

Vergaderjaar 2019–2020

26 643

Informatie- en communicatietechnologie (ICT)

32 761

Verwerking en bescherming persoonsgegevens

Nr. 682

LIJST VAN VRAGEN EN ANTWOORDEN

Vastgesteld 27 mei 2020

De vaste commissie voor Justitie en Veiligheid heeft een aantal vragen voorgelegd aan de Minister voor Rechtsbescherming over de brief van 8 oktober 2019 inzake waarborgen tegen risico's van data-analyses door de overheid (Kamerstukken 26 643 en 32 761, nr. 641).

De Minister voor Rechtsbescherming en de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties hebben deze vragen beantwoord bij brief van 20 mei 2020. Vragen en antwoorden zijn hierna afgedrukt.

De voorzitter van de commissie,
Van Meenen

Adjunct-griffier van de commissie,
Burger

1. Kunt u een lijst geven van alle ingrijpende algoritmische data-analyses van de rijksoverheid, zoals SyRi, waarvoor de richtlijnen moeten gelden?

Een lijst van alle ingrijpende algoritmische data-analyses van de rijksoverheid waarvoor de «Richtlijnen voor het toepassen van algoritmes door overheden» (hierna de richtlijnen) moeten gaan gelden is er niet. Wel is het gebruik van algoritmen binnen overheidsorganisaties eerder in kaart gebracht door het Centraal Bureau voor de Statistiek (CBS).¹ Het onderzoek richtte zich enerzijds op algoritmen die de basis vormen voor besluitvorming of anderszins impact hebben op één of meer personen en anderzijds op zogenaamde intelligente algoritmen. Dit zijn bij uitstek de algoritmen die vanwege hun impact op burgers dan wel de risico's die daaraan kleven, als «ingrijpend» kunnen worden aangemerkt. Daarnaast brengt de Algemene Rekenkamer momenteel het gebruik van algoritmes bij de overheid in kaart en toetst deze in het onderzoek «Zicht op algoritmes».² Ik kijk met belangstelling uit naar de resultaten van dat onderzoek.

Voorts, en zoals is aangekondigd in de recent aan uw Kamer toegestuurde kabinetsreactie op het onderzoeksrapport «Toezicht op het gebruik van algoritmen door de overheid», zal onderzocht worden of, en in welke gevallen, het *algoritme impact assessment* dat dit jaar wordt ontwikkeld voor algoritmen met hoge risico's, gekoppeld kan worden aan een voorafgaande raadpleging bij de toezichthouder en een publicatieverplichting daarvan. Dat overzicht is dan in feite een lijst van algoritmen met hoge risico's (oftewel ingrijpende algoritmen) die de overheid inzet³. Overigens, en zoals opgemerkt in voornoemd rapport, roept de definitie van wat een ingrijpend algoritme is veel vragen op en lijkt de term «ingrijpend» in die zin minder geschikt om als onderscheidend criterium te dienen.⁴

2. Wanneer wordt de transparantie rond data-analyses als onvoldoende beoordeeld? Bestaan er wat dit betreft verschillen tussen de verschillende overheidsorganisaties en bestaan er verschillen tussen overheidsinstanties en niet-overheidsinstanties?

Voor wat betreft data-analyses van zowel overheden als bedrijven waarin persoonsgegevens worden verwerkt, vergt het transparantievereiste uit de Algemene verordening gegevensbescherming (AVG) dat de informatie ten aanzien van betrokkenen begrijpelijk en toegankelijk is en in duidelijke en eenvoudige taal wordt verschaft.⁵ Dit betekent bijvoorbeeld dat de informatie in ieder geval duidelijkheid moet verschaffen over het doel en de wettelijke grondslag van de data-analyse. Informatie die niet aan deze (algemene) eisen voldoet, kan als onvoldoende worden beoordeeld. Uit de AVG vloeit niet voort dat deze informatie openbaar dient te worden gemaakt voor het publiek. Tegen deze achtergrond wordt in de richtlijnen voor het toepassen van algoritmen door overheden bepaald dat overheidsdiensten die data-analyses verrichten het publiek moeten informeren en waarover het publiek geïnformeerd moet worden.⁶ Voor meer informatie over deze informatieverplichtingen, verwijzen we naar de

¹ Zie «Verkennd onderzoek naar het gebruik van algoritmen binnen overheidsorganisaties», CBS, november 2018. Zie ook Brief van 31 december 2018 over onderzoek naar het gebruik van algoritmen binnen de overheid (Kamerstuk 26 643, nr. 588).

² <https://www.rekenkamer.nl/actueel/lopend-onderzoek/zicht-op-algoritmes>

³ Kamerstukken 26 643 en 32 761, nr. 680

⁴ Kamerstuk 26 643, nr. 657.

⁵ Dit beginsel wordt uitgewerkt in verschillende informatieverplichtingen. Een algemeen kader daarvoor is te vinden in artikel 12 AVG.

⁶ Zie bijlage bij de brief, p. 14.

brief van 9 oktober 2018 over transparantie van algoritmes in gebruik bij de overheid.⁷

Zie ook het antwoord op vragen 21 en 22.

De precieze mate van transparantie is daarnaast altijd gebonden aan de context waarin data-analyses plaatsvinden en het daarbij beoogde resultaat. Een overheidsinstantie die data-analyses gebruikt ten behoeve van haar dienstverlenende taak zal doorgaans meer transparantie kunnen en moeten betrachten dan een overheid die als toezichthouder of opsporingsinstantie optreedt. In die zin bestaan er verschillen tussen de verschillende overheidsorganisaties wat betreft de mate van transparantie die zij kunnen en moeten betrachten.

