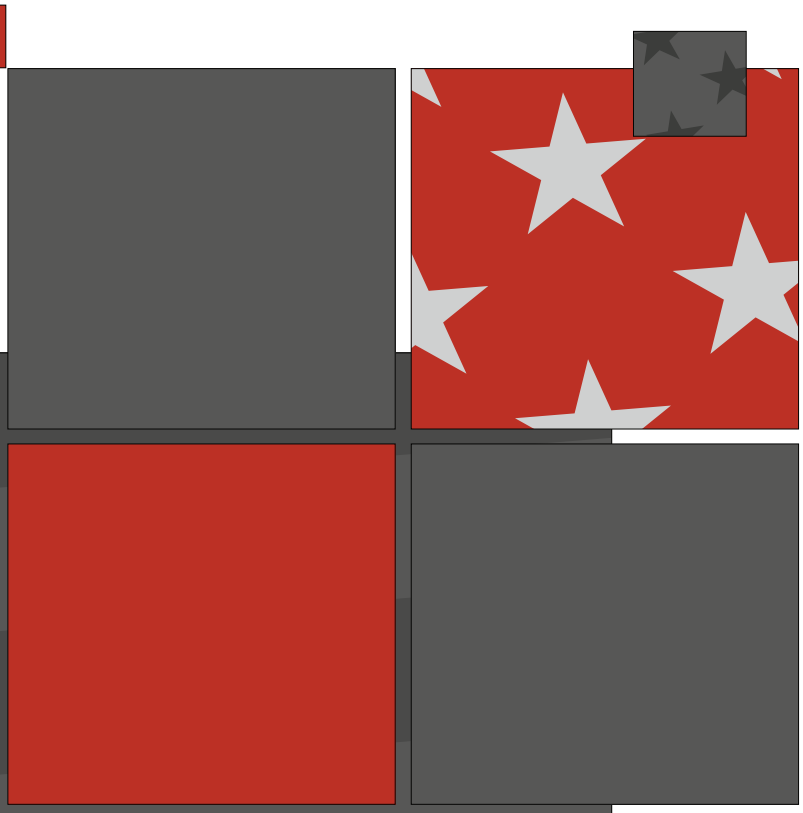
NOB / LOF SCRIPTIEPRIJS 32

EEN WERVELWIND AAN DATA, FUNEST VOOR RECHTSSTATELIJKE BEGINSELEN?

EEN ONDERZOEK NAAR HET RECHTSSTATELIJK GEBRUIK VAN SLIMME OPSPORINGSTECHNIEKEN BIJ DE NEDERLANDSE BELASTINGDIENST



CHARLOTTE KAEBISCH

de Nederlandse Orde van Belastingadviseurs

Een wervelwind aan data, funest voor rechtsstatelijke beginselen?

Een onderzoek naar het rechtsstatelijk gebruik van slimme opsporingstechnieken bij de Nederlandse Belastingdienst.

NOB/LOF Serie

In deze serie verschijnen fiscale doctoraalscripties die bekroond zijn met de NOB/LOF Scriptieprijs. Deze prijs, ingesteld door de Nederlandse Orde van Belastingadviseurs in samenwerking met het Landelijk Overleg Fiscalisten, is in 1992 in het leven geroepen voor studenten fiscaal recht en fiscale economie. De jury van de NOB/LOF Scriptieprijs bestaat dit jaar uit: prof. mr. J.W. Bellingwout (voorzitter van de jury), prof. dr. R.H.C. Luja en mr. N.C. Boef (voorzitter NOB).

Een wervelwind aan data, funest voor rechtsstatelijke beginselen?

Een onderzoek naar het rechtsstatelijk gebruik van slimme opsporingstechnieken bij de Nederlandse Belastingdienst.

Charlotte Kaebisch

Wolters Kluwer

Deventer - 2023

Volledige citeerwijze:
C. Kaebisch, *Een wervelwind aan data, funest voor rechtsstatelijke beginselen? (NOB/LOF Serie)*, Deventer: Wolters Kluwer 2023

Het complete productaanbod vindt u in de online webshop: www.wolterskluwer.nl/shop.

Ontwerp omslag: Orange House

Onze klantenservice kunt u bereiken via: www.wolterskluwer.nl/klantenservice.

Auteur(s) en uitgever houden zich aanbevolen voor inhoudelijke opmerkingen en suggesties. Deze kunt u sturen naar: boeken-NL@wolterskluwer.com.

Voorwoord

Beste Lezer,

U staat op het punt om mijn masterthesis te lezen. Een onderzoek dat ik schreef in het kader van het 'Tilburg-Antwerpen traject' en dat zich richt op het steeds veelvuldiger gebruik van risicoprofielen door belastingadministraties.[1] Voor de meeste studenten is de thesis het slotstuk van hun studententijd. Die vlieger gaat voor mij niet op. Ik zal volgend jaar mijn studie- en studententijd voortzetten door onder meer het volgen van de master International Business Taxation: law track. Toch voelt het schrijven van dit voorwoord momenteel als een einde van een levenshoofdstuk. Het schrijven van mijn thesis heeft de nodige kruim gekost. Ik ben diegenen die mij hebben geholpen en veelvuldig succes hebben gewenst met het schrijven dan ook erg dankbaar.

