

35 212

Initiatiefnota van het lid Middendorp: Menselijke grip op algoritmen

Nr. 2

INITIATIEFNOTA

1. Menselijke Grip op Algoritmen

1.1. Aanleiding

Data-analyse, kunstmatige intelligentie en de algoritmen die deze twee aansturen maken ons leven mooier, makkelijker en vrijer. We moeten daarom in Nederland de grote mogelijkheden die algoritmen bieden, benutten. Het gebruik van algoritmen kan echter ook een keerzijde hebben omdat zij ook gebruikt kunnen worden om mensen emotioneel of financieel te benadelen of te sturen. Vaak zonder dat zij dat zelf door hebben. We moeten innovatie de ruimte geven, maar mensen niet, in een digitale jungle overlaten aan de sturing van algoritmen. Ook in een digitale toekomst, waarin we de enorme kansen pakken die algoritmen bieden moeten mensen online veilig zijn en in vrijheid zelf keuzes kunnen blijven maken.

Algoritmen zijn in computertaal voor-in-gegeven instructies die autonoom of met menselijke betrokkenheid geautomatiseerd beslissingen nemen. Dat doen algoritmen door (1) met (persoons)gegevens in (2) een digitaal systeem tot (3) beslissingen of maatregelen te komen die (4) impact hebben op mensen. Denk aan het koken van boerenkoolstampot waarbij de aardappelen en boerenkool (input) in voorgeschreven volgorde volgens een recept (algoritme) gemengd worden. Het resultaat is boerenkoolstampot (output) die mensen beter kunnen verteren dan de ingrediënten zelf (impact).

Algoritmen worden dus door mensen gemaakt maar nemen daarna automatisch in de digitale wereld beslissingen over kleine en grote zaken in ons leven. Zij zijn de technologische motor van de vooruitgang en worden inmiddels op miljoenen plekken in onze samenleving gebruikt. De grote meerderheid van alle algoritmen helpt onze samenleving mooier maken. Er zijn miljoenen algoritmen in onze huis-, tuin- en keukenapparaten en computers die op de achtergrond voorgeprogrammeerde recepten afdraaien en ons leven gemakkelijk maken. Maar er zijn ook algoritmen, die onbewust als bijeffect of bewust in handen van kwaadwil-

lenden, zeer negatieve invloed op ons leven kunnen hebben. Vaak zonder dat we dat zelf beseffen.¹

Als je boeken over vaccinatie in internetwinkels zoekt bepalen algoritmen of je anti- of juist pro- vaccinatieboeken te zien krijgt.² Als ouder wil je weten of jouw kind na drie keer klikken nog in een veilige omgeving is bij een nieuwe *social media* dienst.³ In het ziekenhuis leveren algoritmen in de medische apparatuur inmiddels een grote bijdrage. Maar als je geen behandeling meer krijgt, willen we zeker weten dat die beslissing door de dokter is genomen en niet door een computer. Als je als vrouw een baan bij de overheid misloopt, wil je zeker weten dat er geen selectiemechanisme diep in een algoritme verborgen zit dat alleen maar mannen selecteert.

Algoritmen spelen een bepalende rol bij megatrends als (buitenlandse) digitale inmenging in onze democratie maar ook bij micro-narigheden als het vreselijke antwoord van een overheidsinstelling *de computer staat dat niet toe*, en digitale oplichting. Daarom moeten we meer inzicht krijgen in die algoritmen die mensen potentieel schaden. Alleen dan kunnen we als samenleving algoritmen inzetten voor het goede, grip houden op de snelle ontwikkelingen en zo Nederland online veilig en sterk houden.

1.2. Doel en strekking

Van oudsher was het altijd het individu dat beschermd moest worden tegen de staat. Die had immers het geweldsmonopolie en ruim toegang tot het persoonlijk leven van mensen. Tegenwoordig hebben grote technologiebedrijven minstens zoveel toegang tot onze persoonsgegevens en met algoritmen kunnen zij onze levens steeds meer sturen.

Gebruik van algoritmen kunnen onze grondrechten aantasten en bijvoorbeeld (1) dehumanisering, (2) discriminatie, (3) beperking keuzevrijheid, (4) kansenongelijkheid en (5) het aantasten van onze privacy veroorzaken.⁴ De snelle opkomst van algoritmen vereist daarom een maatschappelijk debat over normen en waarden in de digitale toekomst. Immers onze grondrechten moeten ook in de digitale wereld geborgd zijn.⁵ Het startpunt van de indiener is dat onze, door de eeuwen heen opgebouwde normen en waarden, ook in onze digitale toekomst van toepassing moeten blijven. Oftewel dat grondrechten online dezelfde moeten zijn als offline. Maar, daar waar algoritmen worden ingezet kunnen de grenzen van onze bestaande wetten, normen en waarden geraakt of overschreden worden. Dan is aanpassing of nieuwe wet- en regelgeving nodig. De voorstellen in deze initiatiefnota gaan het proces waarmee we wetten en beleidsregelingen aanpassen aan de digitale tijd stimuleren.