Voor overheidsdiensten geldt verder dat zij deze informatieverschaffing in individuele zaken achterwege kunnen laten op grond van artikel 23 AVG. Daarbij zal dan moeten worden aangetoond dat dit noodzakelijk en evenredig is ter waarborging van een algemeen belang als bedoeld in deze bepaling. Daartoe behoren onder meer de nationale en openbare veiligheid, economische en financiële belangen of de opsporing en vervolging van strafbare feiten; in die zin bestaan er op dat punt ook verschillen tussen overheidsinstanties en niet-overheidsinstanties.

Transparantie over het gebruik van data-analyses kan ook worden ingegeven door de Wet openbaarheid van bestuur (Wob) en de daarin opgenomen verplichting tot openbaarmaking van informatie over bestuurlijke aangelegenheden (artikelen 3, 8, 10 en 11) dan wel door het motiveringsbeginsel uit de Algemene wet bestuursrecht (artikel 3:46 Awb).⁸ Zie ook het antwoord op vraag 23.

Anders dan de AVG zijn deze verplichtingen uitsluitend van toepassing op de overheid en maken zij dat overheidsinstanties te dienaangaande transparanter moeten zijn dan niet-overheidsinstanties.

3. Hoe vaak komen onregelmatigheden in datasets of algoritmes voor? Wat is het gemiddelde? Bestaan er verschillen tussen de verschillende overheidsorganisaties en tussen overheid en niet-overheidsinstanties?

24. Kunt u aangeven wat op dit moment de marges op risico's en fouten zijn in datasets, algoritmen of methoden en tot welk niveau dit geminimaliseerd moet worden?

Onregelmatigheden in datasets of algoritmen kunnen altijd voorkomen. Er is ook geen eenduidig antwoord te geven op de vraag wat op dit moment de marges op fouten zijn. Om die reden is het volgens het kabinet niet zozeer relevant of er tussen overheidsinstanties verschillen bestaan wat het aantal onregelmatigheden betreft. Veel eerder gaat het om de risico's die de data-analyses en daarbij gebruikte datasets, algoritmen of methoden in zich hebben alsook om de potentiële gevolgen van de analyses voor burgers. Naarmate de risico's en de gevolgen voor de burger groter zijn, dienen de waarborgen en eisen aan de kwaliteit zwaarder te zijn. Dit geldt zeker in gevallen waarin data-analyses tot conclusies of besluiten op individueel niveau kunnen leiden. Omdat het van de context afhangt waarin algoritmen worden gebruikt en als gevolg daarvan de appreciatie van de risico's verschillend kan zijn, is het in ieder geval niet aangewezen om een uniform niveau te hanteren tot welke eventuele risico's en fouten in datasets, algoritmen of methoden

⁷ Kamerstukken 26 643 en 32 761, nr. 570.

⁸ Voor meer informatie over deze verplichtingen, zie voornoemde brief van 8 oktober 2018 over transparantie van algoritmes respectievelijk de kabinetsreactie van 2 november 2018 op het advies van de Raad van State over de effecten van digitalisering voor de rechtstatelijke verhoudingen (Kamerstuk 26 643, nr. 578).

geminimaliseerd dienen te worden.⁹ Zo zal de foutmarge in datasets over de verkeersintensiteit voor de bepaling van preventief wegonderhoud hoger zijn dan wanneer deze dataset wordt gebruikt om de aanrijtijd van ambulances te bepalen.

Hoewel de richtlijnen en de in de brief voorgestelde wettelijke waarborgen zien op de overheid, meent het kabinet dat ook voor niet-overheidsinstanties geldt dat onregelmatigheden in datasets en algoritmen altijd kunnen voorkomen en dat ook deze instanties algoritmen gebruiken die tot conclusies of beslissingen op individueel niveau kunnen leiden. Een voorbeeld hiervan betreft het gebruik van algoritmen voor beslissingen inzake kredietverstrekking. Zie ook het antwoord op vragen 17 en 19.

4. Op welke punten voorziet de Algemene verordening gegevensbescherming (AVG) op dit moment in wettelijke waarborgen op het gebruik van algoritmen?

Voor algoritmen die gebruik maken van persoonsgegevens geldt dat er sprake is van gegevensverwerking in de zin van de AVG. In dat geval moet er aan de voorwaarden uit de AVG worden voldaan.

Ongeacht of er gebruik wordt gemaakt van algoritmen moet bij elke verwerking van persoonsgegevens aan enkele basisvoorwaarden zijn voldaan, zoals het vereiste dat er voor de verwerking een grondslag moet zijn (artikel 6 AVG). Bij algoritmegebruik door de overheid zal de grondslag vaak gelegen zijn in het naleven van een wettelijke verplichting of de uitoefening van een taak van algemeen belang (artikel 6, eerste lid, sub c respectievelijk e, AVG). Daarnaast moeten de beginselen genoemd in artikel 5 AVG, zoals de beginselen van doelbinding, dataminimalisatie en behoorlijkheid en rechtmatigheid van de verwerking, in acht worden genomen. Uit deze beginselen vloeit bijvoorbeeld voort dat een verwerking van gegevens niet mag leiden tot discriminatie. Verder behoeven verwerkingen die waarschijnlijk een hoog risico inhouden voor de rechten en vrijheden van natuurlijke personen een zogenaamde *Data Protection Impact Assessment* (artikel 35 AVG), waarmee ook voldaan wordt aan de verplichting om bij het ontwerpen van algoritmen rekening te houden met de beginselen van gegevensbescherming (artikel 25).¹⁰ Bij gebruik van algoritmische systemen zal vaak sprake zijn van een hoog risico.¹¹ Voorts stelt de AVG extra eisen aan de situatie wanneer er sprake is van uitsluitend geautomatiseerde besluitvorming, dat wil zeggen besluitvorming zonder menselijke tussenkomst (artikel 22), en verbiedt zij in principe de verwerking van bijzondere persoonsgegevens en strafrechtelijke persoonsgegevens (artikel 9). Ook gelden er normen rond de opslag en beveiliging van de persoonsgegevens en bevat de AVG diverse bepalingen over de informatievoorziening aan degenen van wie de persoonsgegevens worden verwerkt. Over deze laatste verplichting, zie ook het antwoord op vraag 2 en vraag 21.

