



Algoritmisch Bestuur
Hoe het gebruik van algoritmen de
legitimiteit van de overheid bedreigt
en wat we hieraan kunnen doen

Preadvies Staatsrechtconferentie 2020

Albert Meijer, Stephan Grimmelikhuijsen

1. Introductie

De sociale, economische en politieke verhoudingen in de samenleving veranderen sterk onder invloed van het gebruik van geavanceerde (*machine learning*) algoritmen. Deze algoritmen worden ingezet door techbedrijven zoals AirBnB, Facebook en Twitter om economische interacties rondom de verhuur van huizen te versoepelen, om vriendschappen gemakkelijker te kunnen onderhouden en om politieke discussies te modereren (Van Dijck, Poell & De Waal, 2018). Deze algoritmen nemen rollen van mensen over en ondervangen deels menselijke tekortkomingen, maar ook de algoritmen zijn niet neutraal (Willson, 2017; Fry, 2018). Dat heeft geleid tot allerlei debatten over de wenselijkheid van de platformeconomie, de verslaving van jongeren aan telefoongebruik en inmenging in democratische processen. Het gebruik van deze technologieën heeft dus een grote – ontwrichtende – invloed op maatschappelijke verhoudingen (Zuboff, 2019). Daarom is er wereldwijd veel zorg over de uitwerking van het gebruik van algoritmen op machtsverhoudingen en publieke waarden.

Een specifiek onderdeel van het bredere debat over de algoritmisering van de samenleving betreft de invloed van dit maatschappelijke proces op het functioneren van de overheid (Peeters & Schuilenburg, 2020). Hoewel het gebruik van algoritmen bij overheden nog in de kinderschoenen staat zien we al dat ook het functioneren van overheidsorganisaties sterk kan worden beïnvloed door het gebruik van deze systemen (Vogl et al. 2020). Specifieke, en veelbesproken, voorbeelden zijn het gebruik van predictive- policing-systemen bij de politie (CAS, Criminaliteits Anticipatie Systeem) en risico-inventarisatie systemen in het toezicht op uitkeringen en belastingen (SyRI, Systeem Risico-Indicatie) (Van Schendel, 2019) maar ook allerlei andere overheidsorganisaties verkennen hoe zij algoritmische systemen kunnen inzetten om de taakuitvoering te verbeteren (voor een breed overzicht: TNO, 2019). Ook bij het gebruik van algoritmische systemen door overheidsorganisaties is de belofte dat dit leidt tot een meer efficiënte en effectieve overheid, maar is er tegelijkertijd veel zorg over de impact van dit gebruik op machtsverhoudingen en publieke waarden. Daarbij wordt met name benadrukt dat de privacy kan worden geschonden, de rechtsbescherming kan worden aangetast en dat het gebruiken van systemen kan leiden tot discriminatie van bepaalde groepen (Kulk, Van Deursen e.a., 2020).

In dit preadvies willen wij het debat over de wenselijkheid van het gebruik van algoritmen door overheidsorganisaties plaatsen binnen het bredere kader van het debat over de legitimiteit van overheidshandelen. Als bestuurswetenschappers benaderen wij het thema legitimiteit niet als een juridisch begrip maar als een sociaal geconstrueerd begrip. In brede zin definiëren wij legitimiteit als het geïnternaliseerde gevoel van het willen gehoorzamen aan autoriteit zonder dat er daadwerkelijke dwang wordt uitgeoefend (Lipset, 1959; Suchman, 1995; Tyler, 1997). De vraag is dan dus hoe het gebruik van algoritmen het geïnternaliseerde gevoel van het willen gehoorzamen aan autoriteit beïnvloedt. Op basis hiervan kan worden bekeken welke institutionele mechanismen noodzakelijk zijn om de legitimiteit van het gebruik van algoritmische systemen door overheidsorganisaties te versterken. Daarbij zal het zowel gaan om 'harde mechanismen' in de vorm van wet- en regelgeving als 'zachtere mechanismen' die betrekking hebben op manieren van werken in de publieke sector. Daarmee stellen we in dit preadvies de volgende vragen aan de orde:

1. Op welke manier kan het gebruik van algoritmen door overheidsorganisaties de legitimiteit van deze organisaties bedreigen?
2. Welke institutionele mechanismen zijn nodig om de legitimiteit van het gebruik van algoritmen door overheidsorganisaties te borgen?

Het doel van ons preadvies is om te komen tot een verdieping van het debat over institutionele mechanismen die nodig zijn om de legitimiteit van algoritmisch bestuur te borgen door de verschillende mogelijke acties te plaatsen in een systematisch overzicht. We willen hierbij benadrukken dat er niet een *silver bullet* bestaat – zoals transparantie van algoritmen of waardengevoelig ontwerp – maar dat het versterken van legitimiteit een divers geheel aan

interventies vergt. Daarbij gaat het meer algemeen om het herijken van bestaande manieren om de legitimiteit van de overheid te borgen.¹

Dit stuk is geschreven als preadvies voor de Staatsrechtconferentie 2020, vanuit een bestuurswetenschappelijk perspectief. Vanuit dit perspectief identificeren wij relevante issues als een startpunt voor een debat over de staatsrechtelijke implicaties. Daarbij is van belang dat de verschillende strategieën die wij benoemen allerlei juridische gevolgen kunnen hebben, maar dat het doel niet is om deze in dit (bestuurswetenschappelijke) essay uit te diepen. Wel zullen wij de vraag oproepen hoe dit dan staatsrechtelijk kan worden geregeld.

Het preadvies is als volgt opgebouwd. We beginnen met een duiding van het centrale begrip algoritmisch bestuur op basis van de bestuurswetenschappelijke literatuur. Centraal hierin staat de idee van algoritmisch bestuur als een nieuwe manier van organiseren rondom het gebruik van een algoritme, dus niet alleen het gebruik van een nieuw instrument binnen de oude organisatie. Vervolgens bespreken we het begrip legitimiteit en maken hierbij een onderscheid tussen drie routes richting legitiem bestuur: input, throughput en output-legitimiteit. Dit onderscheid gebruiken we om de verschillende bedreigingen voor de legitimiteit van algoritmisch bestuur te bespreken en vervolgens om strategieën te identificeren om de legitimiteit hiervan te versterken. We eindigen met conclusies en reflecties en benadrukken met name dat het nodig is om de huidige ontwikkeling in de richting van algoritmisch bestuur niet buiten maar binnen de democratische rechtstaat een plek te geven.

2. Algoritmisch bestuur

Onder het bestuur verstaan wij in dit preadvies het geheel aan uitvoerende overheidsorganisaties. De organisatie van het bestuur is gebaseerd op basiskenmerken van bureaucratistische organisaties zoals eenduidige toepassing van regels, aansturing door politiek verantwoordelijken en gebruik van expertkennis (Weber, 1978 [1909]; Wilson, 2019). De afgelopen decennia zijn bestuurlijke organisaties echter in een hoog tempo veranderd door de introductie van nieuwe technologieën in de uitvoering. Dat heeft ertoe geleid dat, zowel aan de 'voorkant' van de dienstverlening als aan de 'achterkant' van de planning en besluitvorming, overheidsorganisaties radicaal getransformeerd zijn. Typische voorbeelden zijn het Centraal Justitieel Incassobureau (CJIB) en de Dienst Uitvoering Onderwijs (DUO), waarbij de organisatie om de ICT-infrastructuur is heen gebouwd (Zouridis, 2000), maar ook alle andere overheidsorganisaties, van politie tot Staatsbosbeheer, zijn volledig afhankelijk geraakt van informatie- en communicatietechnologieën.

De nieuwste ontwikkeling in de doorgaande ondersteuning van overheidsprocessen met behulp van ICT betreft het gebruik van moderne algoritmen. In de meest basale zin zijn algoritmen gewoon rekenregels en is er met het gebruik van algoritmen niets nieuws aan de hand in vergelijking met 'gewone' vormen van menselijke besluitvorming of met geautomatiseerde besluitvormingsprocessen (Frissen, Van Eck & Drouen, 2019). Moderne algoritmen verdienen echter wel bijzondere aandacht omdat zij een aantal specifieke kenmerken hebben. Allereerst geldt dat de zogenaamde *machine-learning*-algoritmen sterk in opkomst zijn. Dit zijn algoritmen die hun regels aanpassen op basis van leerervaringen en dat betekent dat de programmeurs dus ook niet meer weten volgens welke regels het algoritme functioneert (Kulk, Van Deursen e.a. 2020: 32 - 35). Vetzó, Gerards & Nehmelman (2018: 48) karakteriseren *machine-learning*-algoritmen als

¹ Ons essay heeft – mede om het vraagstuk hanteerbaar te maken – een focus op de bedreigingen van het gebruik van algoritmen voor de legitimiteit van de overheid. Kulk, Van Deursen e.a. (2020) merken ook terecht op dat het gebruik van algoritmen ook nieuwe kansen biedt om de legitimiteit van het bestuur te versterken. Zo merken zij op dat goed-geprogrammeerde en gevalideerde algoritmen in beginsel beter dan mensen in staat zijn om zonder aanzien des persoons een besluit te nemen (p. 4, 5). Voor de strategieën die wij presenteren om met bedreigingen om te gaan geldt dan ook dat toepassing van deze strategieën niet alleen hoeft te leiden tot legitimiteit op hetzelfde niveau, maar mogelijk zelfs een versterking van de legitimiteit ten opzichte van de niet-gealgoritmiseerde situatie tot gevolg kan hebben.

ondoorzichtige en niet-neutrale menselijke constructen.² Ons preadvies richt zich met name op *machine-learning*-algoritmen.

De laatste jaren zien we dat deze moderne algoritmen worden geïntroduceerd om niet alleen routinematige maar ook kennisintensieve overheidstaken te ondersteunen of zelfs over te nemen. Het gaat hierbij om een voortzetting van een bestaande ontwikkeling (evolutie) maar door de nieuwe toepassingen om ook ingrijpende veranderingen (revolutie) (zie ook: WRR: 2016: 37). Daarin ligt het cruciale verschil met de voorgaande vormen van informatisering: kennisintensieve taken worden overgenomen door moderne algoritmen met een zekere mate van artificiële intelligentie. Deze systemen worden bijvoorbeeld gebruikt voor risico-analyses en planningsprocessen van toezichthouders en politie zoals bij SyRI en het Criminaliteit Anticipatie Systeem (Van Schendel, 2019). Het gebruik van algoritmen is momenteel nog beperkt maar groeit snel. De verwachting is dat deze technologieën in de komende jaren een steeds belangrijkere rol gaan spelen in het functioneren van overheidsorganisaties (Vogl et al., 2020).

