hoog-risico AI-toepassingen. In het regeerprogramma staat verder dat het kabinet werk maakt van transparantie over het gebruik van AI en algoritmes door de overheid. Momenteel wordt nader bezien hoe hier invulling aan kan worden gegeven.

Vraag 15

Welke maatregelen gaat u nemen om ervoor te zorgen dat burgers, en met name kwetsbare groepen, worden beschermd tegen discriminerende algoritmes die door de overheid worden ingezet, zoals aangegeven door de ARK?

Antwoord 15

Zie o.a. antwoorden op vragen 6, 9, 10 en 11. Het is belangrijk dat de normen goed toepasbaar worden gemaakt, gestandaardiseerde werkwijzen worden ontwikkeld -met name voor de gevoelige (profilerings-)algoritmes, tijdig wordt getoetst, risico's worden gemitigeerd en een werkwijze achter de hand is om schade te herstellen. Aanvullend wil het kabinet ervoor zorgen dat burgers, met name kwetsbare burgers (of organisaties die hen vertegenwoordigen) worden betrokken en hun input leveren. Dat kan via burgerpanels en/of ethische commissies.

Vraag 16

Hoe zorgt u ervoor dat AI-systemen, zoals die van het UWV en de Belastingdienst, die direct van invloed zijn op burgers, niet leiden tot discriminerende keuzes of ongelijke behandeling op grond van etniciteit of nationaliteit?

Antwoord 16

Zie antwoord op vraag 6.

Vraag 17

Hoe wordt voorkomen dat AI-systemen, zoals die in het algoritmeregister, onrechtmatige beslissingen nemen die burgers onterecht benadelen en schade toebrengen?

Antwoord 17

De verantwoordelijkheid hiervoor ligt primair bij de overheidsorganisaties die het AI-systeem inzetten. Zij worden geacht maatregelen te nemen om te voldoen aan wetgeving en daarvoor intern toezicht op te stellen. Het Ministerie van BZK stelt hiervoor hulpmiddelen ter beschikking, zoals de handreiking non-discriminatie by design, het impact assessment mensenrechten en algoritmes (IAMA) en het algoritmekader. Onrechtmatig handelen kan daarnaast opgespoord worden door toezichthouders.

⁷ <https://algoritmes.overheid.nl/nl/algoritme?page=1&publicationcategory=Hoog-risico+AI-systeem>