5. Is het onderdeel van een taak van de Autoriteit Persoonsgegevens (AP) toe te zien op algoritmegebruik en persoonsgegevens?

⁹ Zie voor eenzelfde uitgangspunt de kabinetsreactie op het Rapport van de Wetenschappelijke Raad voor het Regeringsbeleid «Big Data in een vrije en veilige samenleving», Kamerstukken 26 643 en 32 761, nr. 426, p. 8.

¹⁰ Zie hierover Model gegevensbeschermingseffectbeoordeling rijksdienst (PIA), p.9. http://content.rp.rijksweb.nl/cis/content/media/rijksportaal/kernprocessen_1/rjp/privacy_5/model-gegevensbeschermingseffectbeoordeling-rijksdienst-pia.pdf

¹¹ Zie hierover «Toezicht op algoritmen & AI», Autoriteit Persoonsgegevens, 17 februari 2020, p. 7. https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/toezicht_op_ai_en_algoritmes.pdf

34. In hoeverre voldoet de AP aan een algoritmetoezichthouder?

Als er voor een algoritme persoonsgegevens worden gebruikt, dan valt dit algoritme onder het toezicht van de AP. Zoals in de kabinetsreactie op het onderzoeksrapport «Toezicht op gebruik van algoritmen door overheden» is aangegeven heeft de AP een belangrijke rol als het gaat om het toezicht op gebruik van persoonsgegevens in algoritmen van (onder meer) de overheid.¹² De AP pakt deze rol ook al. Zo heeft de AP recent een publicatie uitgebracht over het huidige en toekomstige toezicht door de AP op het gebruik van algoritmen waarin persoonsgegevens worden verwerkt.¹³ Blijkens het meerjarig visiedocument «Focus AP 2020- 2023: «Dataprotectie in een digitale samenleving» zijn algoritmes en artificiële intelligentie één van de drie focusgebieden waar de AP de komende jaren in haar toezichtwerk extra nadruk zal leggen.¹⁴

Naast de AP hebben ook andere toezichthoudende organisaties een rol bij het toezicht op het gebruik van algoritmen door de overheid, zoals de Rijksinspecties, de Algemene Rekenkamer of de Auditdienst Rijk.¹⁵ Voor een effectieve invulling van de toezichtfunctie is het van belang dat het toezicht door deze organisaties een structureel karakter krijgt en dat deze organisaties actiever met elkaar samenwerken en kennisdelen. Zie over de acties die het kabinet ten aanzien hiervan onderneemt, bovengenoemde kabinetsreactie.

6. Waarom wordt gekozen voor richtlijnen in plaats van doelwetgeving?

Zoals in de brief aangegeven gaat het om materie die relatief nieuw is en voortdurend in ontwikkeling is. Om die reden kiest het kabinet voor een lerende aanpak waarbij in eerste instantie richtlijnen worden ontwikkeld waarmee geëxperimenteerd kan worden en die flexibel kunnen worden aangepast aan de technologische ontwikkelingen en de ervaringen die ermee worden opgedaan. Met deze ervaringen kan vervolgens rekening worden gehouden bij het ontwikkelen van mogelijke wettelijke waarborgen. Beter dan doelwetgeving maakt de keuze voor richtlijnen het mogelijk om bij het ontwikkelen van (wettelijke) normen een lerende aanpak te volgen.

Doelwetgeving kan daarnaast het nadeel hebben dat het veelal open normen zal bevatten, terwijl er vanuit de praktijk juist behoefte bestaat aan concrete en hanteerbare normen: vanuit oogpunt van rechtszekerheid en uniformiteit verdient doelwetgeving in dit geval daarom niet de voorkeur.

7. Hoe ziet u de verhouding toezicht en regels vooraf versus toezicht en regels die gericht zijn op de resultaten van data-analyse achteraf?

Beide vormen van controle en soorten regels zijn van belang voor een verantwoorde inzet van algoritmen en rechtmatig gebruik van data-analyses. Het kabinet zet in op beide aspecten.

¹² Bijlage 2 bij Kabinetsbrief van 20 april 2020 over de Initiatiefnota «menselijke grip op algoritmen» en het onderzoek «Toezicht op gebruik van algoritmen door de overheid», Kamerstuk 35 212, nr. 3.

¹³ Zie voetnoten 3 en 4.

¹⁴ Zie Focus AP 2020- 2023: «Dataprotectie in een digitale samenleving», https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/focus_ap_202-2023_groot.pdf

¹⁵ Zie voor een overzicht van de toezichthouders, Bijlage 3 bij Kabinetsbrief van 20 april 2020 over de Initiatiefnota «menselijke grip op algoritmen» en het onderzoek «Toezicht op gebruik van algoritmen door de overheid», Kamerstuk 35 212, nr. 3.

