

Vergaderjaar 2021–2022

22 112

Nieuwe Commissievoorstellen en initiatieven van de lidstaten van de Europese Unie

Nr. 3222

BRIEF VAN DE MINISTERS VAN ECONOMISCHE ZAKEN EN KLIMAAT, JUSTITIE EN VEILIGHEID, VOOR RECHTSBESCHERMING EN VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES EN DE STAATSSECRETARIS VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 15 oktober 2021

Hierbij zenden wij u de beantwoording van de door uw Kamer gestelde vragen in het schriftelijk overleg over de fiches inzake Kunstmatige Intelligentie d.d. 10 september 2021 (Kamerstuk 22 112, nr. 3129 en Kamerstuk 22 112, nr. 3128) (Kamerstuk 22 112, nr. 3221). Tevens vindt u bijgevoegd een reactie op de brief van het Rathenau Instituut inzake de «Zeven aandachtspunten voor de AI- verordening».

De Minister van Economische Zaken en Klimaat,
S.A. Blok

De Minister van Justitie en Veiligheid,
F.B.J. Grapperhaus

De Minister voor Rechtsbescherming,
S. Dekker

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,
K.H. Ollongren

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,
R.W. Knops

Reactie op Rathenau Instituut: Zeven aandachtspunten voor de AI-verordening

Het Rathenau Instituut heeft op 10 september jl. een «Bericht aan het parlement» gepubliceerd. Daarin zijn zeven aandachtspunten voor de AI-verordening opgenomen. Het Rathenau Instituut meent dat aanscherping van de conceptverordening nodig is om de risico's echt te kunnen beteugelen. Daarnaast is het nodig om de maatschappelijke opbrengst van AI-systemen te beoordelen. Het kabinet gaat hieronder in op de zeven aandachtspunten.

1. Beperk de mogelijkheden voor onbewuste beïnvloeding

Artikel 5, onder a, van de conceptverordening verbiedt AI-systemen die subliminale beïnvloedingstechnieken gebruiken en die kunnen leiden tot fysieke of psychologische schade. Rathenau stelt dat onduidelijk is welke situaties onder dit verbod vallen. Daarnaast worden bepaalde vormen van onbewuste beïnvloeding buiten het verbod gehouden, zoals beïnvloeding van consumenten en politieke microtargeting. Ook noemt het Rathenau Instituut andere vormen van schade, zoals maatschappelijke schade. Tot slot wijst het op immersieve technologie (AR, VR en spraaktechnologie) waarmee de beïnvloeding zich uitbreidt.

Het kabinet onderkent het belang van een helder verwoord verbod en neemt dit in algemene zin en in het bijzonder ook voor dit verbod mee in de onderhandelingen over de conceptverordening. Met het Rathenau Instituut deelt het kabinet de opvatting dat er ook andere vormen van schade bestaan. Maatschappelijke schade bijvoorbeeld wordt als zodanig niet genoemd in de conceptverordening, maar kan indirect wel worden voorkomen door het bedoelde verbod op subliminale beïnvloedingstechnieken. Verwezen wordt naar de SO-beantwoording op de BNC-fiches AI (Kamerstuk 22 112, nr. 3221), specifiek de antwoorden op de vragen 32 tot en met 35 van de leden van de D66-fractie en de antwoorden op de vragen 86 tot en met 89 van de leden van GroenLinks-fractie. Daarin wordt ook ingegaan op de uitzondering voor politieke microtargeting.

2. Verbreed de bescherming van kwetsbare groepen tegen onbewuste beïnvloeding

Artikel 5, onder b, van de conceptverordening verbiedt AI-systemen die gebruikmaken van de kwetsbaarheden van kinderen en mensen met een beperking om hen te beïnvloeden op een manier die kan leiden tot fysieke of psychologische schade. Het Rathenau Instituut merkt op dat het recht op gelijke behandeling meer groepen benoemt en geeft in overweging om het verbod uit te breiden en gelijk te trekken met bestaande wetgeving voor gelijke behandeling.

Het kabinet meent dat ook andere groepen mensen de bescherming van dit verbod verdienen. Het verbod zou wat het kabinet betreft niet beperkt moeten blijven tot AI-systemen die gebruikmaken van de kwetsbaarheden van kinderen en mensen met een beperking om hen te beïnvloeden. Het kabinet neemt dit standpunt mee in de onderhandelingen. Verwezen wordt naar de SO-beantwoording op de BNC-fiches AI (Kamerstuk 22 112, nr. 3221), specifiek naar het antwoord op de vraag 36 van de leden van de fractie van D66.