Die dank gaat vooral uit naar mijn begeleider. Beste meneer Gribnau, wat voelde ik mij vereerd toen u mij aan het begin van dit academisch jaar vroeg om deel te nemen aan het Tilburg-Antwerpen traject. Tegelijkertijd betekende deze eer dat de verwachtingen hooggespannen waren, hopelijk heb ik deze verwachtingen waar weten te maken. Aan uw begeleiding ligt het in ieder geval niet. U heeft mij ontzettend goede feedback gegeven en u heeft dit bovenal zeer snel gedaan. Ik heb uw begeleiding daarom als erg prettig ervaring. Wellicht mag ik in de toekomst ooit nog een keer met u samenwerken. Ook mevrouw Dusarduijn, professor Peeters, professor Van de Vijver en meneer Van der Linden hebben mij voorzien van goede suggesties en feedback, waarvoor ook hartelijk dank. Verder heb ik de bijeenkomsten met de andere deelnemende studenten als erg leerzaam ervaren. Ik ben dan ook blij dat ik heb deel mogen nemen aan het traject.

Daarnaast wil ik in het bijzonder Marc, Nicky en Rick bedanken voor het helpen begrijpen van de werkwijze van de slimme opsporingstechnieken. Ook mijn collega's van Wesselman wil ik graag bedanken voor de geboden tijd en ruimte en de gegeven tips. Anouk en Johan, ik wil jullie in het bijzonder (alvast) bedanken voor het bijwonen van mijn verdediging.

Natuurlijk wil ik ook mijn lieve ouders en zusjes bedanken voor het helpen tijdens én met het schrijven, de succeswensen, het vertrouwen en het geduld.

1 Gaandeweg het onderzoek is gebleken dat dit onderwerp zich helaas niet goed leent voor een rechtsvergelijkend onderzoek. Zodoende is in overleg besloten om het rechtsvergelijkend element uit de thesis te laten.

Allerliefste Werner, ook jou wil ik graag even apart benoemen. Jij hebt mij ook ontzettend geholpen. Dat deed je met tips, liefde, geduld en vooral vertrouwen. Ook als ik het even helemaal niet meer zag zitten, stond jij voor me klaar.

Ook zonder alle anderen die mij succes hebben gewenst, was dit eindresultaat er niet gekomen. Ik ben dan ook erg dankbaar dat ik steun van jullie allen heb gehad. Als laatste wens ik jullie veel leesplezier toe.

Bedankt!

Charlotte

Samenvatting

In dit onderzoek is onderzocht hoe rechtsstatelijkheid van (de inzet van) algoritmen, Big Data-analyse en profiling door de Nederlandse Belastingdienst gewaarborgd kan worden. Als eerste is onderzocht wat deze 'slimme opsporingstechnieken' inhouden. Daarna is een korte geschiedenis geschetst van het gebruik hiervan door de Nederlandse Belastingdienst. Vervolgens is de betekenis van de term transparantie in relatie tot deze technieken onderzocht. Transparantie betekent hier het kunnen inzien en doorgronden van de werkwijze van de slimme opsporingstechnieken. Hoewel de inzet van slimme opsporingstechnieken efficiëntiewinst oplevert, levert het ook risico's op. Dat zijn met name de kans op discriminatie en het feit dat onherroepelijk ook valse resultaten gegenereerd zullen worden. Aan de hand van deze risico's zijn een viertal aanbevelingen opgesteld voor (een) rechtsstatelijke (inzet van de) slimme opsporingstechnieken van de Nederlandse Belastingdienst. Hierbij is inspiratie ontleend aan al bestaande richtinggevende kaders, de visie van de Nationale ombudsman en het Algoritmeregister van de stad Amsterdam als good practice. De geformuleerde aanbevelingen pogen zowel de risico's te beperken als wel de bewustwording van de risico's te vergroten.

Aanbevolen wordt allereerst[1] om de slimme opsporingstechnieken voor dat zij worden ingezet te laten controleren door een aan te stellen controlegroep. Door de verificatie van de controlegroep wordt gewaarborgd dat de slimme opsporingstechnieken blijk geven van gebondenheid aan fundamentele, rechtsstatelijke beginselen en rechtsnormen die niet per definitie juridisch afdwingbaar zijn. Dit dient te gebeuren door gebruik te maken van bias-minimaliserende methoden en door rechtsstatelijke risicofactoren te selecteren. De controlegroep dient zo divers mogelijk te zijn.

Ten tweede wordt aanbevolen om het gebruik van Big Data-analyse en slimme algoritmen zo veel mogelijk te beperken, ofwel enkel in te zetten wanneer andere type slimme opsporingstechnieken niet toereikend zijn. Reden voor deze aanbeveling is dat deze twee technieken de meeste risico's met zich meedragen.

Als derde wordt aanbevolen documentatie verplicht openbaar toegankelijk te stellen. Hetgeen bijdraagt aan transparantie als voorwaarde voor (democratische) verantwoording en de mogelijkheid geeft de toenemende macht van de slimme opsporingstechnieken in te tomen, waardoor tevens de disbalans van de trias politica

1 De volgorde van aanbevelingen is willekeurig gekozen en geeft derhalve geen indicatie van prioriteit aan.

hersteld kan worden. Ook kan de documentatie bruikbaar zijn voor de rechterlijke macht bij het bieden van rechtsbescherming achteraf.

De vierde aanbeveling is het aanstellen van een gespecialiseerd, toezichthoudend orgaan dat een toetsing aan de rechtsstatelijkheid van (de inzet van) de slimme opsporingstechnieken dient uit te voeren. Het orgaan dient de Belastingdienst tijdig te informeren over het toetsingsresultaat. Ingeval sprake blijkt te zijn van een gebrekkige rechtsstatelijke inzet van de slimme opsporingstechnieken, kan de Belastingdienst in samenspraak met het orgaan zorgdragen voor een verbetering van de inzet van slimme opsporingstechnieken. Het toetsingsresultaat kan tevens bruikbaar zijn voor de rechterlijke macht wanneer hij rechtsbescherming achteraf dient te bieden.