Regels vooraf zijn er primair op gericht de risico's op fouten en onregelmatigheden in data-analyses te minimaliseren. Hierbij kan met name worden gedacht aan maatregelen die de kwaliteit en deugdelijkheid van data-analyses verbeteren, zoals regels inzake validatie, trainingsdata, en andere regels gericht op het voorkomen, corrigeren of compenseren van fouten in datasets of modellen. Daarnaast zijn «regels vooraf» ook nodig om controle en toezicht achteraf mogelijk te maken. Voorbeelden hiervan zijn regels inzake documentatie, audits en auditeerbaarheid, uitlegbaarheid of toetsbaarheid. De richtlijnen, het te ontwikkelen algoritme impact assessment en op termijn mogelijke wettelijke waarborgen, bevatten dergelijke normen waarvoor, dit wil zeggen bij de ontwikkeling van algoritmen, aan getoetst moet worden.

Adequate controle en toezicht (achteraf) op het gebruik en de uitkomsten van algoritmen is essentieel voor de rechtsbescherming en gegrond publiek vertrouwen in het gebruik van data-analyses door de overheid. Hierover alsook over de acties die het kabinet hiertoe onderneemt is uw kamer bij brief van 20 april jongstleden geïnformeerd.¹⁶

Eenzelfde benadering wordt gevolgd door de Europese Commissie in het op 19 februari jongstleden gepubliceerde «*White paper on Artificial Intelligence: a European approach to excellence and trust*» (hierna: witboek AI).¹⁷ In haar voorstellen voor een regelgevend kader voor AI benadrukt de CIE zowel het belang van heldere normen en van een ex ante toetsing daaraan als van naleving en toezicht. Deze benadering heeft in beginsel de steun van het kabinet. Zie op dit punt, de Kabinetsappreciatie Witboek over kunstmatige intelligentie dat op 20 april 2020 aan uw Kamer is aangeboden.¹⁸

8. Waarom wordt de scheiding gemaakt tussen gebruik van data-analyse in het openbaar bestuur en in bedrijven?

9. Waarom is niet gekozen voor een systeem zoals bij het toezicht op het gebruik van persoonsgegevens door de AP waarin wetgeving en toezicht voor overheden en niet-overheden niet gescheiden is?

10. Waarom zouden wettelijke waarborgen voor een grensoverschrijdende activiteit moeten verschillen van wettelijke waarborgen voor een niet grensoverschrijdende activiteit als het gaat om data-analyse?

Volgens het kabinet ligt het niet voor de hand om op nationaal niveau aanvullende normen voor data-analyses te stellen voor het bedrijfsleven. Het feit dat bedrijven veelal grensoverschrijdend actief zijn betekent dat bedrijven die (mede) in Nederland algoritmen aanbieden, aan extra regels in Nederland onderhevig zouden zijn. Dit is niet alleen ineffectief, ook kan het in strijd zijn met het principe van vrij verkeer van persoonsgegevens dat een van de doelstellingen is van de AVG. Om dezelfde reden is in voormelde kabinetsreactie op het onderzoek «Toezicht op gebruik van algoritmen door de overheid» erop gewezen dat de instelling van een nieuwe algoritmetoezichthouder – wanneer die zou worden belast met het toezicht op het bedrijfsleven – tegenstrijdigheid kan opleveren met het vrij verkeer van gegevens. Bedrijven zouden, naast de AP, onderworpen zijn aan een extra toezichthouder in Nederland, hetgeen een (indirecte) belemmering op dit principe kan vormen.

¹⁶ Kabinetsbrief van 20 april 2020 over de Initiatiefnota «menselijke grip op algoritmen» en het onderzoek «Toezicht op gebruik van algoritmen door de overheid», Kamerstuk 35 212, nr. 3.

¹⁷ Witboek AI, Brussel, 19.2.2020 COM(2020) 65 final. https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

¹⁸ Kamerstukken 26 643 en 32 761, nr. 680

Volgens het kabinet kunnen verdere regels voor data-analyses door bedrijven en/of aanvullende toezichtmechanismen voor het bedrijfsleven beter in Europees verband worden vastgesteld. Voordeel van Europese regels is voorts dat fragmentatie tussen de lidstaten wordt voorkomen en een gelijk speelveld gestimuleerd wordt. Zoals blijkt uit de voorstellen in het witboek AI wordt in Europees verband momenteel ook nagedacht over verdere normen alsook over *governance* en toezichtstructuren en -mechanismen, die ook zullen gelden voor het bedrijfsleven.¹⁹

Voor de overheid is er wel ruimte om het normenkader voor algoritmen reeds aan te vullen. Dit gebeurt met de richtlijnen voor data-analyse die alleen voor overheden gelden. De ervaring die op dit moment wordt opgedaan met de normen voor de overheid zal worden benut bij de standpuntbepaling van Nederland in Europees verband. Er zij hierbij nog opgemerkt dat de in het Witboek AI voorgestelde vereisten waar AI-toepassingen aan zouden moeten voldoen, grotendeels overeenkomen met de waarborgen in de richtlijnen. Zie op dit punt ook vraag 17.

11. Hoe verhoudt het recht op eigendom zich tot het recht op gelijke behandeling, en het recht om deze gelijke behandeling af te dwingen?

Het recht op eigendom en het recht op gelijke behandeling zijn beide grondrechten. Het recht op gelijke behandeling is een groot goed. De essentie van het grondrecht is, dat gelijke gevallen gelijk moeten worden behandeld en dat ongelijke behandeling gerechtvaardigd moet zijn. Het eigendomsrecht is niet alleen van fundamenteel belang voor het goed functioneren van de economie maar beschermt ook de belangen van particulieren. Grondrechten kunnen elkaar versterken. In een voorkomend geval kunnen grondrechten echter ook botsen. De vraag welk grondrecht in een concreet geval prevaleert is lastig te beantwoorden. Er is geen sprake van een algemene voorrang van het ene boven het andere grondrecht. Botsingen van grondrechten zijn niet specifiek geregeld in wetgeving. Het is veelal aan de rechter om, in het licht van de concrete omstandigheden van het individuele geval, tot een oordeel te komen. De uitkomst van de belangenafweging laat zich moeilijk voorspellen.