Onderstaande voorstellen proberen niet vooraf de beslissingscriteria van huidige en toekomstige algoritmen voor te schrijven. Zij richten zich dan ook niet op algemene regels als: *alle algoritmen en gebruikte gegevens*

¹ Optimity, (December, 2018), *Algo:aware, state of the art report: algorithmic decision-making*. Procured by the European Commission's Directorate-General for Communications Networks, Content and Technology.

² Algemeen Dagblad, 16 maart 2019 (<https://www.ad.nl/politiek/kabinet-bol-com-moet-boeken-antivaxxers-uit-de-etalage-halen~a3e131935/>)

³ Sunday Times, 27 januari 2019 (<https://www.thetimes.co.uk/edition/news/molly-russells-father-cutting-biting-burning-my-daughter-was-shown-it-all-on-social-media-x0grb8vg>)

⁴ Zuiderveen Borgesius, F. (7 februari, 2018), *Discrimination, artificial intelligence, and algorithmic decision-making*. Council of Europe – Strasbourg: Directorate General of Democracy.

⁵ M.J. Vetzo, J.H. Gerards en R. Nehmelman (1 maart 2018), *Algoritmes en grondrechten*, bijlage bij: Kamerstuk 26 643, nr. 553. Zie ook: Kabinetsreactie Kamerstuk 26 643, nr. 601.

transparant maken en controleren. Om te beoordelen of nieuwe regels nodig zijn en deze dan te maken is veel meer kennis en kunde nodig over de toepassingen en werking van algoritmen. De voorstellen hier zijn daarom gericht op meer inzicht in wat algoritmen precies doen, welke kansen zij bieden en welke de samenleving kunnen schaden.

Deze initiatiefnota zet een eerste stap met een aantal concrete oplossingen, gericht op: samenwerking, bewustwording, online weerbaarheid van mensen en communicatie van algoritme gebruikende instellingen met de samenleving. Daarmee kunnen we, zonder door te schieten met nieuwe regels en verboden, algoritmen met menselijk overzicht, veilig benutten en zorgen dat mensen in vrijheid keuzes kunnen blijven maken. De voorgestelde aanpak zal ook een stimulans zijn voor het maatschappelijk debat over normen en waarden in de digitale toekomst en het gebruik van algoritmen.

De indiener wil aldus kennis en kunde over algoritmen in de samenleving en bij de overheid vergroten. Dat is ook de sleutel om algoritmen te kunnen integreren in onze wet- en regelgeving. Door een helder kader te creëren waarmee we in de samenleving en het economisch leven de kansen die algoritmen bieden kunnen pakken, kan Nederland voorloper worden in Europa.

Wat is er nodig om Nederland online veilig en sterk te houden en mensen weerbaar te maken online in de digitale toekomst?

- i) samenwerking op algoritmebeleid binnen en buiten Nederland;
- ii) transparantie en bewustwording over algoritmen;
- iii) mensen instrumenten geven waardoor ze online weerbaar zijn;
- iv) een taskforce die voorstellen doet voor een toezichtkader dat inzicht geeft maar innovatie de ruimte geeft.

2. Concrete stappen naar menselijke grip op algoritmen

2.1 Algoritmen in de digitale toekomst

Algoritmen kunnen met vaststaande beslisregels werken. Ze kunnen ook zelflerend zijn waardoor na verloop van tijd beslisregels zonder menselijke invloed kunnen veranderen. Dan is er sprake van het gebruik van kunstmatige intelligentie. Bij niet-overheidsinstanties, het Rijk, provincies en ook gemeenten wordt steeds vaker gebruik gemaakt van algoritmen. Op de vraag of ze gebruik maken van algoritmen geeft circa 50% van de overheidsinstanties aan dat te doen. Een deel van die algoritmen maakt gebruik van vormen van kunstmatige intelligentie. Tegelijkertijd experimenteren veel Nederlandse bedrijven met algoritmen en vormen van kunstmatige intelligentie.⁶

Hoe goed werken onze wetten nog bij deze snel ontwikkelende technologie? Algoritmen mogen niet gebruikt worden als deze niet uit te leggen zijn of als er geen menselijk overzicht meer is. Maar hoe gaat de overheid in de praktijk om met dit uitgangspunt? Mag een algoritme dat gebruikt wordt voor het afdekken van een maatschappelijk risico, zoals identiteitsfraude, ook gebruikt worden voor het afdekken van een bedrijfsrisico?⁷

⁶ CBS (27 november, 2018), *Verkennd onderzoek naar het gebruik van algoritmen binnen overheidsorganisaties*; en EY & Microsoft (2 oktober, 2018), *AI in Europe, The Netherlands outlook for 2019 and beyond*.