Naast het voorleggen van deze aanbevelingen is kort stilgestaan bij mogelijke sancties, wat hier een lastig thema is, omdat belastingadministraties publieke organen zijn en een boete opleggen als sanctie hierdoor niet voor de hand ligt. Het wordt daarom aanbevolen om nader onderzoek te doen naar nut en noodzaak en naar de mogelijkheden van sanctieoplegging. Ook wordt aanbevolen om de balans tussen transparantie en het risico op *gaming the system* nader te onderzoeken.

Opvolging van de vier geformuleerde aanbevelingen zal leiden tot het waarborgen van een rechtsstatelijke inzet van slimme opsporingstechnieken en kan bijdragen aan het bereiken van een meer inclusieve, diverse en gelijkwaardige maatschappij.

INHOUDSOPGAVE

LIJST MET GEBRUIKTE AFKORTINGEN

btw:	belasting over de toegevoegde waarde
EVRM:	Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden
FSV:	Fraude Signalering Voorziening
GPS:	Global positioning system
HR:	Hoge Raad
ICT:	Informatie- en Communicatietechnologie
IP:	Internet Protocol
IVBPR:	Internationaal Verdrag inzake burgerrechten en politieke rechten
NDFR:	Nederlandse Documentatie Fiscaal Recht
OV:	openbaar vervoer
PwC:	PricewaterhouseCoopers
UVRM:	Universele Verklaring van de Rechten van de Mens
HGEU:	Handvest van de grondrechten van de Europese Unie
WOZ:	Wet waardering onroerende zaken

1 Inleiding

We leven in een digitaal tijdperk waarin gegevensuitwisseling razendsnel gaat. Bankieren in het buitenland, verkopen aan consumenten die 3.000 kilometer verderop wonen of digitaal een concert volgen op afstand, het is allemaal nog nooit zo gemakkelijk geweest als nu. Door deze ongekende mogelijkheden dienen belastingadministraties steeds meer informatie en gegevens in dezelfde tijd te verwerken. Het aantal belastingambtenaren neemt echter niet lineair met de gegevensgroei toe. Hierdoor wordt de werkdruk alsmaar groter. Zelfs al zouden belastingadministraties alle controles handmatig willen uitvoeren, dan is dat onmogelijk, omdat de capaciteit hiervoor ontoereikend is.

Belastingadministraties kunnen daarom niet langer achterblijven bij alle technologische ontwikkelingen. Dat doen zij dan ook niet. Steeds vaker maken belastingadministraties, waaronder de Nederlandse Belastingdienst, bij de uitoefening van hun taken gebruik van risicoprofielen die zijn opgesteld door algoritmen. Hierdoor kan de uitoefening van de taken een stuk sneller verlopen en is minder mankracht nodig. Echter, door de kindertoeslagenaffaire is pijnlijk inzichtelijk geworden dat deze winst niet vanzelfsprekend, zonder enig nadeel valt te behalen. Het gebruik van deze risicoprofielen, bij bijvoorbeeld de controle op aangiftes, kan leiden tot (indirecte) (onbewuste) discriminatie of schending van andere fundamentele, rechtsstatelijke beginselen, zoals het recht op non-discriminatie.

In dit onderzoek zal gezocht worden naar waarborgen voor een rechtsstatelijke inzet van algoritmen, Big Data-analyse en profiling door de Nederlandse Belastingdienst. Kort gezegd stelt rechtsstatelijkheid grenzen aan de bevoegdheidsuitoefening van de overheid. Het bindt de Staat aan het recht, dat wil zeggen aan de wet, maar ook aan fundamentele (rechtsstatelijke) beginselen en grondrechten, zoals het gelijkheidsbeginsel en het recht op privacy.

Over de uitoefening van bevoegdheden door overheidsinstanties dient verantwoording te worden afgelegd. Het gaat dan om politieke verantwoording (aan het parlement), maar ook om verantwoording aan een grotere groep belanghebbenden van de belastingadministratie; de belastingplichtigen. Door het afleggen van verantwoording kan gecontroleerd worden of de overheid zich houdt aan die grenzen van de bevoegdheidsuitoefening. Hiervoor is transparantie vereist.[1] Zonder transparantie kunnen belanghebbenden immers geen inzicht krijgen in het gebruik van bevoegdheden. Inzichtelijk dient dan te zijn hoe de algoritmen, Big Data-analyse en profiling

1 Gribnau 2016, p. 375.

ingezet worden door de Nederlandse Belastingdienst. Welke vormen van transparantie een voorwaarde zijn voor de verantwoording van de inzet van deze technieken zal in dit onderzoek onderzocht worden.

De te beantwoorden onderzoeksvraag met bijbehorende deelvragen zal ik hierna formuleren. Vervolgens voorzie ik in een verdere – begripsmatige – afbakening via het theoretisch kader. Hierna zal ik de theoretische en maatschappelijke relevantie van het antwoord op de onderzoeksvraag behandelen. Daarna behandel ik de methodologie. Als afsluiting van deze inleiding geef ik een leeswijzer van het verdere vervolg van dit onderzoeksverslag.

1.1 Onderzoeksvraag

Zoals hiervoor is gezegd, zal in dit onderzoek gezocht worden naar waarborgen voor een rechtsstatelijk gebruik van algoritmen, Big Data-analyse en profiling door de Nederlandse Belastingdienst.