Wanneer algoritmen een centrale rol gaan spelen in het functioneren van de overheid spreken we van algoritmisch bestuur: het bestuur is dan voor de uitvoering van zijn kerntaken in hoge mate afhankelijk geworden van algoritmen. Algoritmisch bestuur is de meest recente manifestatie van het bredere fenomeen digitaal bestuur (ofwel e-government). Bij digitaal bestuur gaat het om het gebruik van moderne informatie- en communicatietechnologieën om het bestuur in al zijn facetten te ondersteunen (West, 2005). Bij algoritmisch bestuur gaat het specifiek om het gebruik van moderne algoritmen met een zekere mate van artificiële intelligentie voor een variëteit aan overheidsprocessen zoals besluitvorming, dienstverlening en beleidsontwikkeling (Meijer & Grimmelhuijsen, 2020). Algoritmisch bestuur bestaat nog slechts in beperkte mate, maar de beweging in de richting van algoritmisch bestuur verdient onze volle aandacht omdat deze vorm van bestuur een aantal specifieke vragen oproept. Die vragen komen verderop in dit preadvies aan de orde.

De volgende (Nederlandse en internationale) voorbeelden laten zien op welke verschillende manieren algoritmen worden gebruikt in het bestuur en resulteren in een hoge mate van afhankelijkheid van deze algoritmen voor kerntaken zoals planning en besluitvorming. Ze laten daarmee de contouren zien van algoritmisch bestuur. Ook laten deze voorbeelden zien welke maatschappelijke discussie de opbouw van algoritmisch bestuur oproept.

- *Gebruik van algoritmen voor het plannen van inzet van politie in verschillende wijken van de stad.* Wereldwijd maken politiekorpsen gebruik van zogenaamde *predictive-policing*-systemen om de planning van de inzet van politiemensen en middelen te verbeteren (Meijer & Wessels, 2019). Zo maakt de Nederlandse politie gebruik van het Criminaliteit Anticipatie Systeem om de planning van politie-inzet te optimaliseren. Zoals Willems & Doeleman (2014: 41) het formuleren: 'Het systeem is leidend in de planning voor de flexteams, die over de hele eenheid ingezet worden, en is in de verschillende districten van de eenheid een belangrijke informatiebron voor het inzetadvies.' In de wetenschap en de samenleving is er veel discussie over de vraag of dergelijke *predictive-policing*-systemen groepen stigmatiseren en een bestaande bias automatiseren (Meijer & Wessels, 2019).

² Een grondige en ook nog eens zeer toegankelijke beschouwing op algoritmen is te vinden in Fry (2018). Zij maakt ook het belangrijke onderscheid tussen regelgeleide algoritmen en *machine-learning*-algoritmen. Regelgeleide algoritmen bestaan al lange tijd en worden binnen overheden op grote schaal gebruikt om besluiten over bijvoorbeeld toekenning van studiefinanciering te ondersteunen. *Machine-learning*-algoritmen zijn nieuw en gelden als een vorm van Artificiële Intelligentie (AI). *Machine learning* kan plaats vinden met of zonder menselijke supervisie. *Machine-learning*-algoritmen zijn overigens slechts één vorm van wat Artificiële Intelligentie (AI) wordt genoemd. Er zijn ook andere vormen van AI, zoals neurale netwerken en *natural language processing*. Anderzijds is *machine learning* weer een eigen categorie waarbinnen verschillende varianten bestaan, zoals *supervised* en *unsupervised learning*. Dit preadvies gaat met name over *machine-learning*-algoritmen. Voor een gedetailleerdere bespreking van de technologische fitnesses en specifieke problemen die hiermee gepaard gaan verwijzen we ook naar Guidotti e.a. (2018).

- *Gebruik van algoritmen als ondersteuning bij besluitvorming over ondersteuning van daklozen.* Een internationaal voorbeeld uit de Amerikaanse staat Indiana laat zien hoe algoritmen worden gebruikt om de relatieve kwetsbaarheid van daklozen te berekenen zodat ze hen kunnen prioriteren bij het verzorgen van huisvesting. Het algoritme kreeg een sleutelrol in de besluitvorming over toekenning van ondersteuning door de betreffende overheidsorganisatie: de besluiten werden gebaseerd op dit algoritme. De staat wees vervolgens onterecht 1 miljoen aanvragen voor gezondheidszorg voedselbonnen en financiële ondersteuning af omdat het systeem elke fout in het aanvraagproces had gekwalificeerd als niet willen samenwerken aan het overheidsproces (Eubanks, 2017).
- *Gebruik van algoritmen ten behoeve van de WOZ-waarde.* De gemeente Castricum maakt gebruik van een algoritme om de verandering in de waarde van een huis te bepalen ten behoeve van de WOZ. Deze waardebepaling is een complex en informatie-intensief proces en daarom kan een algoritme belangrijke ondersteuning bieden. De wijze waarop dit algoritme precies op basis van de transactiepreizen van de gerealiseerde grondverkoop van de vergelijkingsobjecten tot een bepaling van de waarde komt is echter – ook voor de betreffende ambtenaar – niet doorzichtig en roept daarom belangrijke vragen op over de transparantie van besluitvorming (Gerechtshof Amsterdam, 11 februari 2020, 17/00570).

Voor onze analyse willen we vier kenmerken van moderne algoritmen benadrukken: *complexiteit, onkenbaarheid, afhankelijkheid* en *waarschijnlijkheid*. De complexiteit heeft te maken met zowel de ingewikkelde technologische structuur als met de koppeling met specifieke contexten (Vetzo, Gerards & Nehmelman, 2018: 49). De onkenbaarheid heeft te maken met de *machine learning* waarmee de regels van het algoritme via geautomatiseerd of *human-supervised*-leren worden aangepast, waardoor ze steeds verder evolueren. Met name bij algoritmen die door middel van *unsupervised learning* evolueren is het lastig om te weten wat de doorslaggevende variabelen zijn voor het geven van een bepaalde uitkomst (Burrell, 2016). De afhankelijkheid heeft betrekking op het feit dat moderne algoritmen gebruik maken van allerlei verschillende datasets van de eigen organisatie maar ook van andere organisaties en open datasets. Dit betekent dat de vormgeving van externe datasets invloed heeft op de uitkomsten van het algoritme. Kulk, Van Deursen e.a. (2020) beschrijven de koppeling van verschillende algoritmen aan elkaar, en het voeden van algoritmen met gegevens die zijn verkregen door *enabling technologies*, zoals sensoren of het *internet of things*. Daardoor wordt niet alleen de kenbaarheid nog verder bemoeilijkt, maar kunnen er ook heel veel vragen opkomen rondom aansprakelijkheid en verantwoordelijkheid voor de uiteindelijk genomen besluiten. Het laatste kenmerk – waarschijnlijkheid – houdt in dat een algoritme is gebaseerd op statistische overwegingen (WRR, 2016: 34). Dit betekent dat het algoritme uitspraken doet over hoe waarschijnlijk een bepaalde uitkomst is op basis van profielvorming en ontdekte patronen en correlaties. Daarmee verschillen *machine-learning*-algoritmen van traditionele systemen voor beslissingsondersteuning of besluitvorming. Het informatiesysteem van DUO bijvoorbeeld bepaalt of een student studiefinanciering kan krijgen op basis van gegevens over die specifieke student. Algoritmische systemen zoals SyRI geven aan hoe waarschijnlijk het is dat iemand fraude pleegt op basis van gegevens over de groep waarin de persoon wordt geplaatst (profielvorming) en legt daarmee een heel andere basis onder besluitvorming dan in het verleden gebruikelijk was.³

De hierboven genoemde voorbeelden laten bovendien zien dat het bij het gebruik van algoritmen – net als bij het gebruik van andere ICT-vormen – niet alleen gaat om de kenmerken van dit instrument als zodanig. Er vindt ook een proces van organisatorische verandering rondom het gebruik van dit instrument plaats. Daarom spreken we, net als in eerdere analyses van computerisering (Kling, 2006) en informatisering (Hudson, 1999), van een “algoritmisering” van de organisatie: een organisatie reorganiseert de processen rondom het gebruik van algoritmes en is

³ De bespreking van het verschil tussen besluitvorming op basis van strikte als-dan-logica versus besluitvorming op basis van waarschijnlijkheden gebaseerd op gevonden correlaties is een onderwerp op zich dat we binnen het kader van dit preadvies niet kunnen uitwerken. Wederom biedt het werk van Fry (2018) een helder en toegankelijk overzicht van deze verschuiving in redeneerpatronen.

steeds sterker afhankelijk van deze systemen voor besluitvorming en uitvoering van het werk (Meijer & Grimmelikhuijsen, 2020). Dit proces van organisatieverandering beïnvloedt niet alleen de organisatie zelf maar ook de relatie met de omgeving en daarmee de legitimiteit van de organisatie. In de volgende paragraaf geven wij aan hoe we vanuit de bestuurswetenschap naar deze legitimiteit kijken.

3. Legitimiteit

In de bestuurswetenschap is legitimiteit een cruciaal begrip waarbij het uiteindelijk gaat om het accepteren van het gezag van het bestuur. Het gaat bij legitimiteit om een geïnternaliseerd gevoel van het willen gehoorzamen aan autoriteit zonder dat er daadwerkelijke dwang wordt uitgeoefend (Lipset, 1959; Tyler, 1997). In dit preadvies volgen we de veel gebruikte definitie van Suchman (1995, 574): "*Legitimacy is a generalized perception or assumption that the actions of an entity are desirable, proper, or appropriate within some socially constructed system of norms, values, beliefs, and definitions*". Deze definitie maakt duidelijk dat het perspectief van de burger centraal staat in het bestuurswetenschappelijk perspectief op legitimiteit.