⁷ Denk bijvoorbeeld aan algoritmen die gebruikt kunnen worden voor het afdekken van bedrijfsrisico's (verstrekken hypotheek) en bij het afdekken van maatschappelijke risico's (voorkomen financiële fraude).

Kortom: algoritmen doorbreken vaak de grenzen tussen overheid en niet-overheid.

2.2 Voorstellen voor menselijke grip op algoritmen

Om menselijke grip op algoritmen te behouden is samenwerking, transparantie, bewustwording nodig. Maar ook nieuwe instrumenten die mensen weerbaar maken en een slim georganiseerd toezicht. Een concrete eerste stap daartoe is meer communicatie met de samenleving over algoritmen door de instellingen die deze gebruiken. Dat begint ermee dat instellingen zelf meer inzicht creëren in kansen, risico's en vooral de gevolgen van de algoritmen die zij gebruiken.

2.2.1 Samenwerking op algoritmebeleid binnen en buiten Nederland

Algoritmen zijn nieuw terrein voor beleidsmakers. De verdeling van verantwoordelijkheden tussen de EU, rijksoverheid en lagere overheden wordt al doende gezocht. In dat proces moet de rijksoverheid een centrale rol hebben en richting geven. Bij gebrek daaraan zullen anders verschillende bestuurslagen, zoals de EU en gemeenten zelf aan de slag gaan. Vaak is dat niet erg want we moeten experimenteren zoals dat nu bijvoorbeeld in vele datalabs in gemeenten plaatsvindt omarmen. Daarbij moeten we wel voorkomen dat dit leidt tot fragmentatie of een lappendeken aan regelingen.

De rijksoverheid moet kennisdeling stimuleren en helpen bij het ontwikkelen van standaarden. Een «nationaal algoritme-samenwerkingsverband» zou daarbij een belangrijke rol kunnen spelen. Zonder helder kader is het voor bestuurders op alle niveaus verleidelijk om van te voren te willen beslissen over bijvoorbeeld «ideologische» keuzes (bijvoorbeeld die tussen vrijheid en gelijkheid) die mogelijk in algoritmen worden gemaakt. Er zijn al gemeenten die alle door henzelf, en door derden gebruikte algoritmen vooraf willen gaan controleren. Deze controle moet dan gekoppeld worden aan vergunningen voor bijvoorbeeld het MKB.⁸ Dit is onwerkbaar al is het maar omdat in deze aanpak politiek verantwoordelijke, bij verandering in politieke verhoudingen (door bijvoorbeeld verkiezingen) algoritmen steeds opnieuw zouden moeten herzien.

Algoritmen houden zich niet aan landsgrenzen, dus is ook samenwerking in Europa nodig. Door nu stappen te zetten in het opbouwen van kennis en kunde over algoritmen kunnen we in de Nederlandse economie en samenleving de kansen die algoritmen bieden ten volle benutten en bouwen we aan een sterke onderhandelingspositie in de EU. Bij het vormgeven van de Nederlandse digitale toekomst mogen we niet afhankelijk worden van de EU. Alleen als we zelf kennis en kunde opbouwen kunnen we zorgen dat we innovatie niet belemmeren en oog houden voor het verschil tussen een multinational en bakker op de hoek. EU-regelgeving voor grote technologiebedrijven kan met één druk op de knop ook gelden voor honderdduizenden kleine Europese bedrijven die online actief zijn of dat nog willen worden. In zo'n *one size fits all* aanpak riskeren we een flinke overdracht van competenties die we in de fysieke wereld nooit hebben toegestaan. Nationale lidstaten moeten daarom, naast samenwerken in Europa, ook zelf aan de slag. Nederland moet zelf waarborgen dat het menselijke boven computers gesteld wordt en het MKB wordt ontzien.

⁸ Zie schriftelijke vragen van de leden Middendorp en Van den Bosch (25 maart 2019): «Amsterdam wil eerlijke computers in de stad», 2019Z05744.

2.2.2 Betekenisvolle transparantie en bewustwording

Mensen zijn zich vaak weinig bewust van de kansen en risico's van algoritmen. Transparantie over beslisregels en de (persoons-)gegevens die algoritmen gebruiken is een belangrijke middel om bewustwording over algoritmen te vergroten.