Zodoende kom ik tot de formulering van de volgende onderzoeksvraag:

> *Hoe kan de rechtsstatelijke inzet van algoritmen, Big Data-analyse en profiling door de Nederlandse Belastingdienst gewaarborgd worden?*

Om tot een beantwoording van deze hoofdonderzoeksvraag te komen, zullen de volgende deelvragen beantwoord worden:

1. Wat is de definitie van algoritmen, Big Data-analyse en profiling?
2. Wat is de geschiedenis van het gebruik van algoritmen, Big Data-analyse en profiling bij de Nederlandse Belastingdienst?
3. Welke vormen van transparantie zijn relevant bij het gebruik van algoritmen, Big Data-analyse en profiling?
4. Welke risico's kleven aan (de inzet van) algoritmen, Big Data-analyse en profiling en wat is voor het mitigeren van deze risico's het belang van transparantie?
5. Welke richtinggevende kaders voor overheden voor (transparantie van) het gebruik van algoritmen, Big Data-analyse en profiling bestaan al, meer specifiek voor de Nederlandse Belastingdienst?
6. Welke aanbevelingen kunnen bijdragen aan een rechtsstatelijk gebruik van algoritmen, Big Data-analyse en profiling door de Nederlandse Belastingdienst?

De te formuleren aanbevelingen zullen gericht zijn op de inzet van algoritmen, Big Data-analyse en profiling door de Nederlandse Belastingdienst. Dit neemt echter niet weg dat de te formuleren aanbevelingen ook waardevol kunnen zijn voor andere belastingadministraties die gebruikmaken van algoritmen, Big Data-analyse en profiling.

1.2 Het theoretisch kader

Met het schetsen van een theoretisch kader wordt verantwoording afgelegd ten aanzien van het onderzoek. Het geeft de keuze van de onderzoeker over de invalshoek

van het onderzoek weer.[2] Dit is cruciaal voor de afbakening en de controleerbaarheid van het onderzoek.[3] Het theoretische kader bestaat uit een operationalisering van enkele relevante begrippen uit de onderzoeksvraag en een verdere afbakening over wat per deelvraag onderzocht zal worden.[4]

1.2.1 *Operationalisering*

In het belang van de transparantie en de geloofwaardigheid van het onderzoek behoren kernbegrippen uit de (hoofd)vraagstelling te worden geoperationaliseerd.[5] Tevens dient dit de controleerbaarheid en behoort het te leiden tot navolgbaarheid van het onderzoek.[6]

Enkele begrippen in de hoofdvraagstelling zijn dusdanig omvangrijk dat zij niet in de inleiding, maar in een zelfstandig hoofdstuk geoperationaliseerd zullen worden. Het betreft de begrippen 'algoritmen, Big Data-analyse en profiling', zij komen zelfstandig aan bod bij de beantwoording van de eerste deelvraag.

1.2.2 *Rechtsstatelijkheid*

Rechtsstatelijkheid is een concept dat het recht met de staat verbindt. Volgens Gribnau 'lijkt een *communis opinio* te bestaan over vier kernelementen van de rechtsstaatgedachte'.[7] Dit zijn 'het legaliteitsbeginsel, de trias politica, het beginsel van onafhankelijke rechtspraak en het beginsel dat de overheid grondrechten in acht behoort te nemen'. Rechtsstatelijkheid creëert grenzen aan de bevoegdheidsuitoefening van de overheid. Deze begrenzing komt het sterkst naar voren in het legaliteitsbeginsel dat bepaalt dat de overheid slechts op grond van een wet in formele zin mag ingrijpen in de vrijheden van burgers. Rechtsstatelijkheid betekent gebondenheid aan het recht, meer dan slechts aan het positieve recht. Het houdt ook in gebonden zijn aan fundamentele, rechtsstatelijke beginselen en rechtsnormen die niet per definitie juridisch afdwingbaar zijn. Vanuit die gedachte wordt de overheid ook geacht gebonden te zijn aan bijvoorbeeld adviezen en normen van de Nationale Ombudsman.[8] Hoewel deze adviezen niet juridisch afdwingbaar zijn, dient de overheid zich – vanuit de gedachte van rechtsstatelijkheid – wel te committeren aan deze adviezen. De gedachte van rechtsstatelijkheid houdt daarmee ook in dat de Belastingdienst gebonden dient te zijn aan de aanbevelingen voor rechtsstatelijke slimme opsporingstechnieken die in dit onderzoek geformuleerd zullen worden.

2 Vranken, in: *Recht en Methode* 2015, p. 11.
3 Van Dijck, Snel & Van Golen 2018, p. 65.
4 Van Dijck, Snel & Van Golen 2018, p. 73.
5 Van Dijck, Snel & Van Golen 2018, p. 76.
6 Van Dijck, Snel & Van Golen 2018, p. 76.
7 Gribnau 1998, p. 13.
8 Vgl. Behoorlijkheidsnormen Nationale ombudsman onder de loep 21 februari 2022, raadpleegbaar via nationaleombudsman.nl/professionals/nieuws/2022/behoorlijkheidsnormen-nationale-ombudsman-onder-de-loep.

Om zorg te dragen dat de Belastingdienst deze aanbevelingen respecteert en opvolgt, is verantwoording cruciaal. Om verantwoording af te leggen en deze te kunnen beoordelen, is transparantie vereist.[9] Zodoende vervult transparantie een centrale rol bij het waarborgen van rechtsstatelijke bevoegdheidsuitoefening en dus in dit onderzoek.