Hoe komt legitimiteit dan tot stand? Om dit te begrijpen grijpen wij als bestuurswetenschappers niet terug op juridische begrippen als legaliteit en proportionaliteit, maar maken we gebruik van het klassieke model van de politicoloog Easton (1965) over de werking van het politieke systeem in zeer algemene zin. Easton laat zien dat het bij het politieke systeem in fundamentele zin gaat om het omzetten van input (preferenties van burgers) in output (beleid). Deze omzetting gebeurt in overheidsorganisaties via organisatorische processen (throughput). Scharpf (1999) en Schmidt (2013) laten zien hoe dit model kan worden gebruikt om de verschillende routes naar legitimiteit te begrijpen. Scharpf (1999) betoogt dat het bij input-legitimiteit gaat om het accepteren van gezag op basis van een correct democratisch proces met ruimte voor een open debat en correct verlopen verkiezingen en bij output-legitimiteit om het accepteren van autoriteit op basis van de resultaten die door overheden worden gerealiseerd zoals veiligheid, welvaart, vrede. Schmidt (2013) voegt hieraan toe dat throughput-legitimiteit begrepen moet worden als een aparte route: hierbij gaat het om het correct vertalen van de input in beleidsprocessen.

Deze drie routes zullen wij gebruiken om zowel de bedreigingen voor de legitimiteit voor het algoritmisch bestuur in kaart te brengen als inzicht te bieden in de strategieën om de legitimiteit te versterken. Daarbij willen we benadrukken dat we deze routes niet tegenover elkaar plaatsen maar beschouwen als aanvullende mechanismen: de resulterende legitimiteit van het bestuur ontstaat door de combinatie van de drie verschillende routes.

De klassieke route naar legitimiteit verloopt via de input-legitimiteit. Scharpf (1999: 7-21) geeft aan dat het hierbij gaat om de mate waarin het startpunt van overheidsprocessen overeenkomt met de preferenties van burgers. Democratische processen vormen daarmee de kern van input-legitimiteit (zie ook: Curtin & Meijer, 2006; Pogrebinschi & Ryan, 2018). Het gaat hierbij allereerst om de kwaliteit van de indirecte democratie ofwel het functioneren van het systeem van verkiezingen en van de volksvertegenwoordiging. Het basale idee is dat eerlijke verkiezingen en een goed functionerende volksvertegenwoordiging bijdragen aan de legitimiteit van het politieke systeem. Daarnaast is ook de directe democratie ofwel de participatie van burgers in processen die hen direct aangaan van belang. Het idee is dat betere participatiemogelijkheden de legitimiteit van beleid versterken. Op basis van deze route stellen we dat de legitimiteit van algoritmisch bestuur toeneemt naarmate de preferenties van burgers via democratische processen beter zijn vertaald in het ontwerp en het gebruik van een algoritme door een overheidsorganisatie.

Zoals hiervoor aangegeven heeft Scharpf (1999) op basis van zijn analyses van de Europese Unie hieraan een andere route naar legitimiteit toegevoegd: de output-legitimiteit. Deze vorm van legitimiteit gaat uiteindelijk om het vermogen van het politieke systeem om problemen van burgers op te lossen en wenselijke uitkomsten te genereren (zie ook: Curtin & Meijer, 2006; Gustavsen,

Pierre & Røiseland, 2014). Scharpf (1999) benadrukt dat veel politicologen vooral de kwaliteit van de democratie analyseren, maar voegt hieraan toe dat het voor burgers uiteindelijk ook veel uitmaakt wat het politieke systeem nu oplevert. De EU, zo geeft hij aan, heeft daarom een bepaalde legitimiteit door haar bijdrage aan vrede en veiligheid in Europa. Dezelfde argumentatie kan worden gebruikt om te kijken naar andere politieke systemen. Het geïnternaliseerde gevoel van het willen gehoorzamen aan gezag hangt dan af van wat een gezaghebbend instituut uiteindelijk oplevert. Op basis van deze route stellen we dat de legitimiteit van algoritmisch bestuur toeneemt naarmate de uitkomsten van het gebruik van een algoritme meer bijdragen aan de realisatie van waarden die door burgers als belangrijk worden beschouwd.

Met deze twee routes naar legitimiteit hebben we nog geen volledig beeld. Schmidt (2013) geeft aan dat ook de throughput – de wijze waarop preferenties van burgers worden vertaald in beleid – belangrijk is voor het geïnternaliseerde gevoel van het willen gehoorzamen aan autoriteit. Zij spreekt hierbij over de ‘black box’ van de overheid – de ruimte tussen input en output – die vaak wordt genegeerd door politicologen. Zij geeft aan dat de correctheid van de throughput maar ook de transparantie ervan, de openheid voor participatie en de verantwoording over organisationele processen cruciaal zijn voor de legitimiteit van het politieke systeem (Schmidt & Wood, 2019). Op basis van deze route stellen we dat de legitimiteit van algoritmisch bestuur toeneemt naarmate de wijze waaróp via het algoritme uitkomsten worden gerealiseerd overeenkomt met eisen die burgers, volksvertegenwoordigers en rechtsstatelijke instituties hieraan stellen.

Deze drie routes naar legitimiteit kunnen nu worden gebruikt om systematisch te analyseren welke voorwaarden er zijn voor de legitimiteit van algoritmisch bestuur; van daaruit kan worden beredeneerd welke bedreigingen er kunnen bestaan. Daarbij willen we opmerken dat naar dit onderwerp nog nauwelijks empirisch onderzoek is gedaan en dat we daarom op basis van eerder onderzoek aan willen geven wat mogelijke bedreigingen zouden kunnen zijn. Deze bespreking moet daarmee ook worden opgevat als een aanzet tot een agenda voor empirisch onderzoek waarin deze verschillende mogelijke bedreigingen worden getoetst.

Tabel 1. Routes naar de legitimiteit van algoritmisch bestuur

Route	Legitimiteit van algoritmisch bestuur
Input-legitimiteit	De legitimiteit van algoritmisch bestuur neemt toe naarmate de preferenties van burgers via democratische processen beter zijn vertaald in het ontwerp en het gebruik van het algoritme.
Throughput-legitimiteit	De legitimiteit van algoritmisch bestuur neemt toe naarmate de wijze waaróp via het algoritme uitkomsten worden gerealiseerd overeenkomt met eisen die burgers, volksvertegenwoordigers en rechtsstatelijke instituties hieraan stellen.
Output-legitimiteit	De legitimiteit van algoritmisch bestuur neemt toe naarmate de uitkomsten van het gebruik van een algoritme meer bijdragen aan de realisatie van waarden die door burgers als belangrijk worden beschouwd.

4. Bedreigingen voor de legitimiteit van het algoritmisch bestuur

In deze paragraaf komt de eerste centrale vraag van het preadvies aan de orde: op welke manier kan het gebruik van algoritmen door overheidsorganisaties de legitimiteit van deze organisaties bedreigen?

4.1. Bedreigingen voor de input legitimiteit: ondemocratisch bestuur

Een bedreiging van de input-legitimiteit van bestuur ontstaat doordat de relatie tussen het politieke mandaat – de richting die door politiek verantwoordelijken wordt gegeven aan de uitvoerende overheidsorganisatie – en de inzet van algoritmen in het bestuur onduidelijk is: het overheidsbestuur is dan ondemocratisch. In de bestuurswetenschap is er veel aandacht voor de verbinding tussen politiek en bestuur, waarbij als groot risico wordt benoemd dat het bestuur los komt te staan van de politieke verantwoordelijken (Demir & Nyhan, 2008; Overeen & Rutgers, 2003). Het kernidee is dat in deze verbinding de vertaling plaatsvindt van de preferenties van burgers naar bestuurlijke actie: een meerderheid in de volksvertegenwoordiging resulteert in steun voor een politiek verantwoordelijke, die vervolgens richting geeft aan de uitvoering van overheidsbeleid. Door het technologisch complexe karakter van algoritmen bestaat echter het risico dat hier geen adequate vertaling plaatsvindt, maar algoritmen alleen op basis van bestuurlijke overwegingen vorm krijgen en niet op basis van een politiek proces. In haar analyse van hulpverlening aan arme mensen in de samenleving geeft Eubanks (2017: 197) aan dat bij de ontwikkeling van algoritmen met verstrekkende gevolgen voor burgers cruciale politieke debatten over op welke wijze steun verleend diende te worden aan armen simpelweg niet hadden plaatsgevonden. Meer specifiek kunnen we dit algemene risico duiden aan de hand van drie specifieke bedreigingen.

Een eerste bedreiging is dat politiek geladen beslissingen worden genomen door ontwikkelaars van algoritmen. In zijn klassieke werk over de betekenis van informatiesystemen voor juridische praktijken in de publieke sector geeft Lessig (1999) al aan dat in computerprogramma's impliciet juridische eisen vorm krijgen en dat het gebruik van deze programma's gevolgen heeft voor de beslissingen van het bestuur. 'Code is Law,' noemt hij dit, en dit betekent dat de ontwikkelaar de rol van regelgever aanneemt. Tegelijkertijd zijn degenen die de computerprogramma's ontwikkelen of deze ontwikkeling technisch aansturen zich vaak weinig bewust van het feit dat de technische regels die zij programmeren een politiek-bestuurlijke betekenis hebben (Bovens e.a., 2018; Van Eck, 2018). De beleids- en beslissingsvrijheid van een overheidsorganisatie wordt nader ingevuld aan de hand van algoritmische regels. Zij richten zich met name op de instrumentele rationaliteit – het realiseren van doelstellingen – en zijn zich er niet van bewust dat ze daarmee eigenlijk een regelgevende rol hebben omdat zij de facto wettelijke regels maken.

Een tweede bedreiging is dat er een gebrek aan politieke toezicht op het ontwerp van algoritmen bestaat als gevolg van technologische complexiteit (Meijer, Ruijter & Dekker, 2020; Van Est e.a., 2020). Zowel de ministers die uiteindelijk verantwoordelijk zijn voor de algoritmen als de volksvertegenwoordigers die hen daarop kunnen aanspreken hebben vaak zeer beperkte kennis van algoritmen. Dit gebrek aan kennis maakt het voor hen zeer lastig om te controleren of de algoritmen die worden ontwikkeld wel voldoen aan de preferenties van burgers zoals deze via het proces van verkiezingen naar voren zijn gebracht en die worden vertegenwoordigd door politici via democratische delegatie (Strøm, 2000). Burgers kunnen bijvoorbeeld volksvertegenwoordigers kiezen omdat ze willen dat er goed toezicht is op een eerlijke en correcte bijstandsverlening, maar als dit proces plaatsvindt via algoritmen kunnen volksvertegenwoordigers deze taak niet waarmaken.