Een door een computer gegenereerd besluit van de overheid moet nu al aan dezelfde eisen voldoen als een besluit dat door overheidsdienaren wordt genomen. Digitale besluiten moeten inzichtelijk worden gemaakt, anders kunnen ze worden vernietigd.⁹ Door meer transparantie, uitleg en inzicht over algoritmen kunnen technisch onderlegden algoritmen narekenen waardoor juridische procedures vergemakkelijkt zullen worden. Rechters kunnen zo al doende bestaande regels, die door de digitale ontwikkelingen onduidelijk zijn geworden, verduidelijken. De komende jaren kan zo jurisprudentie ontstaan waardoor algoritmegebruik steeds beter in wetgeving verwerkt wordt.

Volledige transparantie over algoritmen en de gegevens die zij gebruiken kan vaker niet dan wel. Ten eerste vanwege veiligheids- en privacyoverwegingen. Ten tweede omdat bedrijven niet gedwongen moeten worden concurrentiegevoelige informatie te delen. Dat zou innovatie en ondernemerschap belemmeren. Ten derde kan volledige transparantie bij overheidsdiensten strategisch gedrag uitlokken om regels te ontduiken. Tot slot levert volledige transparantie in het geval van algoritmen die kunstmatige intelligentie gebruiken weinig op. Transparantie is dus goed maar vooraf altijd volledige transparantie van de broncode (de computertaal die het algoritme bepaald) van algoritmen en de gegevens die zij gebruiken verplichten is niet de oplossing.

Waar volledige transparantie vooraf niet mogelijk of wenselijk is kan op andere manieren meer inzicht bieden toch helpen. De acceptatie van met algoritmen genomen besluiten of maatregelen wordt groter als mensen weten dat er algoritmen zijn gebruikt. Ook helpt het als mensen weten op basis waarvan een besluit door een algoritme genomen is. Tot slot kan een versimpelde uitleg van een beslissingsmechanisme in een algoritme helpen. Illustraties kunnen veel inzichtelijker zijn dan de broncode van een ingewikkeld algoritme.¹⁰ «Betekenisvolle» transparantie werkt soms beter dan volledige transparantie. Het bewustwordingsproces over algoritmen moet op jonge leeftijd beginnen. Onderwijs kan daarbij een grote rol spelen.

2.2.3 Mensen instrumenten geven om online weerbaar te zijn

Naast bewustwording kunnen mensen ook weerbaarder worden online door nieuwe toepassingen. De overheid zou de private sector en brancheorganisaties in de ontwikkeling van algoritmecheckers, ratingssystemen en keurmerken moeten stimuleren en ondersteunen. Algoritmecheckers zijn apps of programma's die algoritmegebruik, bijvoorbeeld in je telefoon, inzichtelijk maken. Dat kan bijvoorbeeld in combinatie met ratingssystemen of keurmerken. Bij ratingssystemen kan gedacht worden

⁹ Raad van State, 6 september 2018, *Nader rapport inzake de effecten van digitalisering voor de rechtsstatelijke verhoudingen*, Kamerstuk 26 643, nr. 557 en daarin genoemde AERIUS case: Stichting Behoud de Peel tegen gedeputeerde staten van Noord-Brabant. ECLI:NL:RVS:2017:1259 r.o. 14.3, 14.4, 24.3.

¹⁰ Zie bijvoorbeeld DARPA, *Explainable Artificial Intelligence (XAI)*, program update November 2017 (via: <https://www.darpa.mil/attachments/XAIProgramUpdate.pdf>).

aan een programma dat aangeeft dat de nieuwe app die je op je telefoon download op basis van gebruikersreacties «vijf sterren» voor privacy heeft.

Ten tweede kan het ontwikkelen van vormen van online identiteit helpen.¹¹ Dat is in de fysieke wereld al lang een taak van de overheid (voorbeeld: paspoort). Een versimpeld voorbeeld van hoe dat zou kunnen werken is: als je online een «groen» paspoort kiest ga je akkoord met de gebruiksvoorwaarden van algoritme gebruikende diensten. Als je een «geel» paspoort kiest wil je niet bloot staan aan bepaalde algoritme. Als je een «rood» paspoort kiest wil je helemaal niet bloot worden gesteld aan algoritmen die jouw persoonsgegevens gebruiken. Dat laatste zou kunnen betekenen dat je veel innovatieve diensten niet kan gebruiken. Een dergelijk systeem kan op vele manieren vorm gegeven worden en kan alleen in samenwerking met de private sector ontwikkeld worden. De variatie in wat mensen kunnen kiezen beperkt zich ook niet tot drie keuzes groen, geel en rood zoals in het voorbeeld boven. De kern is dat mensen niet meer bij elke overheidsinstelling of technologiebedrijf op de website apart cookies accepteren of lange gebruiksovereenkomsten sluiten maar makkelijker of zelfs in één keer kunnen aangeven wat zij willen toestaan. Bij al deze nieuwe instrumenten is tot slot uiteindelijk keuzevrijheid belangrijk. Door kleine concurrenten van de bestaande grote technologiebedrijven de ruimte te geven kunnen mensen alternatieven zoeken voor algoritmen toepassingen waar ze niet aan bloot willen worden gesteld.