1.2.3 *Verdere afbakening*

In dit onderzoek zal nauwelijks tot geen aandacht besteed worden aan (de schending van) privacy en eerbiediging van de eigen leefruimten zoals is bedoeld in art. 6 van het EVRM. Hiernaar is al meer onderzoek verricht, dan naar schending van andere rechtsstatelijke rechten, zoals het recht op non-discriminatie. Daarnaast is de wet- en regelgeving ter voorkoming van privacyschending (relatief) ver ontwikkeld. Onderhavig onderzoek is bovendien te kort om ook stil te staan bij de privacyproblematiek. De focus ligt zodoende op het gelijkheidsbeginsel. De rechtsstatelijke inzet van algoritmen, Big Data-analyse en profiling, zoals is bedoeld in de onderzoeksvraag, dient daarmee met name het gelijkheidsbeginsel te respecteren.

Daarnaast zal door de rechtsstatelijke inzet verantwoording afgelegd kunnen worden. De te formuleren aanbevelingen dienen namelijk ook te zorgen voor transparantie. Transparantie is een voorwaarde voor het kunnen afleggen van verantwoording en draagt mogelijk bij aan het vertrouwen van de burger in de belastingadministratie. Meer transparantie kan ook leiden tot meer vragen, wat juist afbreuk zou kunnen doen aan het vertrouwen. Om deze mogelijke afbreuk te voorkomen dient steeds weer opnieuw verantwoording afgelegd te worden. Gribnau betitelt deze paradox als 'Fiscale transparantie: de moeilijke weg naar meer vertrouwen'.[10] Hoewel dit een interessant onderzoeksthema is, ook in relatie tot (de inzet van) algoritmen, Big Data-analyse en profiling, valt de relatie tussen transparantie en vertrouwen niet binnen de reikwijdte van dit onderzoek.

Dit onderzoek kent een aantal handelingsdoelen. Deze handelingsdoelen omschrijven welke handeling verricht dient te worden om tot een beantwoording van de deelvragen te komen, oftewel de wijze waarop het doel bereikt kan worden. De handelingsdoelen voor de eerste vier deelvragen zullen (met name) beschrijven, analyseren en rechtsvergelijken zijn.[11] Voor het beantwoorden van deelvraag 5 zullen de relevante wet- en regelgeving en overige richtinggevende kaders onderzocht en beoordeeld worden. De beantwoording van deelvraag 6 zal bestaan uit het formuleren van aanbevelingen voor het waarborgen van rechtsstatelijkheid van algoritmen, Big Data-analyse en profiling gebruikt door de Nederlandse Belastingdienst. Bij het formuleren van deze aanbevelingen zullen de geconstateerde risico's centraal staan. Ook zal hiervoor inspiratie ontleend worden aan de geraadpleegde richtinggevende kaders.

9 Gribnau 2016, p. 375.

10 Dit is de titel van de beschouwing van Gribnau in het *MBB* 2016 waarin hij verschillende visies op de relatie tussen transparantie en vertrouwen beschouwt, waaronder ook de visie die ik hier noem.

11 IJzermans 2015, p. 11.

1.3 Relevantie

1.3.1 *Maatschappelijke relevantie*

'Belastingdienst schatte frauderisico regelmatig in op uiterlijk of nationaliteit'[12], 'Belastingdienst schuldig aan structurele discriminatie van mensen die toeslagen ontvingen'[13], 'Boete voor Belastingdienst van 2,7 miljoen voor discriminatie toeslagenouders'[14]. Enkele koppen van nieuwsberichten die de ophef in de maatschappij over de discriminatie in de kindertoeslagenaffaire inzichtelijk maken. Op 17 december 2020 is het eindverslag over het onderzoek naar de kindertoeslagenaffaire bij de Tweede Kamer ingediend, met als titel *Ongekend onrecht*.[15] Bij de afdeling toeslagen werd gebruikgemaakt van risicoprofielen. Eén van de selectiecriteria was afkomst of nationaliteit. Dit selectiecriterium had een discriminerende werking. Veel ouders zijn ten onrechte aangemerkt als fraudeur, vandaar de titel *Ongekend onrecht*.

Het intreden van discriminatie wordt aangemerkt als een, al dan niet onbewust, risico van het gebruik van risicoprofielen door belastingadministraties, hetgeen strijdigheid oplevert met het verbod op discriminatie dat onder meer is vastgelegd in art. 1 van de Nederlandse Grondwet. Discriminatie kan leiden tot polarisatie van de samenleving, uitsluiting, kansenongelijkheid, verharding van relaties en door psychische problemen van het individu tot druk op de gezondheidszorg[16]. Deze nadelige effecten zorgen voor verstoring van een inclusieve, diverse en gelijkwaardige maatschappij.

Om te voorkomen dat een affaire zoals de kindertoeslagenaffaire zich nog een keer voordoet, zal in dit onderzoek gezocht worden naar waarborgen voor een rechtsstatelijke inzet van algoritmen, Big Data-analyse en profiling. Zoals is betoogd in par. 1.2.1 stelt rechtsstatelijkheid grenzen aan de bevoegdheidsuitoefening. Rechtsstatelijkheid betekent het gebonden zijn aan het recht in zijn breedste opvatting. Dat wil zeggen niet enkel gebondenheid aan het positieve recht (de wet, via het grondwettelijk legaliteitsbeginsel), maar ook gebondenheid aan rechtsstatelijke beginselen en rechtsnormen die niet per definitie juridisch afdwingbaar zijn. De aanbevelingen die worden geformuleerd in dit onderzoek streven naar een rechtsstatelijke inzet van slimme opsporingstechnieken waarbij een belemmering van een inclusieve, diverse en gelijkwaardige maatschappij voorkomen dient te worden.