Een derde bedreiging is een beperkte participatie van betrokkenen in het ontwerp en het opstellen van richtlijnen voor de ontwikkeling en het gebruik van algoritmen door overheidsorganisaties. Op beleidsterreinen zoals de ruimtelijke ordening is de participatie van burgers in besluitvorming formeel georganiseerd en zijn er inspraakavonden. Ook in andere publieke sectoren bestaan er

medezeggenschaps- en cliëntenraden die ervoor zorgen dat burgers kunnen participeren in besluitvorming die hen treft (Hendriks, 2012; Michels & De Graaf, 2017). Het gebruik van algoritmen kan allerlei groepen van burgers direct treffen – denk aan het algoritme SyRI voor de detectie van uitkeringsfraude (Van Schendel, 2019) –, maar door het technische karakter van de ontwikkeling en het gebruik van het systeem komt de mogelijkheid van participatie door burgers vaak niet eens ter sprake. Hierdoor ontbreekt de mogelijkheid om deze systemen via directe participatie beter af te stemmen op de preferenties van burgers.

4.2. Bedreigingen voor throughput-legitimiteit: onrechtmatig bestuur

Een bedreiging van throughput-legitimiteit ontstaat doordat de wijze waarop de besluitvorming met behulp van algoritmen plaatsvindt niet wordt getoetst aan eisen die hieraan vanuit het recht kunnen worden gesteld. Er is dan sprake van onrechtmatig bestuur. Zo kent het bestuursrecht in de algemene beginselen van behoorlijk bestuur een belangrijke set aan regels die zien op de normering van overheidsbesluiten. Deze normen gaan ook op voor algoritmisch genomen besluiten, maar het is de vraag of normen zoals het motiveringsbeginsel of het zorgvuldigheidsbeginsel voldoende getoetst kunnen worden wanneer een besluit grotendeels is genomen door een algoritme. Dit komt doordat er door het gebruik van complexe algoritmen fundamentele veranderingen plaatsvinden in de aard van overheidsbesluitvorming. De technologiefilosoof Van den Hove (1998) spreekt hier van het afnemen van de epistemische ruimte: de besluitvormer moet vertrouwen op een instrument dat hij/zij zelf niet meer helemaal kan doorgronden. Hoewel we dit in het dagelijks leven allemaal doen (wie weet hoe zijn of haar mobiele telefoon werkt?), heeft dit voor overheidsbesluitvorming als gevolg dat besluitvorming op basis van algoritmen moeilijk kan worden gemotiveerd en getoetst. Daarbij treedt wederom een aantal bedreigingen van de legitimiteit op.

Een eerste bedreiging komt voort uit de beperkte transparantie van algoritmen. De beperkte transparantie is een belangrijk punt in (internationale) discussies over algoritmen (Lepri et al. 2018; Kroll et al. 2017; Burrell 2016; Diakopoulos 2016; De Fine Licht & De Fine Licht, 2020). Van Eck (2018) laat zien dat beslisregels in algoritmen en ook de aannamen van programmeurs vaak onzichtbaar zijn voor zowel de persoon die met behulp van een algoritme een besluit neemt als voor controlerende instanties. Ook artikel 22 van de in 2018 in werking getreden Algemene Verordening Persoonsgegevens (AVG) benadrukt de “uitlegbaarheid” van algoritmische beslissingen. Kulk, Van Deursen e.a. (2020: 5) benadrukken dat door gebrek aan transparantie van algoritmische beslissingen het recht op rechtsbescherming in het gedrang kan komen. De ondoorzichtigheid van complexe systemen is een belangrijk punt in discussies over informatiesystemen in de publieke sector (Meijer, 2009) en specifiek ten aanzien van algoritmen wordt benadrukt dat door *machine learning* de besluitvormingsregels van het algoritmen evolueren en daardoor ook niet meer bekend zijn bij de ontwerpers (Lepri et al. 2018; Kroll et al. 2017; Burrell 2016; Diakopoulos 2016). Ook geldt dat algoritmen vaak weinig transparant zijn doordat ze zijn ontwikkeld door commerciële partijen die over intellectuele-eigendomsrechten beschikken die in de weg kunnen staan aan de openbaarmaking van de code (Mittelstadt et al. 2016). Daaraan kan worden toegevoegd dat het gebrek aan transparantie ook kan gaan over de wijze waarop een organisatie met een algoritme omgaat en welke regels er gelden ten aanzien van het al dan niet volgen van het advies van een algoritme.

Een tweede veelbesproken bedreiging in de literatuur is de inbreuk die algoritmen kunnen maken op de privacy van burgers, in het bijzonder hun recht op persoonsgegevensbescherming (Young, Katell and Krafft, 2019; Kulk, Van Deursen e.a., 2020). Ook hier vormt de Algemene Verordening Gegevensbescherming (AVG) een belangrijk juridisch ankerpunt (Brkan, 2019). De toepassing van algoritmen vergt dat er veel data uit verschillende datasets worden gecombineerd en op geavanceerde wijze worden verwerkt om bijvoorbeeld risicoscores uit te rekenen. Veel van deze data zijn nooit verzameld met dit doel. Daarbij geldt bovendien dat de combinaties van verschillende datasets kan leiden tot nieuwe inzichten over individuele personen (Kulk, Van

Deursen e.a., 2020: 5). Ook is voor individuen vaak onbekend welke data nu precies op welke manier worden verwerkt. Hierbij geldt dat de privacy van burgers zelfs kan worden geschaad als er geanonimiseerde data worden gebruikt omdat de combinatie van data uit verschillende sets weer kan leiden tot de unieke identificatie van individuen.

Een derde bedreiging is meer in algemene zin een gebrekkige vertaling van algemene en specifieke juridische eisen in het ontwerp en gebruik van algoritmen. De juridische eisen – met name de eisen op het gebied van fundamentele rechten en andere publieke waarden, zoals het recht op non-discriminatie en het recht op rechtsbescherming (Kulk, Van Deursen e.a., 2020) – zijn van groot belang voor het rechtmatig functioneren van algoritmes. Het ontwerpen van algoritmen vindt echter plaats door technische experts die – zoals we hierboven al aangaven – vaak een beperkte kennis hebben van juridische regels. Daarmee ontstaat het risico dat een algoritme wordt ontwikkeld dat goed functioneert volgens technische standaarden maar dat niet voldoet aan de bredere juridische eisen – bijvoorbeeld op het gebied van mensenrechten (Livingston & Risse, 2019) – die hieraan kunnen worden gesteld. Een complicerende factor is daarbij dat juridische eisen vaak niet eenduidig zijn, waardoor omzetting in een algoritmische regel complex of misschien in bepaalde gevallen onmogelijk is.

Een vierde bedreiging is het verdampen van verantwoordelijkheid in de complexe relaties die ontstaan rondom het gebruik van algoritmen (Meijer, 2009; Frissen e.a., 2019: 7; De Fine Licht & De Fine Licht, 2020). Kulk, Van Deursen e.a. (2020: 5) schrijven: *“Van belang is verder dat de verantwoordelijkheidsvragen toenemen en complexer te beantwoorden zijn naarmate de samenleving verder gedigitaliseerd raakt en systemen in toenemende mate met elkaar interacteren.”* Men zou zeggen dat degene die de algoritmen gebruikt verantwoordelijk blijft, maar dit wordt ingewikkelder als men weet dat deze het algoritme niet volledig kan doorgronden. De vraag ontstaat dan of niet de ontwikkelaar van het systeem verantwoordelijk blijft. Tegelijkertijd geldt dat het systeem zich verder ontwikkelt op basis van processen van *machine learning*. Dan geldt misschien dat degenen die het algoritme ‘trainen’ verantwoordelijk blijven, of degenen die de datasets beheren waarmee het algoritme wordt getraind, of een combinatie daarvan. Gezien deze complexiteit wordt soms zelfs gesteld dat de algoritmen als eigenstandige actoren moeten worden gezien en daarmee zelf verantwoordelijk zijn, maar het is moeilijk om daaraan juridisch op een goede manier vorm te geven. Het risico bestaat dat in deze complexe verhoudingen uiteindelijk niemand meer echt verantwoordelijk kan worden gehouden (Bovens, 1998; Meijer, 2009).

4.3. Bedreigingen voor de output-legitimiteit: wanpresterend bestuur

Een bedreiging voor de output-legitimiteit ontstaat wanneer het gebruik van een algoritme niet leidt tot de realisatie van waarden die door burgers als belangrijk worden beschouwd. Er is dan sprake van ‘wanpresterend bestuur’: het bestuur levert niet de uitkomsten op die door burgers worden verwacht (Scharpf, 1999). Daarbij zal de legitimiteit vooral bedreigd worden wanneer het gebruik van algoritmen rechtmatig verloopt maar toch resulteert in uitkomsten die door burgers als wanprestatie worden gezien, zoals discriminatie of het ontbreken van menselijk contact.

Een eerste bedreiging is hierbij dat er een bias optreedt in de besluitvorming wanneer deze wordt ondersteund door algoritmische systemen. Kulk, Van Deursen e.a. (2020: 6) schrijven: *“Discriminatie-risico’s kunnen zich ... concreet voordoen als vooroordelen of onaanvaardbare stereotypen via de programmeur(s) van een algoritme of via anderen die betrokken zijn bij de ontwikkeling van het algoritme (bewust of onbewust) een weerslag krijgen op het algoritme.”* In de literatuur worden onder andere de volgende soorten van *bias* genoemd (Jackson, 2018; Williams, Brooks & Shmargad, 2018): focus op specifieke doelgroepen (soms op basis van etnische profilering), focus op specifieke gebieden (waar soms bepaalde groepen van mensen wonen) en focus op *past performance* in plaats van de huidige en toekomstige situatie (waardoor demografische veranderingen onvoldoende worden meegenomen). Deze bias kan ontstaan door gebruik van vertekende data waarmee het algoritme wordt getraind (waarbij het vaak gaat om data waar al een bias in aanwezig was), gebruik van selectieve data (waarbij de bias al optreedt bij

het selecteren van data en vervolgens doorwerkt in het 'trainen' van het algoritme) en incorrecte analyses op basis van de data (waarbij bepaalde patronen verkeerd worden geïnterpreteerd). Deze concrete bedreiging wordt veel besproken in de literatuur en komt ook steeds aan de orde wanneer het gaat over algoritmen om fraudepatronen met uitkeringen te identificeren, zoals SyRI, of systemen die worden ingezet voor de planning van overheidsactiviteiten, zoals CAS (Van Schendel, 2019).