3. Scherp het verbod op sociale scores door overheidsinstanties aan

Het verbod in artikel 5, onder c, van de conceptverordening moet voorkomen dat mensen, of groepen mensen, nadelig worden behandeld door overheden, doordat ze op basis van hun gedrag of kenmerken zouden worden geclassificeerd met «een sociale score». Het doel van de Commissie is niet om sociale scores onmogelijk maken, maar om excessen te voorkomen. Het Rathenau vraagt zich af of het verbod daar in slaagt, gezien de abstracte formuleringen en vraagt het kabinet om te verhelderen hoe excessen worden voorkomen, zowel met het oog op de mogelijke nadelige behandeling van burgers, als op het voorkomen van grootschalige privacyinbreuken in hun levens.

Het kabinet hecht eraan te benadrukken dat het geen voorstander is van een sociaalkredietsysteem naar Chinees model. Zo'n systeem verhoudt zich moeilijk tot onze grondrechten. Daarom is het kabinet blij met de inzet van de conceptverordening. Het kabinet is van mening dat vanuit het oogpunt van rechtszekerheid de in artikel 5 geformuleerde verboden voldoende nauwkeurig en specifiek moeten zijn. Deze categorie AI-systemen maken een grote inbreuk op de mensenrechten, het is daarom des te meer van belang dat helder is wat er wel of juist niet onder het verbod valt. De door de Commissie voorgestelde tekst omtrent sociale scoring acht het kabinet in beginsel voldoende nauwkeurig en toegesneden op specifieke praktijken. Verwezen wordt naar de SO-beantwoording op de BNC-fiches AI (Kamerstuk 22 112, nr. 3221), specifiek naar de beantwoording van vraag 37 en 38.

4. Verbied biometrische identificatie in de openbare ruimte – niet alleen voor opsporing

Het vierde verbod (artikel 5, onder d) van de conceptverordening gaat over real-time biometrische identificatie op afstand in openbare ruimte voor opsporingsdoeleinden. Een voorbeeld is gezichtsherkenning. De politie mag door dit verbod iemand die op straat loopt niet direct via de camerabeelden identificeren. Het verbod kent drie uitzonderingen. De politie mag de technieken wel inzetten voor het zoeken van slachtoffers van een misdaad en vermiste kinderen, ter voorkoming van een acute dreiging, zoals een terroristische aanslag, en bij het vinden en identificeren van een verdachte van een crimineel vergrijp (de zogeheten «Eurocrimes»). Het Rathenau pleit voor een verbod van biometrische identificatie in de openbare ruimte – niet alleen voor opsporing.

Het kabinet is voorstander van strenge regels en strikte voorwaarden voor de inzet van technologie – die bijvoorbeeld biometrische gegevens verwerkt – die gemakkelijk inbreuk kan maken op de persoonlijke levenssfeer. Vanwege deze inbreuk op de mensenrechten staat voor het kabinet buiten kijf dat deze technologie alleen kan worden ingezet op een wijze die in overeenstemming is met het recht. Dat houdt onder meer in dat er moet worden getoetst aan de eisen van noodzakelijkheid, proportionaliteit en subsidiariteit. Het kabinet onderstreept daarbij dat het ontbreken van een verbod van biometrische identificatie in de conceptverordening nooit kan betekenen dat biometrische identificatie juist wél is toegestaan. Dit geldt tevens voor de suggestie dat uitzonderingen op het in artikel 5, eerste lid, onder d geformuleerde verbod van deze conceptverordening ten aanzien van «real-time» gezichtsherkenning zou betekenen dat de Nederlandse politie real-time gezichtsherkenning voor deze doeleinden in mag zetten. De Europese Commissie heeft aan het kabinet bevestigd dat de in conceptverordening opgenomen bepalingen hieromtrent géén rechtsgrondslag bieden voor de inzet van biometrische

systemen. Voor de verwerking van biometrische gegevens ten behoeve van identificatie van betrokkenen gelden immers reeds kaders, zowel toeziend op de relatie tussen burgers en bedrijven onderling (in hoofdzaak de Algemene verordening gegevensbescherming (AVG)) als op de rechtshandhaving (zoals de Wet politiegegevens (Wpg) en de Wet justitiële en strafvorderlijke gegevens (Wjsg)). Aan de uit deze kaders voortvloeiende eisen moet worden voldaan alvorens biometrische gegevens kunnen worden verwerkt.