2.2.4 Inzicht door toezicht

Op dit moment werkt overheid versnipperd. Op verschillende ministeries wordt op deelterreinen naar vormen van toezicht op het gebruik van algoritmen gekeken. Een voorbeeld is het pleidooi van de Staatscommissie parlementair stelsel voor een speciale toezichthouder op algoritmen bij verkiezingen.¹² Een toezichtkader voor algoritmen moet innovatie de ruimte geven, kleine ondernemingen zoals het MKB ontzien en geen onnodige administratieve lasten creëren. Niet regels die verbieden, zonder dat we precies overzien of die nodig zijn maar regels gericht op meer informatie (*disclosure*) zijn nu nodig.

Toezicht kan vooraf, continu of achteraf plaatsvinden. Het zijn mensen die algoritmen bedenken en programmeren. Toch is het vooraf vastleggen van de gedetailleerde uitkomsten van algoritmegebruik alleen in theorie mogelijk. Het aantal algoritmen is enorm, groeit razendsnel en het belangrijkste: ontwikkelingen in de toekomst zijn per definitie niet vast te leggen. Daarbij maakt het gebruik van kunstmatige intelligentie dat beslisregels kunnen veranderen. Alle algoritmen vooraf beoordelen op de uitkomsten die zij *kunnen* genereren zou dus enorme menskracht eisen en enorme administratieve lasten betekenen.¹³ Daarom worden hier voorstellen gedaan voor een toezichtkader dat zich veel meer richt op de resultaten van algoritmegebruik¹⁴ en «risicogericht» is. Voor dat laatste is de beoordeling of en hoe een bepaald algoritme, soms onbedoeld en onvoorzien, negatieve invloed op mensen kan hebben, van groot belang.

¹¹ Initiatiefnota van de leden Middendorp en Verhoeven: *Online identiteit en regie op persoonsgegevens*, Kamerstuk 34 993, nr. 2.

¹² Zie: eindrapport Staatscommissie parlementair stelsel, *Lage drempels, hoge dijken. Democratie en rechtsstaat in balans*. Kamerstuk 34 430, nr. 9.

¹³ Om alle uitkomsten van alle mogelijke algoritmen te voren te beoordelen is een *superalgoritme* nodig.

¹⁴ Hier wordt aangesloten bij het verschil tussen *ex ante* (vooraf) en *ex post* (achteraf) toezicht.

De indiener wil elementen van het risicobeheer in de financiële sector en het bestaande jaarverslagensysteem in Nederland combineren om tot specifiek algoritmetoezicht te komen. Dat kan door een drieslag. Ten eerste rapportage door algoritme gebruikende instellingen zelf over: (1) algoritmen met een hoog risicoprofiel (specifieke aandacht voor economische-, veiligheid- en privacy risico's); (2) mogelijke (economische) risico's voor mensen van door hen gebruikte algoritmen; (3) interne risicobeheersingsprocessen; (4) de resultaten die de gebruikte algoritmen genereren. Ten tweede externe partijen (bijvoorbeeld accountants) die met algoritme gebruikende instellingen meekijken. Ten derde een publieke algoritmetoezichthouder die zich met kennis en kunde van algoritmegebruik specifiek richt op de hier beschreven principes en vormen van rapportage. Door meer te communiceren over algoritmen kan de samenleving meer inzicht krijgen maar wordt ook richting gegeven aan de interne inspanningen van algoritme gebruikende instellingen. Deze systematiek moet de basis zijn voor meer inzicht, externe controle en in het uiterste geval ingrijpen. Zij kan worden ingepast in de jaarlijkse rapportagecyclus van (overheids-) instellingen over bedrijfsprocessen en financiën. In control-verklaringen zoals accountants die nu afgeven bij jaarverslagen kunnen hierbij een rol spelen.