Een tweede bedreiging voor de legitimiteit is dat het algoritme de kwaliteit van menselijke contacten en van menselijke inbreng in besluitvorming ondermijnt (WRR, 2016: 131). In de meest vergaande vorm vervangt het algoritme immers de mens en heeft een burger alleen met een algoritme te maken en niet met een mens. Dit geldt nu bijvoorbeeld al bij beslissingen die massaal worden genomen, zoals bij de studiefinanciering of verkeersboetes (Van Eck, 2018), al gaat het daarbij vooral om regelgebaseerde en niet zozeer om *machine-learning*-algoritmen. Dit leidt ertoe dat burgers zich letterlijk geplaatst zien tegenover een machine. Ook bij het gebruik van algoritmes op de achtergrond kan gelden dat de rol van de menselijke besluitvormer wordt gereduceerd tot het toepassen van het advies van het algoritme. Daarbij treedt het risico van *automation bias* op: de mens vertrouwt op het algoritme, zelfs als dit het duidelijk bij het verkeerde eind heeft (Goddard et al. 2011).

Een derde bedreiging voor de output-legitimiteit is dat de inzet van algoritmen gepaard gaat met hoge kosten maar niet leidt tot de beloofde verbeteringen. De verwachtingen van de inzet van algoritmen zijn hoog, vooral als het gaat om de effectiviteit en de efficiency van overheidsprocessen, maar het harde bewijs voor de bijdrage daaraan wordt niet altijd duidelijk geleverd. Vaak lijkt er eerder sprake van het volgen van een trend en een groot geloof in technologische mogelijkheden dan dat er sprake is van een heldere business case. In de literatuur wordt overigens veel meer ingegaan op de risico's voor de legitimiteit die verbonden zijn aan bias en de daaraan verbonden ongewenste effecten dan op het risico van de verspilling van publiek geld doordat gewenste effecten niet worden gerealiseerd.

Een vierde bedreiging voor deze vorm van legitimiteit is dat de effecten van het gebruik van een specifiek algoritme in de loop van de tijd verschuiven. Het kan bijvoorbeeld zo zijn dat er een bias ontstaat omdat het algoritme leert op basis van bepaalde datasets. Ook kan het zijn dat de interacties met andere gebruikspatronen en datasets leiden tot veranderende uitkomsten. Bij die gebruikspatronen kan het ook gaan om reacties in de samenleving op het gebruik van algoritme. Denk bijvoorbeeld aan de manieren waarop automobilisten elke keer weer proberen om snelheidscontroles te omzeilen of burgers die de controles van de Belastingdienst proberen te ontlopen. Zo kunnen ook manieren worden gevonden om de algoritmes te ontlopen.

4.4. Overzicht van de bedreigingen van de legitimiteit

Op basis van deze bespreking van de verschillende routes naar legitimiteit presenteren we nu het antwoord op de eerste deelvraag – op welke manier kan het gebruik van algoritmen door overheidsorganisaties de legitimiteit van deze organisaties bedreigen? – in de onderstaande tabel:

Tabel 2. Bedreigingen voor de legitimiteit van algoritmisch bestuur

Bedreiging	Mechanismen
Ondemocratisch bestuur	<ul style="list-style-type: none"> • Politieke besluiten door ontwikkelaars van algoritmen • Gebrek aan politiek toezicht op het ontwerp van algoritmen • Beperkte participatie in het ontwerp van algoritmen
Onrechtmatig bestuur	<ul style="list-style-type: none"> • Beperkte transparantie van algoritmen • Inbreuk op de privacy van burgers • Gebrekkige vertaling van juridische eisen in algoritmen • Verdampen van verantwoordelijkheden rondom algoritmen
Wanpresterend bestuur	<ul style="list-style-type: none"> • Bias in algoritmische systemen • Algoritmen beperken het menselijk contact • Algoritmische systemen zijn kostbaar maar leveren weinig op • Baten en lasten van algoritme verschuiven in de tijd

De tabel laat zien dat er een groot aantal verschillende bedreigingen van de legitimiteit van algoritmisch bestuur bestaat. Deze bedreigingen zijn veelal nieuw en bouwen voort op de bedreigingen van bureaucratische organisaties in algemene zin. Daarbij gelden immers ook de algemene bedreigingen dat de bureaucratie niet wordt aangestuurd door de politiek maar haar eigen logica heeft (gebrek aan input-legitimiteit), dat de bureaucratie weinig transparant is en het niet helder is waarop precies bepaalde uitkomsten van besluitvormingsprocessen zijn gebaseerd (gebrek aan throughput-legitimiteit) en dat de bureaucratie niet de waarden oplevert die burgers wensen (gebrek aan output-legitimiteit). Deze algemene punten worden echter versterkt door het gebruik van algoritmen met een hoge mate van complexiteit, onkenbaarheid, afhankelijkheid en waarschijnlijkheid. Deze kenmerken leiden tot nieuwe problemen bij het politieke toezicht op de technologie, nieuwe problemen bij het helder verantwoorden van adviezen en besluiten en nieuwe problemen bij het produceren van wenselijke uitkomsten.

Voor de bedreigingen geldt ook dat we moeten begrijpen dat legitimiteit is gebaseerd op percepties van burgers. Voor de legitimiteit is het niet zozeer van belang of het algoritme echt al deze beperkingen heeft; het gaat er uiteindelijk om of burgers het inzetten van algoritmes zo percipiëren. Dit betekent dat de bedreigingen zowel te maken kunnen hebben met het algoritme zelf en de wijze waarop een algoritme door een overheidsorganisatie wordt gebruikt, als met de beeldvorming die hierover plaatsvindt. Om legitimiteit te versterken is het daarom nodig om zaken goed op orde te hebben én dit via een helder verhaal overtuigend te kunnen overbrengen. In de volgende paragraaf gaan we in op verschillende manieren om dit te kunnen doen.

5. Strategieën om de legitimiteit te versterken

In de vorige paragraaf hebben we de problemen – de bedreigingen voor de legitimiteit van algoritmisch bestuur – systematisch in kaart gebracht. In deze paragraaf verkennen we oplossingsrichtingen en staat de tweede deelvraag centraal: welke acties zijn nodig om de legitimiteit van het gebruik van algoritmen door overheidsorganisaties te borgen? We bespreken strategieën om de legitimiteit te versterken aan de hand van de input-, throughput- en output-legitimiteit.

5.1. Versterken van de input-legitimiteit: democratisch ontwikkelde algoritmen

Bij het versterken van de input-legitimiteit gaat het om interventies om de verbinding tussen democratie – breed gezien als het vertalen van de preferenties van burgers in politieke richtingen – en bestuur – het geheel aan uitvoerende overheidsorganisaties – te versterken. Het is de ambitie

om het democratisch gehalte van bestuur te waarborgen; centraal staat hierin de verbinding tussen politiek verantwoordelijken en bestuur. Dit raakvlak tussen ambtelijke actie en politieke wilsexpressie dient op verschillende manieren te worden versterkt om ervoor te zorgen dat er geen sprake is van technocratisch, maar van democratisch bestuur.

Een eerste strategie om de input-legitimiteit van algoritmisch bestuur te versterken betreft het versterken van politieke gevoeligheid van de ambtelijke aansturing van het ontwerp van algoritmen. De politieke gevoeligheid van ambtenaren betreft het vermogen om onderscheid te kunnen maken tussen situaties waarin ambtelijk besluitvorming voldoet en situaties waarbij politieke besluitvorming nodig is ('t Hart & Wille, 2006). Ambtelijke besluitvorming voldoet wanneer situaties gelden als routineus en kan worden ingegrepen op basis van de bestaande kaders, die eerder zijn afgestemd via politieke besluitvorming. Politieke besluitvorming is echter nodig wanneer het gaat om zaken die een nieuwe afweging van waarden vergt. Bij de ontwikkeling van systemen voor *predictive policing* zijn vragen over bias bijvoorbeeld zeer gevoelig en dienen deze te worden afgestemd met de politiek. Voor de ambtelijke aansturing van ontwerpprocessen is het belangrijk om te kunnen identificeren welke aspecten van algoritmen dusdanig gevoelig zijn dat deze – op begrijpelijke wijze – worden voorgelegd aan politieke besluitvormers. Frissen e.a. (2019: 3) geven aan dat een algemeen normenkader dat is geschreven voor dataspecialisten – en dus niet in juridisch jargon – hierbij behulpzaam kan zijn.

Een tweede strategie betreft een interventie aan de andere kant van de politiek-ambtelijke dichotomie: het versterken van het vermogen tot politieke toezicht op algoritmen (Van Est e.a., 2020; Frissen et al., 2019: 3, 4). De politieke betrokkenheid bij een systeem als SyRI was lang zeer beperkt, omdat de inrichting van het systeem werd gezien als een uitvoeringsissue en de politiek gevoelige aspecten onvoldoende werden geïdentificeerd. Belangrijk is dat de capaciteiten van politiek verantwoordelijken zoals ministers, gedeputeerden en wethouders wordt versterkt, zodat zij in staat zijn om politiek gevoelige issues te identificeren zoals privacy, discriminatie of eigenaarschap over data en om daarop te sturen (Van Est et al., 2020). Dit vergt enige kennis van technische processen en ook een ondersteuning die erop gericht is om het politieke toezicht mogelijk te maken. Ook het vermogen van de volksvertegenwoordiging om te sturen op publieke waarden bij onderwerpen met hoge technische complexiteit is hierbij van belang (Meijer, Ruijter & Dekkers, 2020); denk bijvoorbeeld aan het tijdig onderkennen van zorg over gezondheid rondom de implementatie van 5G-netwerken. Dit vergt kennisopbouw en een adequate ondersteuning van de volksvertegenwoordiging op dit terrein.