12. Welke kosten moeten worden gemaakt voor het ontwikkelen van waarborgen bij de verdere ontwikkeling en toepassing van data-analyses gebaseerd op algoritmes? En voor wie zijn deze kosten?

De richtlijnen helpen overheidsorganisaties bij het verantwoord inzetten van data-analyses gebaseerd op algoritmen. Voordat deze richtlijnen beschikbaar waren, maakten partijen reeds kosten om data-analyses zorgvuldig in te zetten. Afhankelijk van de nadere concretisering van de richtlijnen, brengt implementatie hiervan mogelijk extra kosten voor overheidsorganisaties met zich mee. In het kader van het evaluatietraject dat momenteel ten aanzien van de richtlijnen loopt, wordt ook een kosten-baten analyse uitgevoerd waarbij de extra kosten en baten voor zover mogelijk in beeld zullen worden gebracht. Daarnaast voert de VNG een impactanalyse uit, waarin eveneens ingegaan wordt op de extra kosten die de richtlijnen voor gemeenten met zich meebrengen.

13. Voor wanneer zijn de richtlijnen nader uitgewerkt?

¹⁹ Zie hierover het door de Europese Commissie op 19 februari 2020 gepubliceerde Witboek AI. https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

Op dit moment worden de richtlijnen op hun effectiviteit en uitvoerbaarheid getoetst. Op basis van de uitkomsten van deze toetsing zullen de richtlijnen waar nodig worden aangepast of aangescherpt.²⁰ Een nadere uitwerking van de richtlijnen verwachten we begin 2021 aan uw Kamer te kunnen aanbieden.

14. Wat gebeurt er met ingrijpende algoritmes die nu werkzaam zijn zonder toetsen aan de richtlijnen?

15. Wanneer treden de richtlijnen in werking?

Zoals gezegd waren overheidsorganisaties, ook voordat de richtlijnen beschikbaar kwamen, gehouden om data-analyses zorgvuldig en rechtmatig in te zetten. Voor ingrijpende algoritmen geldt te meer dat het inzetten daarvan zorgvuldig en met inachtneming van reeds bestaande normen (bijvoorbeeld uit de AVG) dient te gebeuren.

De richtlijnen zijn nu al beschikbaar voor toepassing door overheidsorganisaties. De richtlijnen hebben geen dwingend karakter. Wel is het uiteraard wenselijk om deze te volgen, bijvoorbeeld in het kader van een P&C-cyclus. Dit geldt in eerste instantie voor algoritmen die nieuw worden ontwikkeld, maar ook voor algoritmen die reeds werkzaam zijn. Vanaf het moment dat de aangepaste richtlijnen begin 2021 aan uw Kamer zijn aangeboden zal het gebruik daarvan actief worden aangemoedigd, vanuit het beginsel «comply or explain».

16. Voor welke overheden en overheidsorganisaties zullen de richtlijnen gaan gelden?

De richtlijnen gelden voor alle overheden, zowel centrale als decentrale, en voor alle overheidsorganisaties die voor de uitoefening van hun taken, gebruik maken van algoritmische data-analyses.

17. Wordt met het voornemen van het kabinet om naast voornoemde richtlijnen toe te werken naar waarborgen in wetgeving nieuwe wetgeving bedoeld of wordt dit betrokken bij bestaande wetgeving?

Welke wetgeving betreft dit indien dit betrokken wordt bij bestaande wetgeving? Binnen welk tijdspad kan dit worden verwacht?

19. Op welke termijn kunnen de besproken wettelijke waarborgen naar verwachting worden verwacht.

Op basis van de evaluatie, waaronder de kosten-batenanalyse, en ervaring die met de richtlijnen is opgedaan zal worden bezien of het wenselijk en noodzakelijk is onderdelen van de richtlijnen wettelijk verplicht te stellen. Daarbij kan worden gedacht aan waarborgen die voldoende uitgekristalliseerd zijn om in wetgeving te worden opgenomen en bovendien dusdanig generiek zijn dat zij een plek zouden kunnen krijgen in eveneens generieke wetgeving, zoals de Uitvoeringswet AVG (UAVG), de Algemene wet bestuursrecht (Awb) of eventueel een afzonderlijke wet.²¹ Een concrete termijn daarvoor is nog niet te geven.

Voor deze beslissing zijn tevens relevant de wetgevingsvoorstellen die de Europese Commissie, in vervolg op het Witboek AI, zal uitbrengen. Immers, deze voorstellen die later dit jaar worden verwacht zullen op termijn hun weerslag hebben op nationaal niveau. Afhankelijk van de

²⁰ Zie op dit punt ook Bijlage 2, p. 4–5, bij Kabinetsbrief van 20 april 2020 over de Initiatiefnota «menselijke grip op algoritmen» en het onderzoek «Toezicht op gebruik van algoritmen door de overheid», Kamerstuk 35 212, nr. 3

²¹ Zoals in de brief uiteengezet zouden de wettelijke waarborgen van toepassing zijn op twee typen data-analyses, te weten profilering en gebiedsgebonden analyses.

inhoud daarvan zal worden bepaald of en welke aanvullende nationale wettelijke normen nog nodig zijn, en welk wetgevingstraject daarvoor nodig is.²²

Hieronder wordt een aantal relevante punten met betrekking tot de voorstellen van de Commissie in het witboek AI aangehaald, die voor Nederland en het verdere wettelijke traject op dit terrein van belang zijn.