Bestaande toezichthouders moeten hun verantwoordelijkheden behouden maar er is een extra inspanning op het snijvlak van consumentenbescherming, data-, identiteit- of privacygebied die alle door algoritmegebruik geraakt worden, nodig.¹⁵ Dat kan door een toezichthouder die zich specifiek richt op algoritmegebruik. Die moet zorgen voor de voorgestelde rapportagesystematiek en kennisdeling bij overheid. Om bovenbeschreven toezichtkader gebaseerd op de principes: betekenisvolle transparantie; risico- en resultaatgericht; kennisdeling en gericht op communicatie met de samenleving vorm te geven is een overheidstaskforce nodig. Deze moet de bestaande kennis in de private- en publieke sector bundelen en bestaande wetgeving en toezichtstructuren als basis nemen.

3. De huidige stand van zaken en uitvoering

3.1 Stand van zaken en wettelijk kader

Overheden overal ter wereld zijn op zoek naar manieren om algoritmegebruik te integreren in de samenleving en bestaande wet en regelgeving. In Nederland heeft het kabinet als onderdeel van haar *Nederland Digitaal Strategie* een *Data Agenda Overheid* en een *Datadeel Visie Bedrijven* naar de Kamer gestuurd.¹⁶ In het bedrijfsleven lopen tal van initiatieven rondom algoritmen en kunstmatige intelligentie bijvoorbeeld via zelf-opgelegde ethische codes.¹⁷ In het debat over algoritmen wordt vaak de nadruk gelegd op een deelsegment van de digitale samenleving en/ of uitgaan van vergaande, vooraf opgelegde, controle op broncodes en gebruikte gegevens.¹⁸ In de Verenigde Staten is in het Amerikaans Congres wetgeving in behandeling die ook voorstellen zoals hier bepleit bevat.¹⁹

¹⁵ Zie: <https://icdppc.org/wp-content/uploads/2018/11/ICDPPC-DCCWG-Report-Final.pdf>

¹⁶ Zie: Nederland Digitaal (15 juni 2018), Kamerstukken II 2017/18, 26 643, 541; en: *Agenda Digitale Overheid*. Kamerstuk 26 643, nr. 549; en: *Inzake visie op data delen*, Kamerstuk 26 643, nr. 594.

¹⁷ <https://www.nederlandict.nl/ethischecodeai/>

¹⁸ Zie o.a. *Big data en de bescherming van persoonsgegevens* (AO d.d. 30/05) en Kamerstuk 26 643, nr. 570.

¹⁹ Zie de *Algorithmic Accountability Act* van 1 mei 2018 (<https://www.wyden.senate.gov/imo/media/doc/Algorithmic%20Accountability%20Act%20of%202019%20Bill%20Text.pdf>).

AVG en persoonsgegevens

De Algemene verordening gegevensbescherming (AVG)²⁰ is voor deze nota van belang. Ten eerste omdat algoritmen bijna altijd gebruik maken van (geanonimiseerde) persoonsgegevens. In de AVG wordt in artikel 12 bepaald dat persoonsgegevens op een beknopte, transparante, begrijpelijke, gemakkelijke en toegankelijke wijze moeten worden verwerkt. Dit wordt uitgewerkt in verschillende informatieverplichtingen. Naast verplichtingen met betrekking tot persoonsgegevens zijn er ook verplichtingen over geautomatiseerde besluitvorming.

Ten tweede verplicht de AVG de logica en de beoogde gevolgen van geautomatiseerde besluitvorming toe te lichten. Ook moeten betrokkenen geïnformeerd worden als zij onderhevig zijn aan geautomatiseerde besluitvorming (artikel 13 AVG). De beoordelingscriteria die algoritmen gebruiken moeten transparant worden gemaakt en «verwerkingen waarbij de oorsprong van de uitkomst niet te herleiden is mogen niet gebruikt worden» (artikel 12). «Black box» algoritmen mogen dus niet worden gebruikt.²¹ Tot slot is een belangrijk element in de AVG de «menselijke factor»: «*betrokkene heeft recht om niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft*».²² Algoritmen die met kunstmatige intelligentie werken of geen menselijke controle meer mogelijk maken, kunnen dus volgens deze twee voorschriften niet gebruikt worden. Vrijstelling van delen van de AVG kan verkregen worden als uitvoering bijvoorbeeld de nationale veiligheid in gevaar brengt.