Een derde strategie heeft te maken met directe participatie van burgers in aanvulling op het toezicht door hun politieke vertegenwoordigers. De redenering is hierbij grotendeels hetzelfde als bij participatie in ruimtelijke plannen of cliëntenparticipatie in onderwijs, gezondheidszorg of huisvesting (Michels & De Graaf, 2010). Via participatie in het ontwerp van algoritmen kunnen burgers direct aangeven waar gevoelige issues liggen en welke aandachtspunten hierbij van belang zijn. Het delen van code via platforms zoals Github, zoals recentelijk is gebeurd bij het ontwikkelen van de CoronaMelder, kan hieraan bijdragen. Daarbij het ook gaan om participatie in het monitoren van de effecten van het gebruik van algoritmen, zodat burgers mede aan kunnen geven waarop deze monitoring zich moet richten. Dan kunnen burgers bijvoorbeeld aangeven welke privacyaspecten moeten worden gewaarborgd bij het gebruik van een systeem zoals SyRI (Van Schendel, 2019).

5.2. Versterken van de throughput-legitimiteit: rechtmatig bestuur

Het versterken van de throughput-legitimiteit vraagt om verschillende acties die te maken hebben met het verhelderden van de wijze waarop de preferenties van burgers worden vertaald in algoritmisch bestuur. Het is de ambitie om de legitimiteit te versterken door de rechtmatigheid van bestuur te waarborgen. De 'black box' van bestuurlijke actie dient gericht te worden geopend om te laten zien dat wat er in deze 'black box' gebeurt correct is. Wederom gelden wettelijke kaders en met name de AVG hier als uitgangspunt en deze wettelijke kaders bieden ook nu al handvatten voor het versterken van de throughput-legitimiteit.

Een eerste strategie om de throughput-legitimiteit te versterken betreft het vergroten van de transparantie van algoritmisch bestuur (De Fine Licht & De Fine Licht, 2020). Een eerste stap is hierbij transparantie over het gebruik van algoritmen – welke algoritmen worden waarvoor gebruikt? –, maar dit is niet afdoende.⁴ In de literatuur over algoritmen is de transparantie ervan wellicht het meest besproken punt: benadrukt wordt dat de uitlegbaarheid en toegankelijkheid moet worden vergroot (Lepri et al. 2018). Uitlegbaarheid betekent dat – ook als een *machine-learning*-algoritme wordt gebruikt bij de besluitvorming – duidelijk gemaakt moet worden dat de substantiële redenen voor een besluit helder en correct zijn (Tutt 2017). Toegankelijkheid betekent dat zowel de beslisregels als de gebruikte data vrij worden gegeven (Mittelstadt et al. 2016). De gemiddelde burger zal weinig kunnen met deze toegankelijkheid, maar externe experts zullen deze wel kunnen benutten voor een kritische analyse. Hieraan willen wij toevoegen dat de uitlegbaarheid en toegankelijkheid niet alleen dienen te gaan over de techniek van het algoritme, maar ook over de wijze waarop dit wordt ingezet in de organisatie. De Fine Licht & De Fine Licht (2020) benadrukken dat het erom gaat dat duidelijk is welk besluit is genomen, op basis van welke argumenten en wie ervoor verantwoordelijk is, en Young, Katell & Krafft (2019: 2) geven aan dat er manieren moeten worden gevonden waarom algoritmische systemen 'leesbaar' zijn voor beleidsmakers en stakeholders. De verwachting is dat een grotere toegankelijkheid mogelijkheden creëert voor externe partijen om het algoritme te controleren en de organisatie ter verantwoording te roepen over het algoritme. Het feit dat deze mogelijkheden bestaan draagt bij aan de legitimiteit van algoritmisch bestuur.

Een tweede strategie betreft het uitvoeren van een Data Protection Impact Assessment (DPIA).⁵ Een DPIA is een organisatorisch instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen zodat er betere besluiten kunnen worden genomen over de vraag of en hoe een algoritme kan worden ingezet (Bu-Pasha, 2020). Het uitvoeren van een DPIA is overigens vaak geen vrije keuze: onder de Algemene verordening gegevensbescherming (AVG) zijn overheidsorganisaties verplicht een DPIA uit te voeren wanneer de organisaties *"systematisch en uitgebreid persoonlijke aspecten evalueert gebaseerd op geautomatiseerde verwerking, waaronder profiling, en daarop besluiten baseert die gevolgen hebben voor mensen"* en/of *"op grote schaal bijzondere persoonsgegevens verwerkt of strafrechtelijke gegevens verwerkt"*.

Een derde strategie betreft het invoeren van een mensenrechten-impact-assessment of zelfs een nog bredere, algemene juridische toets op algoritmisch bestuur.⁶ Voor juristen is dit een voor de hand liggende maatregel maar dat wil niet zeggen dat dit ook altijd gebeurt. De juridische toets wordt uitgevoerd bij de planning van het gebruik van een algoritme door de overheidsorganisatie.

⁴ De gemeente Amsterdam heeft een register geopend waarin alle algoritmen die de gemeenten gebruikt zijn geregistreerd: <https://algoritmeregister.amsterdam.nl/>. Per algoritme wordt hierbij aangegeven welke data worden gebruikt, hoe deze data worden verwerkt, hoe discriminatie wordt tegengegaan, hoe mensen toezicht houden op de werking van het algoritme, welke andere risico's het gebruik van het algoritme met zich meebrengt en wat de gemeente doet om deze risico's te beperken.

⁵ Voor een heldere beschrijving van DPIA, zie: <https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia>.

⁶ Deze richting is al ingezet: het Ministerie van BZK heeft de opdracht gegeven om een mensenrechten-impact-assessment voor algoritmen te ontwikkelen. Een dergelijk instrument kan bijdragen aan het verbreden van de focus van de DPIA's.

De toets betreft een serie vragen ten aanzien van relevante juridische kaders zoals bewaring en openbaarheid van gegevens, beveiliging, etc. (zie ook: Kulk, Van Deursen e.a., 2020), maar ook ten aanzien van bredere kwesties gerelateerd aan mensenrechten. De beantwoording van deze vragen leidt tot een rapport waarin wordt gerapporteerd of het algoritme en de wijze waarop dit wordt gebruikt binnen de overheidsorganisatie voldoet aan alle juridische eisen die hieraan kunnen worden gesteld. De uitvoering van dergelijke toetsen kan mogelijk landelijk worden ondersteund door middel van een kennispunt of expertisecentrum.

Een vierde strategie betreft het expliciteren van de verantwoordelijkheden ten aanzien van algoritmisch bestuur (Busuioac, 2020). Waar liggen de verantwoordelijkheden van de bestuurlijke organisatie, van de ontwikkelaar van het algoritme, van de toeleveranciers van datasets, van degene die het algoritme onderhoudt, etc.? Bij het in gebruik nemen van een algoritme in een organisatie dient helder te worden aangegeven waar de verantwoordelijkheden liggen voor het gebruik en de uitkomsten van het algoritme en dit wordt vastgelegd in een document. Dit verhelderen vergroot de aanspreekbaarheid en verkleint de kans dat verschillende betrokkenen naar elkaar kijken en verwachten dat eisen door anderen worden verwerkt.

Een vijfde strategie is het invoeren van een onafhankelijke toezichthouder voor algoritmen in het openbaar bestuur (Tutt, 2017). Deze toezichthouder kan eenzelfde positie hebben als de Autoriteit Persoonsgegevens, maar een veel breder mandaat: er wordt niet alleen gekeken naar de behandeling van persoonsgegevens, maar ook naar allerlei andere aspecten van het correct functioneren van algoritmen in een bestuurlijke context. Deze toezichthouder kan daarmee toezien op de vorige punten – het uitvoeren van de juridische toets en het expliciteren van verantwoordelijkheden –, maar ook reageren op specifieke klachten van burgers over algoritmen bij het bestuur. Overigens adviseren Frissen e.a. (2019) tegen een afzonderlijke toezichthouder omdat het gebruik van algoritmen voorsnog beperkt is en bovendien de toezichthouder het gebruik van het algoritme altijd moet plaatsen binnen het inhoudelijke toezichtsveld. Men kan daarom stellen dat een toezichthouder specifiek voor algoritmen alleen waarde heeft wanneer deze sterk samenwerkt met inhoudelijke toezichthouders. Ook kunnen bestaande toezichthouders afdelingen oprichten die zich specifiek richten op toezicht op algoritmen binnen een specifieke sector. Daarom pleiten Kulk, Van Deursen e.a. (2020) ervoor om de werkzaamheden van allerlei bestaande actoren eerst eens goed te coördineren, of eventueel te bekijken of de toezichthoudende taak bij een van de bestaande actoren kan worden neergelegd.

5.3. Versterken van de output-legitimiteit: presterend bestuur

Het versterken van de output-legitimiteit vergt dat er veel preciezer en explicieter wordt gekeken naar de opbrengsten van het gebruik van het algoritme dan op dit moment de praktijk is. Leidt het gebruik van het algoritme in de bestuurlijke organisatie tot wenselijk uitkomsten voor de samenleving? Daarbij is het zaak om niet alleen gefocust te zijn op de belofte van de technologie, maar deze belofte kritisch te bevragen en op verschillende manieren de mogelijke onwenselijke effecten in beeld te brengen. Vervolgens dienen maatregelen te worden genomen om te waarborgen dat het gebruik van algoritmen leidt tot een optimalisering van wenselijke uitkomsten en een minimalisering van onwenselijke uitkomsten.

Een eerste strategie om de output-legitimiteit te versterken betreft het minimaliseren van bias bij het ontwikkelen van het algoritme (Baer, 2019). Om de bias in algoritmen te minimaliseren is het van belang om kritische tegendenkers vanuit diverse achtergronden in projectteams te betrekken die steeds aan kunnen geven welke vormen van bias kunnen ontstaan. Ook is het bij het gebruik van de algoritmen van groot belang om allerlei mogelijke vormen van bias te meten om te controleren dat het algoritme niet vertekent. Kulk, Van Deursen e.a. (2020: 4, 5) merken op dat, mits de bias in data en algoritmen kan worden voorkomen, het gebruik van algoritmen de mogelijkheid biedt om de non-discriminatie te versterken omdat goed-geprogrammeerde en gevalideerde algoritmen in beginsel beter dan mensen in staat om zonder aanzien des persoons een besluit te nemen. Ook geven zij aan dat het gebruik van algoritmen kan helpen om besluiten

beter af te stemmen op betrokken personen en zo kan bijdragen aan het realiseren van materiële gelijkheid.