Het kabinet heeft in een eerdere brief aan uw Kamer beschreven dat de AVG weinig ruimte biedt voor de inzet van gezichtsherkenning tussen burgers en bedrijven onderling.¹ De eisen voor de verwerking van biometrische gegevens zijn in de AVG reeds streng, in hoofdzaak omdat dit zogeheten «bijzondere persoonsgegevens» zijn die vallen onder het verwerkingsverbod in artikel 9 AVG. Op dit verwerkingsverbod zijn slechts beperkte uitzonderingen mogelijk (zie hierover de bijlage bij de kabinetsreactie op het bericht in de Volkskrant). Ook voor overheidsorganisaties zijn de mogelijkheden voor de inzet van biometrische systemen beperkt. De verwerking van biometrische gegevens door een overheidsorganisatie moet berusten op een wettelijke grondslag (welke aan genoemde eisen voor het maken van een inbreuk op fundamentele rechten moet voldoen). De conceptverordening biedt de mogelijkheid de ontwikkeling en inzet van bepaalde systemen – waaronder systemen waarvoor biometrische gegevens worden verwerkt nog verder in te kaderen of aan kwaliteitseisen te verbinden. Die benadering acht het kabinet in beginsel juist. Het is van mening dat een algeheel verbod nodig noch wenselijk is.

De wijze waarop in Nederland gezichtsherkenningstechnologie wordt ingezet ten behoeve van de taakuitvoering van de Nederlandse politie vindt plaats conform daarvoor bestaande wet- en regelgeving. Voor de rechtshandhaving wordt thans gewerkt aan een nieuwe gegevenswet politie en justitie. Hierover heeft de Minister voor Rechtsbescherming uw Kamer in november 2020 geïnformeerd.² Vanzelfsprekend zal in dit traject aandacht zijn voor een duidelijk stelsel aan uitzonderingsgronden met betrekking tot de verwerking van (biometrische) persoonsgegevens door de politie en justitie.

5. Vul de lijst van hoog-risico-systemen aan

De verordening geeft ook aan welke AI-systemen een «hoog-risico» kennen, met het oog op gezondheid en veiligheid van mensen en waar grondrechten in het geding komen. In de bijlage noemt de Europese Commissie acht domeinen waarin dit het geval kan zijn: biometrische identificatie, kritieke infrastructuur, onderwijs, toegang tot werk, toegang tot essentiële private of publieke diensten en sociale zekerheid, opsporing, migratie, asiel en grenscontrole, en de rechtspraak. Het Rathenau Instituut ziet in haar onderzoeken in deze domeinen inderdaad een hoog risico op schending van mensenrechten en pleit daarnaast voor uitbreiding van de lijst.

Wanneer in de toekomst blijkt dat nieuwe manieren van de inzet van AI-systemen in de genoemde domeinen kunnen leiden tot gelijke risico's voor gezondheid, veiligheid en fundamentele rechten, of zelfs groter, dan kunnen deze worden toegevoegd aan de lijst. Het is belangrijk om te wijzen op een andere lijst die is opgenomen in de verordening, specifiek Bijlage II. Dit is een lijst van bestaande geharmoniseerde Europese wetgeving die ook raakt aan AI-systemen in bepaalde domeinen zoals

¹ Kamerstuk 34 926, nr. 11.

² Kamerstuk 32 761, nr. 173.

bijvoorbeeld de zorg en de luchtvaart. De eisen die uit de verordening gelden voor de lijst van hoog-risico AI-systemen dienen ook te worden opgenomen in de bestaande geharmoniseerde wetgeving zoals onder Annex II. Zo zullen meer AI-systemen dan die uit de lijst van hoog-risico AI-systemen in de toekomst moeten voldoen aan de vereisten uit de verordening. In artikel 7 staan de voorgestelde voorwaarden en systematiek beschreven voor aanpassingen aan bijlage III, en daarmee dus eventueel de mogelijkheid tot het aanvullen van deze lijst. De Commissie stelt voor dit per gedelegeerde handeling vast te stellen, wat een beperkte rol voor lidstaten en het Europees Parlement behelst. Het kabinet is van mening dat het van belang is om lidstaten en andere belanghebbenden een betekenisvolle rol te geven bij het aanpassen van de bijlagen van de conceptverordening en buigt zich over de beste manier om dit in te passen in de conceptverordening in consultatie met verschillende stakeholders.

Op emotieherkenningssystemen zijn weliswaar de additionele transparantieplichtingen onder artikel 52 van de conceptverordening van toepassing. De aanvullende regels voor hoog-risico systemen (ex artikel 6) van de conceptverordening gelden alleen voor emotieherkenning in de context van de rechtshandhaving, asiel, migratie en beheer van grenscontroles (zie hiervoor Annex III). Voor emotieherkenningssystemen geldt tevens dat de inzet daarvan niet in alle gevallen leidt tot een verwerking van biometrische of anderzijds bijzondere persoonsgegevens. Dit heeft onder meer als consequentie dat het verwerkingsverbod uit artikel 9 AVG niet geldt. Het kabinet is met het Rathenau instituut eens dat het nodig kan zijn dergelijke systemen ook in andere contexten – en in aanvulling op de daarvoor conform de AVG wél geldende eisen³ – aan nadere voorwaarden te verbinden, mogelijk door aanpassing van de in de conceptverordening voorziene lijst van «hoog-risico systemen».