Huidige toezichtstructuur

De Autoriteit Consument en Markt (ACM) ziet toe op mededinging, telecommunicatie en consumentenrecht. De recente beslissing van het Duitse *Bundeskartellamt* dat persoonsgegevens die technologiebedrijven gebruiken een «relevante factor» voor marktdominantie kunnen zijn²³ laat zien dat regulering van de digitale wereld op twee benen moet staan: mededinging maar ook andere vormen van consumentenbescherming. Voor de Autoriteit Financiële Markten (AFM) is het toezicht op data en technologie een prioriteit. Deze instelling heeft veel kennis over algoritmen. De Autoriteit Persoonsgegevens (AP) ziet toe op privacywetgeving en richt zich op persoonsgegevens. De AP werkt met een zogenaamde passieve informatieplicht en heeft de bevoegdheid boetes uit te delen. De AP heeft een samenwerkingsprotocol met de ACM gericht op het uitwisselen van informatie.²⁴ Het College voor de Rechten van de Mens richt zich op de gelijke behandeling en heeft de digitale wereld als speerpunt. De Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten houdt toezicht op de geheime diensten. Het Commissariaat voor de media, is verantwoordelijk voor het toezicht op de naleving van de Mediawet waarbij online media steeds belangrijker wordt.

²⁰ Verordening (EU) nr. 2016/679 (27 april 2016) over bescherming persoonsgegevens, het vrije verkeer van gegevens en intrekking van richtlijn 95/46/EG.

²¹ Zie: brief van de Minister voor Rechtsbescherming inzake *transparantie van algoritmes in gebruik bij de overheid*. Kamerstukken 26 643 en 32 761, nr. 570.

²² AVG (PbEU 2016, L 119), Artikel 22, lid 1.

²³ *Bundeskartellamt* (7 februari 2019), *Bundeskartellamt prohibits Facebook from combining user data from different sources*, https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen-/2019/07_02_2019_Facebook.html.

²⁴ Zie: https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/convenant_acm-ap.pdf

De huidige wetgeving met betrekking tot rapportageverplichtingen is divers en afhankelijk van organisatietype en grootte (klein, middelgroot, groot). Beursgenoteerde ondernemingen, organisaties van openbaar belang zoals die worden gedefinieerd in de Wet toezicht accountantsorganisaties (Wta) en provincies en gemeenten rapporteren allemaal anders over hun financiën en bedrijfsvoering. De AFM houdt toezicht op de naleving van nationale wettelijke voorschriften en internationale verslaggevingsstandaarden (IFRS) bij beursgenoteerde bedrijven. Daarvoor is de Wet toezicht financiële verslaggeving (Wtfv) de basis. Gemeenten en provincies hebben verplichtingen over de verslaglegging van de jaarrekening, zo benoemen zij zelf accountants voor externe controle op basis van de Gemeente- en Provinciewet.²⁵ Op de hoofdprincipes van verslaglegging zijn er veel overeenkomsten. En daar wil de indiener bij aansluiten.

Europees kader

Naast verschillende toezichthouders en verschillende bestuurslagen op nationaal niveau speelt ook supranationaal beleid en toezicht een rol. De Autoriteit Persoonsgegevens is inmiddels onderdeel van een Europese structuur. Het land van de hoofdvestiging van de persoonsgegevens bewerkende instelling is binnen de EU bepalend voor wat de competente persoonsgegevensautoriteit is. Tegelijkertijd kan in het geval van persoonsgegevens de Nederlandse wet boven de AVG gaan. De Europese Commissie onderzoekt momenteel hoe zij om wil gaan met algoritmen en hoe bewustwording van het gebruik van algoritmen kan worden vergroot.²⁶

3.2 Uitvoering

Om de digitale toekomst van Nederland vorm te geven is veel kennis en kunde nodig. In de eerste plaats moet de overheid zo veel mogelijk op hetzelfde kennisniveau als technologiebedrijven komen. In de tweede plaats moet zij, waar dat niet kan, gebruik maken van de beschikbare kennis in de private sector.²⁷ Binnen de overheid moet kennis zoveel mogelijk gedeeld worden. Tevens moet in de uitvoering zoveel mogelijk bij bestaande structuren en wet- en regelgeving aangesloten worden. Ook zullen bij het inpassen van algoritmegebruik door overheidsinstellingen en niet-overheidsinstellingen in bestaande regelgeving soms de grenzen tussen departementen doorbroken moeten worden. Kennis kan immers op allerlei plekken bij de overheid beschikbaar zijn. Kijk bij het uitwerken van de hier gedane voorstellen ook naar de mogelijkheden die een Rijksinspectie Digitalisering daarbij zou bieden.²⁸

4. Financiële consequenties

Voor de voorgestelde onderzoeken kan gebruik gemaakt worden van de bestaande kennisinfrastructuur op de departementen, maar ook in instituten als TNO en het Rathenau Instituut. Er zijn geen nieuwe kosten gemoeid met de beoogde samenwerking met het bedrijfsleven en maatschappelijke organisaties. De inventarisatie van toepassingen in het buitenland, alsook het agenderen van algoritmen in dit verband, kan met

²⁵ Zie: Gemeentewet (Artikel 213, lid 2) en Provinciewet (artikel 217, lid 2).