1.3.2 *Theoretische relevantie*

Er is nog weinig wetenschappelijk onderzoek verricht naar het gebruik van algoritmen, Big Data-analyse en profiling bij de Nederlandse Belastingdienst. Onderhavig onderzoek zal hier verandering inbrengen.

12 NU.nl/ANP laatste update 26 januari 2022.
13 Hofs 17 juli 2020.
14 NOS 7 december 2021.
15 Zie hiervoor: tweedekamer.nl/nieuws/kamernieuws/eindverslag-onderzoek-kinderopvangtoeslag-overhandigd.
16 Andriessen e.a. maart 2020, p. 52-55.

De in dit onderzoek te formuleren aanbevelingen voor een rechtsstatelijk gebruik van algoritmen, Big Data-analyse en profiling door de Nederlandse Belastingdienst kunnen dienen als startpunt voor soortgelijke aanbevelingen voor andere overheidsorganisaties.

Daarnaast kan het inzichtelijk maken van de risico's die kleven aan de inzet van algoritmen, Big Data-analyse en profiling bijdragen aan toekomstig (vervolg)onderzoek naar andere methoden om deze risico's te mitigeren. Verder kunnen de te formuleren aanbevelingen ook waardevol zijn voor andere belastingadministraties die algoritmen, Big Data-analyse en profiling inzetten. Dit onderzoek kan daarom ook bruikbaar zijn voor andere belastingadministraties die een rechtsstatelijke inzet hiervan willen waarborgen.

1.4 Methodologie

In dit onderzoek zal gebruik worden gemaakt van de klassiek juridische onderzoeksmethode en in beperkte mate van de rechtsvergelijkende onderzoeksmethode. Bij de klassiek juridische onderzoeksmethode worden juridische literatuur, relevante wet- en regelgeving en jurisprudentie uit één enkel rechtssysteem geraadpleegd. Bij de rechtsvergelijkende onderzoeksmethode wordt juist een vergelijking gemaakt tussen verschillende rechtssystemen. Daarnaast zal voor de beantwoording van de eerste deelvraag niet-juridisch georiënteerd literatuuronderzoek uitgevoerd worden. Hierbij zal met name in Google Scholar gezocht worden naar relevante literatuur op het gebied van algoritmen, Big Data-analyse en profiling. Hierbij zal de sneeuwbalmethode gehanteerd worden. Voor de beantwoording van de overige deelvragen zal gezocht worden in de juridische dogmatiek, de geldende wet- en regelgeving en eventuele relevante rechtspraak. Hierbij zullen databanken als NDFR, Kluwer Navigator, EUR-Lex, Jura en Google Scholar geraadpleegd worden. Via deze databanken is ook wet- en regelgeving te vinden. Ook hier zal de sneeuwbalmethode gehanteerd worden.

1.5 Leeswijzer

Om tot een beantwoording van de onderzoeksvraag te komen, zal allereerst in hoofdstuk 2 uiteengezet worden wat wordt verstaan onder algoritmen, Big Data-analyse en profiling. Vervolgens zal in hoofdstuk 3 kort stilgestaan worden bij het gebruik van deze technieken door de Nederlandse Belastingdienst. Na deze verkenning zal in hoofdstuk 4 het begrip transparantie in relatie tot het gebruik van deze slimme opsporingstechnieken geduid worden. In hoofdstuk 5 zal vervolgens aandacht worden besteed aan het belang van transparantie van deze technieken. Daarna zal in hoofdstuk 6 ingezoomd worden op de al bestaande richtinggevende kaders, hulpmiddelen en een good practice van het gebruik van algoritmen, Big Data-analyse en profiling door overheidsinstanties in het algemeen. Alvorens tot een conclusie te komen zullen in hoofdstuk 7 aanbevelingen voor het waarborgen van (een) rechtsstatelijke (inzet van) algoritmen, Big Data-analyse en profiling gegeven worden. Deze aanbevelingen richten zich met name op het waarborgen van het gelijkheidsbeginsel. Aanvullend dragen zij ook bij aan het waarborgen van andere rechtsstatelijke beginselen zoals het recht op privacy.

2 Algoritmen, Big Data-analyse en profiling

2.1 Een wervelwind aan data

Zoals al is gesteld, dienen belastingadministraties een steeds grotere stroom aan data te verwerken. In 2020 ontving de Nederlandse Belastingdienst bijna tien miljoen aangiften in twee maanden tijd[1], in een korte periode komt daarom een gigantische hoeveelheid data binnenstromen. Zonder de toepassing van technieken om die dataverwerking te versnellen en (deels) te automatiseren zouden de belastingadministraties niet in staat zijn om onder meer hun taak van belastingheffing adequaat uit te voeren. Zij maken daarom gebruik van algoritmen, Big Data-analyse en profiling.

2.2 Algoritmen

2.2.1 *Wat zijn algoritmen?*

Een algoritme is een eindige reeks aan opvolgende instructies die moeten leiden tot het bereiken van een bepaald doel.[2] Een handleiding voor het in elkaar zetten van een kast of een recept voor een taart zijn daarmee in feite ook algoritmen. Echter, algoritmen worden doorgaans geassocieerd met computers, wiskunde en/of cijferreeksen.