Zoals in de «Kabinetsappreciatie Witboek over kunstmatige intelligentie» is benadrukt, acht Nederland het van belang dat nieuwe Europese normen zo mogelijk aansluiten bij, en niet afdoen aan reeds bestaande wettelijke kaders, zoals de AVG en de Richtlijn gegevensbescherming opsporing en vervolging.²³ Vooral nog lijkt dit ook de inzet van de Europese Commissie.

Ook staat Nederland positief ten aanzien van nieuwe aanvullende regels die, beter dan de nu bestaande regels, toegespitst zijn op de specifieke kenmerken en bijbehorende risico's van AI-toepassingen. Ook dit punt lijkt vooral nog in overeenstemming met de intentie van de Commissie om normen te ontwikkelen die erop gericht zijn de specifieke risico's van AI-toepassingen te beperken.

Verder zijn, net als de richtlijnen, de voorgestelde vereisten waar AI-toepassingen aan zouden moeten voldoen, erop gericht de transparantie, de kwaliteit en betrouwbaarheid van algoritmen/AI te vergroten, en vormen zij in die zin goede vertrekpunten voor Nederland. Voor meer informatie, zie voornoemde «Kabinetsappreciatie Witboek over kunstmatige intelligentie».²⁴

18. Wat wordt bedoeld met auditeerbaarheid? Gaat het dan ook om de risicomangementprocessen bij overheids- en niet overheidsinstellingen? Waarom wordt gesproken over een keuze tussen interne en externe controle? Kan dat niet allebei plaatsvinden?

Met auditeerbaarheid wordt bedoeld dat gebruikte modellen, algoritmen, data en beslissingen moeten worden gedocumenteerd en vastgelegd, zodat ze (achteraf) geverifieerd kunnen worden. Daarbij hoort dat bepaalde keuzes, (zoals de keuze voor specifieke algoritmen of type data) en waarnemingen (zoals geconstateerde afwijkingen in de gegevens of onverwachte resultaten) worden onderbouwd en vastgelegd. In overeenstemming hiermee wordt in voormelde kabinetsreactie op het onderzoek «Toezicht op gebruik van algoritmen door de overheid» opgemerkt dat welke algoritmen aan een audit moeten worden onderworpen onder andere afhankelijk is van hoe deze worden ingezet, met welk doel het algoritme wordt ingezet en welke gevolgen dit heeft voor een individu of groep. Ook is de begrijpelijkheid en uitlegbaarheid van een ingezet algoritme essentieel om daarover verantwoording te kunnen afleggen, zonder dat een audit altijd noodzakelijk is.

Audits kunnen interne audits zijn die binnen de eigen organisatie plaatsvinden dan wel externe audits zijn, uitgevoerd door een externe, onafhankelijke partij. Als het gaat om de overheid kunnen de Auditdienst Rijk (ADR) en de Algemene Rekenkamer (ARK) bovendien gevraagd en ongevraagd onderzoeken en audits uitvoeren naar de taakuitoefening van de overheid en het gebruik daarbij van algoritmen. Dit betreft (onafhankelijke) interne en externe controle op de overheid.

²² Wanneer het Europese regelgevend instrument daarvoor ruimte biedt, is bijvoorbeeld een optie dat er in de nationale implementatie- of uitvoeringswetgeving gekozen wordt voor nationale normen die verder strekken dan de Europese normen.

²³ <http://data.europa.eu/eli/dir/2016/680/oj>

²⁴ Kamerstukken 26 643 en 32 761, nr. 680

Het kabinet acht het uitvoeren van audits op algoritmen van belang. Voor effectieve audits is nodig dat er een helder normenkader beschikbaar is. De nadere concretisering van de richtlijnen dient daarin te voorzien. Voor de vraag of audits intern en/of extern moeten plaatsvinden is het type algoritme en de impact daarvan op individuen relevant. In het verlengde hiervan is in voornoemde Kabinetsreactie aangegeven dat de Ministeries van JenV en BZK dit jaar, samen met medeoverheden en uitvoeringsorganisaties, zullen verkennen of en onder welke voorwaarden, een eventuele vorm van rapportage wenselijk is. Daarnaast zal met de Auditdienst Rijk worden verkend welke rol zij kan spelen bij het op structurele basis uitvoeren van audits op het algoritmegebruik door de rijksoverheid.

20. Hoe gaan de wettelijke waarborgen waarover voor publieke instellingen gesproken wordt, verschillen van de waarborgen voor niet-publieke instellingen met betrekking tot aangekochte algoritmes?

25. Hoe vaak komt het voor dat derde partijen zijn betrokken bij het gebruik van algoritmes en hoe is deze inzet van derde partijen verdeeld over de ministeries en organisaties?

30. Wat is een voorbeeld van een contractuele maatregel zoals hier genoemd? Zou er een wettelijke verplichting moeten komen om dit soort contractuele maatregelen op te nemen? Wie is verantwoordelijk als het algoritme verstrekt door een derde niet inzichtelijk is?

Waarborgen voor overheidsorganisaties met betrekking tot aangekochte algoritmen moeten contractueel worden geregeld, via de inkoopvoorwaarden van de overheid. Er wordt thans ook onderzocht of de inkoopvoorwaarden kunnen worden aangepast om de inkoop van uitsluitend transparante algoritmen te bevorderen. Hierin zal ook worden bezien of het openbaar beschikbaar stellen van de broncode als een mogelijke inkoopvoorwaarde kan worden gezien. Dit betreft een voorbeeld van een contractuele maatregel die op dit punt zou kunnen worden genomen.