²⁶ Europese Commissie, *Algorithmic Awareness-Building*: <https://ec.europa.eu/digital-single-market/en/algorithmic-awareness-building>.

²⁷ Zie: <https://icai.ai/> en de Taskforce AI voor Nederland waarin door Ministerie van Economische Zaken en Klimaat en VNO-NCW met vele partijen werkt aan een nationaal Kunstmatige Intelligentie actieplan.

²⁸ Gewijzigde motie van het lid Middendorp, *Rijksinspectie Digitalisering*, Kamerstuk 35 000 VII, nr. 34.

het bestaande apparaat. Het oprichten van de voorgestelde taskforce kan binnen de huidige begroting. Het voorgestelde toezichtkader kan wel kosten met zich meebrengen, bijvoorbeeld in de vorm van Fte's maar de indiener verwacht dat dit een kleine organisatie kan worden.

5. Beslispunten

De indiener vraagt de Kamer in te stemmen met het verzoek aan de Minister voor Rechtsbescherming om met betrokken collega's – in het bijzonder de Minister van Binnenlandse Zaken en Koninkrijksrelaties de Minister van Economische Zaken en Klimaat – te werken aan onderstaande deeloplossingen:

I) Samenwerking op algoritmebeleid binnen en buiten Nederland

- a) Het nauwgezet en stelselmatig betrekken van maatschappelijke organisaties, bedrijven en mensen uit de praktijk. Dat kan in een nationaal algoritme-samenwerkingsverband waarin het ontwikkelen van ideeën en het agenderen van en het bevorderen van een praktische discussie over de rol van algoritmen in onze samenleving centraal staat;
- b) Europese en internationale samenwerking gericht op het veilig inzetten van algoritmen waarbij innovatie niet belemmerd wordt en op een manier die werkt voor grote en kleine bedrijven;
- c) Onderzoeken waar Europese en waar nationale standaarden nodig zijn. Daarbij steeds de Nederlandse kennis en kunde waarborgen. Bijzondere aandacht geven aan die situaties waar algoritmen (potentieel) grote impact op mensen hebben;
- d) Analyse van de huidige samenwerking tussen gemeenten, provincies en Rijk als het gaat om algoritmen en voorstellen doen voor een kenniscentrum voor algoritmen waar ideeën over het gebruik en regulering kunnen worden uitgewisseld.

II) Bewustwording over algoritmen vergroten

- a) Vergroten van het maatschappelijk bewustzijn over kansen en risico's van algoritmegebruik en de werking daarvan. Daarbij speciale aandacht voor de rechterlijke macht;
- b) Waar mogelijk mensen duidelijk maken wanneer er algoritmen gebruikt zijn bij beslissingen, inclusief een versimpelde uitleg of illustratie;
- c) Onderzoeken hoe onderwijs kan bijdragen aan bewustwording over kansen en risico's van algoritmen;

III) Mensen instrumenten geven om ze online weerbaar te maken

- a) In overleg met technologiebedrijven de mogelijkheden onderzoeken om mensen online de mogelijkheid te geven in één keer aan te geven wat ze algoritme gebruikende instellingen willen toestaan en wat niet;
- b) Onderzoek met technologiebedrijven en ICT-brancheorganisaties naar algoritme checkers, keurmerken en ratingsystemen en bestaande initiatieven in deze stimuleren.

IV) Toezicht dat innovatie de ruimte geeft, MKB-proof is en Nederland online sterk en veilig houdt

- a) Een inventarisatie maken van de gekozen aanpak in het buitenland om algoritme gebruikende instellingen meer te laten communiceren over algoritmegebruik. Daarbij specifiek naar Duitsland, Frankrijk Groot-Brittannië en de Verenigde Staten te kijken;

- b) Bundelen van huidige kennis en lopende onderzoeken op de verschillende ministeries en toezichthouders;
- c) Inventariseren van lacunes in het huidige wettelijk- en toezichtkader;
- d) Een taskforce instellen met als opdracht bovenbeschreven operationeel toezichtkader uit te werken op basis van de genoemde principes:
 - i. communicatie met de samenleving van algoritme gebruikende instellingen door rapportage;
 - ii. betekenisvolle transparantie;
 - iii. risicogerichte selectie;
 - iv. *ex post* rapportage, dus achteraf en gericht op resultaten;
- e) daarbij bestaande rapportages van overheid en niet-overheidsinstellingen om over financiën en bedrijfsprocessen te rapporteren als voorbeeld te nemen;
- f) een toezichthouder die bestaande inspanningen van toezichthouders in de digitale wereld aanvult als het gaat om toepassingen en gebruik van algoritmen en bovenstaande principes en rapportagekader handhaaft.

Middendorp