Ten aanzien van deepfakes zal het kabinet na oplevering van het WODC onderzoek over de regulering van deepfakes dat momenteel wordt uitgevoerd door de *Tilburg University* bezien of verdere wettelijke inkadering nodig is en zo ja, of de conceptverordening daarvoor het gepaste instrument is.

6. Beoordeel de maatschappelijke opbrengst van AI-systemen

Voor de systemen met een hoog risico gelden extra eisen voor risicobeheersing (artikel 6). Het Rathenau stelt dat naast een inhoudelijke ethische beoordeling van het systeem, ook informatie noodzakelijk is over de effectiviteit van het voorgestelde AI-systeem. Doet het systeem wat het belooft? Het Rathenau Instituut merkt op dat het ook van belang om te kijken naar de maatschappelijke opbrengst van AI-systemen, juist gelet op de kans op een mensenrechtenschending door de inzet van deze systemen en suggereert een betere onderbouwing van de effectiviteit van het systeem te eisen.

Het kabinet meent dat het Rathenau Instituut hier een goed punt maakt. Het is van belang om gedurende de hele levenscyclus van een AI-systeem te blijven toetsen of deze nog voldoet aan de regels. Dit wordt geborgd door de conceptverordening. Het kabinet verwijst naar eerdere beleidsbrieven aan de Kamer waarin beschreven staat dat mensenrechten en publieke waarden het uitgangspunt voor het Nederlandse AI-beleid

³ Zoals onder meer het naleven van beginselen inzake de verwerking van persoonsgegevens uit artikel 5 AVG (de verwerking moet onder meer behoorlijk, rechtmatig en transparant zijn), het vereiste uit artikel 6 om een rechtsgrond voor de verwerking te hebben en een DPIA uit te voeren als met een verwerking grote privacyrisico's zijn gemoeid.

vormen en inzet op AI-systemen die de mens dienen, veilig zijn en vertrouwd kunnen worden, die publieke waarden borgen en waarbij een goede rechtsbescherming verzekerd is. Het kabinet heeft daartoe ook verschillende instrumenten gecreëerd om daarbij te helpen. Daarnaast vindt het kabinet het belangrijk dat als de overheid AI inzet steeds goed afweegt voor welke taak een AI-systeem wordt ingezet, niet elke taak is daarvoor immers even geschikt, en de effectiviteit van het systeem monitort. Het kabinet zal zich beraden op de suggestie van het Rathenau Instituut.

7. Transparantie is belangrijk, maar onvoldoende

Tot slot komt de conceptverordening met transparantieverplichtingen voor bepaalde type AI-systemen. Het gaat om systemen die specifieke risico's op imitatie of bedrog met zich meebrengen, zoals AI-systemen die met mensen interacteren (een chatbot), emotieherkenning, «biometrische categorisatie» en AI-systemen waarmee beeld, audio- of videocontent kan worden gemaakt of gemanipuleerd (deepfakes). Bij deze systemen moet steeds duidelijk zijn dat je met een computersysteem praat en niet tegen een mens, en dat het om beelden gaat die kunstmatig gemaakt of gemanipuleerd zijn.

Het kabinet is in beginsel positief over de aanvullende transparantieverplichtingen van artikel 52 conceptverordening. Het is met het oog op de menselijke waardigheid een goede zaak dat mensen weten dat ze interacteren met een AI-systeem. Ook is het met het oog op de specifieke gevaren hiervan belangrijk dat mensen gewaarschuwd worden voor AI-systemen die bedoeld zijn voor emotieherkenning, biometrische categorisatie en «deepfakes». Het voorstel van de Europese Commissie hanteert een aantal uitzonderingen voor de transparantieverplichtingen. Het kabinet acht het terecht dat er in het belang van de rechtshandhaving redenen zijn om transparantie richting de betrokkene afwijkend in te richten. Dat neemt echter niet weg dat ook in het kader van de rechtshandaving de inzet van AI-systemen zo transparant mogelijk dient te zijn en dat daarover, bijvoorbeeld in het kader van het strafproces, uitleg over kan worden gegeven en verantwoording over kan worden afgelegd.