Wanneer op het punt van inzichtelijkheid niets is geregeld, komt het gebrek aan transparantie van een algoritme dat bij een derde is ingekocht, voor rekening van de desbetreffende overheidsorganisatie. Zoals aangegeven, wordt thans verkend hoe de inkoopvoorwaarden kunnen worden aangepast om dit soort situaties te voorkomen. Het is op dit moment niet bekend hoe vaak derde partijen betrokken zijn bij het gebruik van algoritmen en hoe deze inzet is verdeeld over de overheidsorganisaties.

21. Welke andere vormen van informatieverspreiding van overheidsorganen richting individuele betrokkenen ziet u nog meer?

Naast de in de brief en in de richtlijnen voorgestane informatieverstrekking aan het publiek, gelden uiteraard de bestaande verplichtingen op grond van de artikelen 13 en 14 AVG om individuele betrokkenen van wie persoonsgegevens worden verwerkt, daarover te informeren. Dat geldt ook voor verwerkingen daarvan ten behoeve van profilering, gebiedsgebonden analyses dan wel andere vormen van data-analyses. Zie in het bijzonder artikel 13, eerste lid, onder f, en 14, tweede lid, onder g.²⁵

22. Met welke motivatie kiest de overheid voor een privacyverklaring op de website van overheidsorganen als informatie aan het publiek?

²⁵ Zie voor meer informatie over deze verplichtingen, kamerbrief van 9 oktober 2018 over transparantie van algoritmes in gebruik bij de overheid, Kamerstukken 26 643 en 32 761, nr. 570.

Wanneer het publiek wil weten of een bepaalde overheidsorganisatie vormen van data-analyses, aan de hand van persoonsgegevens, uitvoert en daarover meer informatie wil hebben, ligt het voor de hand te veronderstellen dat het daarvoor de website van de desbetreffende organisatie bezoekt. Gelet op het doel van een privacyverklaring, ligt het dan tevens voor de hand om dergelijke informatie daarin op te nemen. Opneming daarvan op de website is daarnaast een wijze van informatie-verstrekking die voor de desbetreffende overheidsorganisatie relatief weinig uitvoeringslasten meebrengt.

23. Hoe kan een betrokkene een verzoek indienen voor een verdergaande mate van detaillering in de informatie? Wie is hierbij betrokken en hoe verhoudt dit zich tot de huidige mogelijkheden?

Eenieder kan voor meer specifieke informatie over de eventuele verwerking in een algoritme van zijn persoonsgegevens terecht bij de overheidsorganisatie die dit algoritme toepast. Die organisatie kan betrokkene informeren over het daarin al dan niet verwerken van hem betreffende persoonsgegevens. Wanneer dat laatste het geval is, kan betrokkene vragen om informatie te verkrijgen over onder meer het doel van de verwerkingen, de betrokken categorieën van persoonsgegevens en, als daarvan sprake is, het bestaan van geautomatiseerde besluitvorming, met inbegrip van eventuele profilering. Betrokkene heeft recht op deze informatie op grond van artikel 15 AVG.

Volledigheidshalve wordt hier nog opgemerkt dat ook de Wob in deze relevant kan zijn. Ingevolge artikel 3 Wob kan eenieder om openbaarmaking van onder de overheid berustende informatie over bestuurlijke aangelegenheden vragen. Daaronder kan ook informatie worden begrepen over het gebruik van algoritmes die (persoons)gegevens verwerken. Wel kan openbaarmaking achterwege blijven als sprake is van een of meer in die wet genoemde weigeringsgronden (artikelen 10 en 11).²⁶

26. Welke invloed hebben keuzes over wie, waar en welke, op de mogelijke vooringenomenheid (bias) in een dataset ten aanzien van wijken en groepen in de samenleving, gelet op het feit dat het kabinet het risico op fouten en onjuistheden in de gebruikte datasets, algoritmes of methodes en de mogelijke discriminerende effecten die daaruit kunnen volgen, wil minimaliseren? Hoe wordt de controle hierop vormgegeven?

Keuzes van databronnen, datasets of classificatie van data kunnen gevolgen hebben voor de resultaten van data-analyses. Wanneer bijvoorbeeld een algoritme voor werving van medewerkers zou worden getraind met een dataset waarin (aanzienlijk) meer mannen promotie hebben gekregen, kan dit er bijvoorbeeld toe leiden dat het algoritme de kansen op geschiktheid bij vrouwen lager inschat. Daarnaast kennen AI-systemen die classificeren per definitie een foutmarge. Dit komt omdat deze systemen constatering voor groepen toepassen op het individu. Er zijn daardoor altijd gevallen die volgens het model onder een bepaalde categorie vallen, maar in werkelijkheid daar niet onder passen. Hierdoor kunnen mensen verkeerd worden ingedeeld; classificaties op basis van postcodegebieden kunnen er bijvoorbeeld toe leiden dat mensen verkeerd worden ingedeeld en onterecht als kredietwaardig (*false positive*) of onterecht níét als kredietwaardig (*false negative*) worden aangemerkt.

²⁶ Openbaarmaking van informatie kan bijvoorbeeld achterwege blijven, voor zover dit de veiligheid van de Staat zou kunnen schaden. Andere gronden voor weigering zijn onder meer gelegen in het belang van de opsporing en vervolging van strafbare feiten en het belang van inspectie, controle en toezicht doorbestuursorganen.

Classificaties naar groepen of geografische gebieden kunnen daarbij ook discriminerende of stigmatiserende effecten hebben.