Het woord algoritme is vernoemd naar de Perzische wiskundige Abu Abdallah Muhammad ibn Musa al-Khwarizmi, die in de negende eeuw leefde.[3] Eén van de grootste werken van Al-Khwarizmi is *Arithmetic*. Arndt schrijft hierover: 'One well-read Latin translation begins with the words Dixit algorizmi, or 'Algorithm says,' and follows with instructions for making various computations. Thus algorithm, a Latinized version of the mathematician's name, has come to its present meaning of general computational procedure.'[4]

Voor de komst van het woord algoritme bestonden al berekeningsmethodes. Het Euclides algoritme is er daar één van. Het algoritme, dat in 300 voor Christus is geformuleerd door Euclides, vindt de grootste gemeenschappelijke deler van twee

1 Zie hiervoor: 'Bijna 10 miljoen aangiften binnengekomen bij de Belastingdienst, rijksoverheid.nl/actueel/nieuws/2021/05/11/bijna-10-miljoen-aangiften-binnen-gekomen-bij-belastingdienst.
2 Engelsman 'De impact van algoritmes'.
3 Arndt 1983, p. 668.
4 Arndt 1983, p. 670.

getallen.[5] Het toe te passen stappenplan is gemakkelijk te gebruiken en vereist geen inzicht in de problematiek. Om tot de formulering te komen, is bij de bedenker Euclides echter veel inzicht aanwezig geweest.[6]

Het Euclides algoritme is zo geformuleerd dat het altijd het correcte antwoord zal geven, dat is wiskundig bewezen. Dergelijke algoritmen heten 'deterministische algoritmen'. 'Een deterministisch algoritme is een algoritme dat louter bepaald wordt door zijn input, zonder dat willekeur daarbij is betrokken en geeft altijd dezelfde *output* (cursivering door auteur).'[7] Hiertegenover staan 'niet-deterministische algoritmen'. Niet-deterministische algoritmen kunnen bij één input meerdere outputs (uitkomsten) krijgen. Bij niet-deterministische algoritmen is altijd sprake van een kans. Door de aanwezigheid van deze kans zullen deze algoritmen niet altijd aantoonbaar correcte outputs geven.

Het algoritme kan ook niet-wenselijke of niet-correcte uitkomsten geven. Engelsman omschrijft dit met een voorbeeld over de treindienstregeling.[8] Als een stuk spoor wordt verwijderd, dan is het model van vóór de verwijdering van dit stuk spoor geen juiste representatie meer van de werkelijkheid. Hierdoor zal het algoritme niet langer correct functioneren.

In de tijd van Euclides en Al-Khwarizmi waren de problemen waar algoritmen voor werden ingezet relatief beperkt in omvang. Rekenkracht was beperkt beschikbaar en ook waren er weinig bekende data. Tegenwoordig zijn de problemen die worden opgelost met behulp van algoritmen veel groter in omvang. Hiervoor is een grote rekenkracht vereist welke doorgaans niet door de mens kan worden geleverd, maar slechts door een computerprogramma.

Mede door de inzet van computers is een grote variëteit aan soorten algoritmen ontstaan. Dit onderzoek richt zich op 'niet-deterministische algoritmen' en beperkt zich daarbij tot het onderscheid tussen zogenaamde 'niet-zelflerende' en 'zelflerende' algoritmen. Niet-zelflerende algoritmen kennen een 'als dit, dan dat' structuur. Zij volgen een gegeven, vooraf vastgestelde set aan instructies op.[9] Een sensorlamp bijvoorbeeld werkt op basis van een niet-zelflerend algoritme. Als de sensor beweging waarneemt, dan gaat de lamp aan. Hier is het 'als dit, dan dat' karakter in te herkennen. Een niet-zelflerend algoritmen volgt altijd dezelfde stappen, deze veranderen niet. Echter, doordat de stappen niet dusdanig zijn geformuleerd dat zij altijd dezelfde uitkomst gegeven, zullen zij – ondanks dat zij altijd dezelfde stappen volgen – niet altijd dezelfde uitkomst geven. Een simpel voorbeeld is een algoritme in een auto die het volgende stappenplan volgt: start bij de kerk met rijden, neem bij ieder kruispunt, t-splitsing of rotonde een willekeurige afslag en stop na 100 kilometer met

5 Zie o.a. Engelsman 'De impact van algoritmes' en Bultheel & Van Barel 1996.
6 Engelsman 'De impact van algoritmes'.
7 'Deterministic Algorithm' raadpleegbaar via techopedia.com/definition/18830/deterministic-algorithm.
8 Engelsman 'De impact van algoritmes'.
9 Vetzo, Gerards & Nehmelman 2018, p. 48.

rijden. Als het algoritme meerdere keren deze stappen opvolgt – starten bij de kerk, een willekeurige afslag nemen en na 100 kilometer stoppen – dan eindigt het algoritme niet iedere keer op dezelfde plaats, ondanks dat het steeds dezelfde stappen heeft gevolgd. De stap 'neem een willekeurige afslag bij ieder kruispunt, t-splitsing of rotonde' is namelijk afhankelijk van een kans. De eerste keer dat het algoritme het stappenplan opvolgt kan het bij het eerste kruispunt linksaf slaan, terwijl het algoritme de tweede keer bij het eerste kruispunt rechtsaf kan slaan. Hierdoor is de uitkomst niet altijd hetzelfde, terwijl het bij ieder kruispunt, t-splitsing of rotonde wel dezelfde handeling uitvoert (een willekeurige afslag nemen).