Een tweede strategie betreft – in aanvulling op reeds bestaande kader van de AVG – het nader uitwerken van regels voor het recht op menselijk contact (zie Kulk, Van Deursen e.a., 2020: 67 voor een bespreking van dit recht op menselijk contact in de context van moderatie van platformen). Vooral in het geval van het gebruik van algoritmen die beslissingen nemen over individuele burgers is het van groot belang dat burgers voor de uitleg over een beslissing niet alleen worden verwezen naar een website maar daadwerkelijk contact kunnen krijgen met een menselijke besluitvormer (Frissen e.a., 2019: 4).⁷ Daarnaast dient wettelijk te zijn vastgelegd dat een menselijke besluitvormer het besluit van het algoritme moet kunnen heroverwegen. Dit betekent dat algoritmen expliciet *aanvechtbaar* moeten zijn (Almadal, 2019).

Een derde strategie betreft het verplichten van een kosten-/batenanalyse van algoritmen. Deze kan een onderdeel vormen van de DPIA (zie paragraaf 5.2), maar nu gaat het sterk om de uitkomsten. Het gebruik van algoritmen wordt vaak gestuurd door de grote belofte van technologie, maar het is zaak dat, voordat de algoritmen in gebruik worden genomen, een realistisch assessment plaatsvindt van deze beloften en ook van de (financiële en niet-financiële) kosten van het gebruik van het algoritme. Bij de analyse van kosten en baten dienen verschillende expertises en stakeholders te worden betrokken zodat vooral ook de mogelijke onwenselijke bijeffecten goed in beeld worden gebracht.

Een vierde en meer algemene strategie om de output-legitimiteit te versterken betreft een ethische toets op uitkomsten van het algoritme. Deze toets vormt een aanvulling op de DPIA en juridische toets die eerder zijn genoemd en richt zich specifiek op de wenselijkheid van uitkomsten van het gebruik van het algoritme. Daarbij kan bijvoorbeeld worden gedacht aan ongelijke uitkomsten voor delen van de stad bij het gebruik van het CAS voor de planning van inzet van politie of bij de inzet van SyRI voor het bestrijden van sociale zekerheidsfraude. Ook bij deze ethische toets is het van belang dat verschillende soorten experts en stakeholders worden betrokken. Gezien het feit dat het gebruik van algoritmen zich ontwikkelt over de tijd is het verstandig de ethische toets niet alleen voorafgaand aan het gebruik, maar ook meer doorlopend bij het gebruik van het algoritme uit te voeren.

Een vijfde strategie om de output-legitimiteit te versterken is het invoeren van een periodieke audit op het gebruik van algoritmen. Het doel van deze audit is om te checken of het gebruik van het algoritme nog leidt tot de gewenste uitkomsten en ongewenste uitkomsten worden vermeden. Frissen e.a. (2019: 4) pleiten voor een periodieke audit door een externe partij op onder andere de werking van de algoritmen, het dienen van het doel waarvoor ze worden ingezet, en het in acht nemen van de menselijke maat.

5.4. Overzicht van de strategieën om de legitimiteit te versterken

Op basis van deze bespreking presenteren we nu het antwoord op de tweede deelvraag – welke acties zijn nodig om de legitimiteit van het gebruik van algoritmen door overheidsorganisaties te borgen? – in de onderstaande tabel:

⁷ In allerlei initiatieven rondom *human-centered AI* komt de nadruk op de positie van de mens in relatie tot het algoritme sterk naar voren. Zie ook de focus area op dit terrein van de UU: <https://www.uu.nl/en/research/human-centered-artificial-intelligence/about-human-centered-artificial-intelligence>.

Tabel 3. Strategieën om de legitimiteit van algoritmisch bestuur te versterken

Ambitie	Strategieën
Democratisch bestuur	<ul style="list-style-type: none"> • Versterken van politieke gevoeligheid van ambtenaren die ontwerp van algoritmen aansturen • Versterken van het vermogen tot politiek toezicht op algoritmisch bestuur • Participatie in het ontwerp en het monitoren van algoritmen
Rechtmatig bestuur	<ul style="list-style-type: none"> • Transparantie van algoritmisch bestuur • Data Protection Impact Assessment • Juridische toets op algoritmisch bestuur • Verhelderen van verantwoordelijkheden bij algoritmisch bestuur • Onafhankelijke toezichthouder op algoritmen
Presterend bestuur	<ul style="list-style-type: none"> • Minimaliseren van bias • Richtlijnen voor recht op menselijk contact en aanvechtbaarheid • Kosten-/batenanalyse van het algoritme • Ethische toets op algoritmen • Periodieke audits op het gebruik van algoritmen

Deze tabel laat zien dat er een veelheid aan strategieën nodig is om de legitimiteit van algoritmisch bestuur te waarborgen door democratisch, rechtmatig en presterend bestuur te garanderen. Hierbij gaat het niet alleen om harde institutionele mechanismen, zoals het handelen in overeenstemming met wettelijke vereisten, maar ook om zachte institutionele mechanismen zoals de politieke sensitiviteit van ambtenaren die het ontwerp van algoritmen aansturen. Ook gaat het zowel om interventies binnen de organisatie zoals het vergroten van de transparantie als om externe interventies zoals het opzetten van een onafhankelijke toezichthouder op algoritmen.⁸

Naast deze specifieke punten willen we benoemen dat het in algemene zin van belang is dat er helder wordt gecommuniceerd over de wijze waarop de legitimiteit van algoritmisch bestuur wordt gewaarborgd. Legitimiteit is sterk afhankelijk van percepties van burgers en daarom dienen er niet alleen goed institutionele mechanismen te bestaan, maar dient ook helder naar buiten toe te worden aangegeven hoe deze mechanismen werken en op welke manier deze bijdragen aan de legitimiteit van algoritmisch bestuur.

⁸ Het geheel aan maatregelen dat we hebben genoemd lijkt zeer uitgebreid, maar dat is mede het resultaat van onze analytische aanpak van dit vraagstuk. We hebben specifiek aangegeven welke strategieën passen bij de verschillende bedreigingen van de verschillende vormen van legitimiteit. Bij het ontwikkelen van aanpakken kunnen waarschijnlijk verschillende strategieën gecombineerd worden. De verschillende assessments die we hebben genoemd – DPIA, juridische toets, kosten-/batenanalyse en ethische toets – kunnen bijvoorbeeld gecombineerd worden en leiden tot een brede assessment van algoritmisch bestuur. Frissen e.a. (2019: 4) spreken ook wel over een Algoritme Impact Assessment dat organisaties helpt om risico's te identificeren en te mitigeren, en na te gaan of zich nog restrisico's voordoen.

6. Conclusies

Het gebruik van algoritmen in de publieke sector is nog beperkt maar neemt snel toe en dit kan grote gevolgen hebben voor het functioneren van overheidsorganisaties (Vogl e.a., 2020). Dit gebruik van algoritmen in de publieke sector biedt potentieel allerlei mogelijkheden om de effectiviteit van taakuitvoering te versterken, maar roept, door de specifieke kenmerken van deze technologie, ook een aantal fundamentele vragen op ten aanzien van de legitimiteit van het bestuur. In dit preadvies hebben wij de risico's in kaart gebracht van ondemocratisch bestuur, het risico van onrechtmatig bestuur en het risico van wanpresterend bestuur.

Op basis van de indeling in input-, throughput- en output-legitimiteit hebben we ook aangegeven op welke wijze deze legitimiteit kan worden versterkt. Een algemene boodschap is dat er een veelheid aan verschillende institutionele mechanismen nodig is om de legitimiteit van algoritmisch bestuur te waarborgen. Centraal staan hierbij de ideeën van democratische inbedding, passendheid binnen juridische kaders en het leveren van een aantoonbare bijdrage aan publieke waarden. Deze algemene principes zijn niet nieuw, maar vergen in deze tijd van algoritmisch bestuur een 'update' zodat de bestaande institutionele mechanismen gaan passen bij de nieuwe, hoogtechnologische manieren van werken in het openbaar bestuur.

Graag willen we ook enkele moeilijkheden noemen die een rol zullen spelen bij het invoeren van nieuwe institutionele mechanismen om de legitimiteit van algoritmisch bestuur te versterken. Een eerste moeilijkheid betreft de vele verbindingen tussen algoritmen. De voorbeelden van SyRI en CAS suggereren dat er een aanwijsbaar algoritme is en dat het gaat om de legitimiteit van het organisationele gebruik van dit specifieke algoritme. In de praktijk gaat het echter vaak om een veelheid van verbonden algoritmen die elkaar op allerlei wijzen beïnvloeden. Deze algoritmen worden gebruikt door verschillende organisaties – soms zelfs buiten de overheid – en het uiteindelijke functioneren hangt af van deze interacties. Een tweede moeilijkheid betreft het internationale karakter van de technologieontwikkeling. Vele technologische componenten zijn niet in Nederland maar in andere landen ontwikkeld en specifiek inzicht in het functioneren van deze technologische componenten is soms lastig te verkrijgen.

De vormgeving van legitimiteit van algoritmisch bestuur is daarom een opgave van institutioneel ontwerp. Hoewel Kulk & Van Deursen (2020: 6, 7) terecht opmerken dat algemene juridische kaders een voldoende basis bieden is er ook een nadere invulling nodig. Er zal een veelheid aan nieuwe institutionele mechanismen moeten worden ontwikkeld die waarborgen dat het gebruik van algoritmen door overheidsorganisaties niet leidt tot een uitholling van de legitimiteit van het bestuur. Deze institutionele mechanismen betreffen soms regelgeving (zoals de eis tot een juridische toets op algoritmen), soms het uitbreiden van organisationele capaciteiten (zoals het vermogen tot politiek toezicht op algoritmisch bestuur) en soms ook aandacht voor nieuwe manieren van werken (bijvoorbeeld de politieke sensitiviteit van ontwerpers). Dit geheel aan activiteiten is nodig om de huidige ontwikkeling in de richting van algoritmisch bestuur niet buiten maar binnen de democratische rechtstaat een plek te geven en te voorkomen dat er ondemocratisch, onrechtmatig en wanpresterend bestuur ontstaat.