Dit is reden voor het kabinet om in te zetten op (kwaliteits)maatregelen waarmee de risico's op dergelijke bias beperkt worden. De richtlijnen bevatten diverse regels die op dit punt relevant zijn. Zo vragen de richtlijnen aandacht voor de mogelijke bias en discriminerende of stigmatiserende factoren en schrijven zij voor dat onderzoek naar de kwaliteit van databronnen en de beperkingen daarvan noodzakelijk is, zoals bijvoorbeeld de (on)geschiktheid van databronnen voor een bepaalde type data-analyse. Daarbij moet onder meer worden beschreven hoe omgegaan wordt met bias en fouten in de datasets en uitkomsten. Ook moeten er controlemechanismen worden opgebouwd die toetsen of er geen sprake is van discriminatie of stigmatisering. Ook de regels inzake validatie en gegevensherkenning strekken er toe het risico op fouten en onjuistheden, waaronder discriminerende effecten, te beperken. Daarbij wordt specifiek aandacht gevraagd voor de keuze van (trainings)gegevens, de gevolgen van bepaalde keuzes voor de uitkomsten van data-analyses en een verkenning van potentiële discriminerende factoren.²⁷

De wijze van controle hangt af van een aantal omstandigheden. Zo zullen altijd de eigen, interne controlemechanismen van de betreffende organisatie van toepassing zijn, zoals de controle door de eigen functionaris gegevensbescherming op de verwerking van persoonsgegevens. Daarnaast, en zoals uiteengezet onder vraag 7, bevatten de richtlijnen ook regels die controles achteraf, van bijvoorbeeld de keuzes die zijn gemaakt, mogelijk maken zoals de regels inzake documentatie, auditeerbaarheid, uitlegbaarheid of toetsbaarheid. Indien er persoonsgegevens worden verwerkt, is bovendien toezicht achteraf door de AP van toepassing.

27. Wat voor soort standaarden moeten er gelden voor algoritmen, het analyseren van datasets en de gevonden statistische correlaties in termen van kwaliteit, zorgvuldigheid en herhaalbaarheid?

Er worden door verscheidene nationale en internationale organisaties standaarden ontwikkeld voor het gebruiken en ontwikkelen van algoritmen. In bovengenoemde kabinetsreactie van 20 april jongstleden over de Initiatiefnota «Menselijke grip op algoritmen» is een overzicht gegeven van de verschillende standaarden die thans in ontwikkeling zijn. Deze bevatten onder andere kaders en eisen voor betrouwbare en ethische AI-toepassingen. Voor meer informatie hierover, verwijs ik naar voornoemde kabinetsbrief en bijlage 1 bij deze brief.²⁸

28. Is het doel alle data-gedreven processen transparant en controleerbaar te maken en alle data-inzet aan toezicht te onderwerpen?

Hoewel de data-gedreven processen zoveel mogelijk transparant en controleerbaar moeten zijn, is gelet op de enorme hoeveelheid aan data-processen, een differentiatie noodzakelijk om de uitvoeringslast voor overheidsorganisaties beheersbaar te houden. Vandaar de focus op risicovolle data-analyses als profilering en gebiedsgebonden analyses

²⁷ Zie voor andere initiatieven op dit punt: Kabinetsbrief van 20 april 2020 over de Initiatiefnota «menselijke grip op algoritmen» en het onderzoek «Toezicht op gebruik van algoritmen door de overheid», p.4 en bijlage 1 bij deze brief.

Zie ook brief van de Minister van Binnenlandse Zaken en Koninkrijksrelaties over «AI, publieke waarden en mensenrechten», Kamerstukken 26 643 en 32 761, nr. 642.

²⁸ Kamerstuk 35 212, nr. 3.

(wettelijke waarborgen) respectievelijk data-analyses met een aanmerkelijke impact op burgers (richtlijnen).

29. Kunt u omschrijven hoe u gaat vaststellen of algoritmes en analysemethoden op wetenschappelijk verantwoorde wijze zijn ontwikkeld?

Dat is aan de organisaties zelf om te organiseren. Dat kan bijvoorbeeld door methoden wetenschappelijk te laten valideren. Bepaalde analysemethoden zoals lineaire regressie en logistische regressie worden geaccepteerd als valide (wetenschappelijk verantwoorde) methoden om toe te passen.

Ook kunnen organisaties nieuwe analysemethoden (laten) ontwikkelen. Daarbij zal de afweging moeten worden gemaakt of deze voldoende uitlegbaar, toetsbaar en valideerbaar zijn om te worden toegepast, zodat sprake is van een methode die op wetenschappelijk verantwoorde wijze is ontwikkeld dan wel wetenschappelijk is gevalideerd.

31. Welke kosten zijn betrokken bij de validatie en audits van de resultaten van data-analyses en hoe zijn deze kosten opgebouwd?

33. Gaat het alleen om audits van resultaten of ook van systemen en processen?

Daar is geen precies antwoord op te geven. Deze kosten zijn namelijk sterk afhankelijk van het type data-analyse en de complexiteit daarvan die bepalend zijn voor de omvang van de validatie en audit traject en de kosten daarvan. In voormelde kosten-batenanalyse zal specifiek aandacht worden besteed aan de opbouw van de kosten.

De richtlijnen richten zich niet enkel op de technische waarborgen maar ook op de processen daaromheen. Ook de audits zullen daar betrekking op hebben.

32. Wie zal verantwoordelijk zijn voor de validatie en audits van resultaten van data-analyses?

Overheidsorganisaties die data-analyses gebruiken zijn zelf verantwoordelijk voor een rechtmatige en verantwoorde inzet daarvan. Daaronder valt ook de verantwoordelijkheid voor het treffen van de maatregelen die daarvoor nodig zijn, zoals validatie en audits.

Bij data-analyses waarbij persoonsgegevens worden gebruikt, zal deze verantwoordelijkheid samenvallen met de verantwoordelijkheid van de verwerkingsverantwoordelijke in de zin van de AVG.