Referenties

- Almadal, M. (2019). Human intervention in automated decision-making: Toward the construction of contestable systems. In *Seventeenth International Conference on Artificial Intelligence and Law (ICAIL '19)*, June 17–21, 2019, Montreal, QC, Canada. ACM, New York, NY, USA, 10 pages.
- Baer, T. (2019). *Understand, Manage, and Prevent Algorithmic Bias: A Guide for Business Users and Data Scientists*. New York, NY: Apress
- Bovens, M.A.P. (1998). *The quest for responsibility: Accountability and citizenship in complex organisations*. Cambridge: Cambridge University Press.
- Bovens, M.A.P., Zouridis, S., & Van Eck, M. (2018). Algoritmische rechtstoepassing in de democratische rechtsstaat. *Nederlands juristenblad*, 93(40), 3008-3017.
- Brkan, M. (2019). Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond. *International journal of law and information technology*, 27(2), 91-121.
- Bu-Pasha, S. (2020). The controller's role in determining 'high risk' and data protection impact assessment (DPIA) in developing digital smart city. *Information & Communications Technology Law*, 29(3), 391-402.
- Burrell, J. (2016). How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society*, 3(1), 2053951715622512.
- Busuioac, M. (2000). Accountable Artificial Intelligence: Holding Algorithms to Account. *Public Administration Review*. <https://doi.org/10.1111/puar.13293>
- Curtin, D., & Meijer, A.J. (2006). Does transparency strengthen legitimacy? *Information Polity*, 11(2), 109-122.
- de Fine Licht, K., & de Fine Licht, J. (2020). Artificial intelligence, transparency, and public decision-making. *AI & SOCIETY*, 1-10.
- Demir, T., & Nyhan, R. C. (2008). The politics-administration dichotomy: An empirical search for correspondence between theory and practice. *Public Administration Review*, 68(1), 81-96.
- Dijck, J. van, Poell, T., & De Waal, M. (2018). *The platform society: Public values in a connective world*. Oxford: Oxford University Press.
- Eck, M. van (2018). *Geautomatiseerde ketenbesluiten & rechtsbescherming: Een onderzoek naar de praktijk van geautomatiseerde ketenbesluiten over een financieel belang in relatie tot rechtsbescherming*. Proefschrift. Tilburg University.
- Est, R. van, Bakker, E. de, Broek, J. van den, Deuten, J., Diederens, P., Keulen, I. van, Korthagen, I. & Voncken, H. (2020). *Waardevol digitaliseren Hoe lokale bestuurders vanuit publiek perspectief mee kunnen doen aan het 'technologiespel'*. Den Haag: Rathenau Instituut.
- Frissen, V., Van Eck, M. & Drouen, T. (2019). *Toezicht op het gebruik van algoritmen door de overheid*. Den Haag: Hooghiemstra & Partners.
- Fry, H. (2018). *Hello World. How to be Human in the Age of the Machine*. London: Black Swan.
- Goddard, K., Roudsari, A., & Wyatt, J. C. (2011). Automation bias: a systematic review of frequency, effect mediators, and mitigators. *Journal of the American Medical Informatics Association*, 19(1), 121-127.
- Guidotti, R., Monreale, A., Ruggieri, S., Turini, F., Giannotti, F., & Pedreschi, D. (2018). A survey of methods for explaining black box models. *ACM computing surveys (CSUR)*, 51(5), 93.

- Gustavsen, A., Pierre, J., & Røiseland, A. (2014). Introduction: Toward output legitimacy in local government. *Urban Research & Practice*, 7, 119-122.
- Hart, P. 't, & Wille, A. C (2006). Ministers and top officials in the Dutch core executive: Living together, growing apart? *Public Administration*, 84, 121– 146.
- Hendriks, C. M. (2012). *The politics of public deliberation: Citizen engagement and interest advocacy*. Heidelberg: Springer.
- Hoven, M.J. van den (1998). Moral responsibility, public office and information technology. In: *Public administration in an information age*, eds. I. T. M. Snellen and W. B. H. J. van de Donk, pp. 97–111. Amsterdam: IOS Press.
- Jackson, J.R. (2018). Algorithmic bias. *Journal of Leadership, Accountability and Ethics*, 15 (4), 55–65.
- Kulk, S., Deursen, S. van e.a. (2020). *Juridische aspecten van algoritmen die besluiten nemen. Een verkennend onderzoek*. Den Haag: WODC.
- Livingston, S., & Risse, M. (2019). The future impact of artificial intelligence on humans and human rights. *Ethics & international affairs*, 33(2), 141-158.
- Meijer, A.J. (2009). Complex Responsibilities: An empirical analysis of responsibilities and technological complexity in Dutch immigration policies. *Public Management Review*, 11(6), 771-790.
- Meijer, A. & Grimmelikhuijsen, S. (2020). Responsible and Accountable Algorithmization: How to Generate Citizen Trust in Governmental Usage of Algorithms. In: Schuilenburg, M. & Peeters, R. (eds). *The Algorithmic Society: Technology, Power and Knowledge*. London: Routledge.
- Meijer, A., Ruijter, E. & Dekkers, R. (2020). Navigatiestrategie. Lessen uit drie casusstudies over de kennispositie van de Tweede Kamer op het gebied van digitalisering. Rapport voor de Tijdelijke Commissie Digitale Toekomst van de Tweede Kamer. Utrecht: Universiteit Utrecht.
- Michels, A. & De Graaf, L. (2010). Examining citizen participation: Local participatory policy making and democracy. *Local Government Studies*, 36(4), 477-491.
- Overeem, Patrick, & Rutgers, M.R.. 2003. Three Roads to Politics and Administration: Ideational Foundations of the Politics/Administration Dichotomy. In: *Retracing Public Administration*, edited by Mark R. Rutgers, 161– 84. London: JAI/Elsevier Science.
- Pogrebinschi, T., & Ryan, M. (2018). Moving beyond input legitimacy: When do democratic innovations affect policy making?. *European Journal of Political Research*, 57(1), 135-152.
- Scharpf, F.W. (1999). *Governing in Europe: Effective and democratic?*. Exford: Oxford University Press.
- Schendel S. van (2019) The Challenges of Risk Profiling Used by Law Enforcement: Examining the Cases of COMPAS and SyRI. In: Reins L. (eds) *Regulating New Technologies in Uncertain Times. Information Technology and Law Series*, vol 32. T.M.C. Asser Press, The Hague. https://doi-org.proxy.library.uu.nl/10.1007/978-94-6265-279-8_12
- Schmidt, V., & Wood, M. (2019). Conceptualizing throughput legitimacy: Procedural mechanisms of accountability, transparency, inclusiveness and openness in EU governance. *Public Administration*, 97(4), 727-740.
- Schuilenburg, M. & Peeters, R. (2020). *The Algorithmic Society: Technology, Power and Knowledge*. London: Routledge.

Strøm, K. (2000). Delegation and accountability in parliamentary democracies. *European journal of political research*, 37(3), 261-290.

TNO (2019). Quick scan AI in de publieke dienstverlening. Den Haag: TNO. Beschikbaar op: <https://www.rijksoverheid.nl/documenten/rapporten/2019/04/08/quick-scan-in-de-publieke-dienstverlening>.

Tutt, A. 2017. An FDA for algorithms. *Administrative Law Review*, 69(1), 83-124.

Vetzo, M.J., Gerards, J.H. & Nehmelman, R. (2018). Algoritmes en grondrechten. Den Haag: Boom juridisch.

Vogl, T. M., Seidelin, C., Ganesh, B., & Bright, J. (2020, Online First). Smart Technology and the Emergence of Algorithmic Bureaucracy: Artificial Intelligence in UK Local Authorities. *Public Administration Review*. DOI: <https://doi-org.proxy.library.uu.nl/10.1111/puar.13286>.

Weber, M. (1978). *Economy and society: An outline of interpretive sociology*. Berkeley: University of California Press.

West, D.M. (2005). *Digital government: Technology and public sector performance*. Princeton University Press.

Willems, D., & Doeleman, R. (2014). Predictive Policing – wens of werkelijkheid?. *Het Tijdschrift voor de Politie*, 76(4), 5.

Williams, B.A., Brooks, C.F., & Shmargad, Y. (2018). How algorithms discriminate based on data they lack: Challenges, solutions, and policy implications. *Journal of Information Policy*, 8, 78-115.

Willson, M. (2017) Algorithms (and the) everyday, *Information, Communication & Society*, 20:1, 137-150,

Wilson, J.Q. (2019). *Bureaucracy: What government agencies do and why they do it*. New York: Basic Books.

WRR (2016). *Big Data in een vrije en veilige samenleving*. Amsterdam: AUP.

Young, M., Michael K., & Krafft, P.M.. (2019). Municipal Surveillance Regulation and Algorithmic Accountability. *Big Data & Society* 6, no. 2.

Zouridis, S. (2000). *Digitale disciplineren: over ICT, organisatie, wetgeving en het automatiseren van beschikkingen*. Proefschrift. Tilburg: Katholieke Universiteit Brabant.

Zuboff, S. (2019). *The Age of Surveillance Capitalism*. London: Profile Books.

BIJLAGE: Stellingen

Onderstaande stellingen geven de belangrijkste hoofdlijnen kort en bondig weer. Daarmee bieden deze stellingen hopelijk een goede basis voor een verder gesprek over de acties die noodzakelijk zijn om de legitimiteit van algoritmisch bestuur te waarborgen.

STELLING 1: Voor democratische toezicht op algoritmisch bestuur is momenteel het gebrek aan kennis van politici en de beperkte politieke sensitiviteit van de betrokken ambtenaren een probleem.

STELLING 2: Legitimiteit van algoritmisch bestuur vergt niet alleen transparantie van het algoritme maar ook transparantie van het gebruik van het algoritme in de organisatie.

STELLING 3: De legitimiteit van algoritmisch bestuur vergt niet alleen een correct juridisch kader maar vooral een breed democratisch debat over (on)wenselijke uitkomsten van algoritmisch bestuur.

STELLING 4: Een brede juridische impact-assessment is nodig om de legitimiteit van algoritmisch bestuur te garanderen.

STELLING 5: Bij het ontwerp van elk algoritme moeten – op vergelijkbare wijze als bij de ruimtelijke ordening – burgers participeren in het ontwerpproces.

STELLING 6: Expliciet vastleggen van de verantwoordelijkheden van de verschillende publieke en private partijen betrokken bij algoritmisch bestuur is cruciaal voor de legitimiteit.