Kortom, afhankelijk van de inputdata volgt een niet-zelflerend, niet-deterministisch algoritme een vooraf vastgestelde set aan instructies op en gedraagt zich zodoende altijd op dezelfde wijze, maar zal niet altijd dezelfde uitkomst hebben. Niet-zelflerende algoritmen zijn, doordat zij zich steeds op dezelfde wijze gedragen, statisch.

Zelflerende algoritmen daarentegen zijn dynamisch en gedragen zich niet altijd op dezelfde wijze. Zij maken een analyse van de inputdata, afhankelijk van die analyse verandert de set aan instructies. Deze nieuwe set aan instructies wordt de volgende keer dat het algoritme wordt gebruikt, gevolgd. Hierdoor evolueert het zelflerende algoritme en kan eenzelfde input de tweede keer tot een andere output leiden. Het algoritme leert zogezegd van de inputdata. Voordat een zelflerend algoritme gebruikt wordt, wordt het getraind met trainingsdata.

Een algoritme dat een voorwerp moet herkennen, krijgt tijdens de training een reeks aan foto's van voorwerpen te zien. Als het algoritme getraind wordt om bijvoorbeeld een pen te herkennen, dan hebben de foto's onderschriften als 'geen pen' of 'pen'. Hierdoor kan het algoritme getraind worden om het verschil tussen een potlood en een pen te herkennen. Die set aan foto's aan de hand waarvan het algoritme wordt getraind, wordt trainingsdata genoemd. Een grotere en meer diverse set aan trainingsdata, zal leiden tot een algoritme dat beter in staat is tot het herkennen van pennen, dan een algoritme dat is getraind op een kleinere, minder diverse set aan trainingsdata. Een dergelijk zelflerend algoritme leert van de input en de gemaakte observaties. De observaties worden toegevoegd aan de trainingsdata waardoor de kennis van het algoritme groeit en het steeds beter in staat zal zijn om pennen te herkennen.[10]

2.2.2 *Algoritmiek*

Het vakgebied dat zich bezighoudt met het ontwerp en de analyse van algoritmen wordt algoritmiek genoemd.[11] Algoritmiek stelt zich ten doel om allerlei probleemstellingen op te lossen. Om dit te realiseren is het uiteraard van belang dat het

10 Vetzo, Gerards & Nehmelman 2018, p. 48.
11 Bodlaender maart 2017, p. 43.

algoritme correct functioneert. Wil men spreken over een goed algoritme, dan is daarvoor ook vereist dat het efficiënt is.[12]

De mate van efficiëntie van een algoritme kan op verschillende wijzen gemeten worden. Zo wordt de efficiëntie uitgedrukt in het aantal te volgen stappen of in de benodigde hoeveelheid opslag.[13] De grootheid tijd, gemeten in seconden, lijkt wellicht voor de hand liggend voor het uitdrukken van de mate van efficiëntie. Echter, de gebruikte tijd is afhankelijk van de gebruiker van het algoritme, bijvoorbeeld een computer of een natuurlijk persoon, en daarom niet objectief meetbaar. Zodoende is het aantal te nemen stappen een meer objectieve maatstaf. Belangrijk daarbij is wel dat de mate van efficiëntie uitgedrukt in stappen afhankelijk is van de hoeveelheid input. Bij het Euclides algoritme bijvoorbeeld, duurt het vinden van de grootste gemeenschappelijke deler van twee getallen door eenzelfde gebruiker langer naar mate de twee gekozen getallen groter zijn. Soms is efficiëntie uitdrukken in stappen daarom minder geschikt.

Voor de mate van efficiëntie is de benodigde hoeveelheid opslag van de gebruiker, een computer, van het algoritme eveneens van belang. Een computer met meer beschikbaar geheugen kan sneller gegevens verwerken dan een verder identieke computer met minder beschikbaar geheugen. De computer die het algoritme gebruikt, is daarom relevant. Dient het algoritme toegepast te worden met gebruikmaking van weinig beschikbaar geheugen, dan zal dit ten koste gaan van de snelheid van het algoritme. Andersom zal meer beschikbaar geheugen zorgen voor een hogere snelheid. De snelheid van de computer is zodoende afhankelijk van het beschikbare, vrije geheugen.

Binnen de algoritmiek worden enkele moeilijkheden onderkend zoals de combinatorische explosie en de data-explosie. De combinatorische explosie is het verschijnsel van een exponentiële groei van het aantal mogelijke oplossingen naarmate het zoekgebied wordt vergroot.[14] Data-explosie is het fenomeen van de productie van steeds meer gegevens waardoor het vinden van de juiste oplossing van de probleemstelling wordt bemoeilijkt.

2.3 Big Data-analyse

Het begrip big-data-analyse bestaat uit twee delen: ‘Big Data’ en ‘-analyse’. Talloze definities van het begrip Big Data zijn in omloop. Letterlijk vertaald, betekent Big Data ‘grote hoeveelheid gegevens’. Zo veel gegevens dat reguliere data-analyses onvoldoende capaciteit bieden om de grote hoeveelheid data te verwerken. Hierna zal een definitie gegeven worden voor het begrip Big Data en vervolgens voor Big Data-analyse.

12 Engelsman ‘De impact van algoritmes’.
13 Bodlaender maart 2017, p. 43.
14 Bodlaender omschrijft de combinatorische explosie met het Königsberger bruggenprobleem. Om hier niet te ver in de diepte te treden, verwijs ik hier graag naar: Bodlaender maart 2017, p. 43.

2.3.1 *Wat is Big Data?*

Naast de talloze definities van Big Data, pogen veel artikelen te komen tot een alom breed gedeelde, bekende definiëring van Big Data.[15] Hier zullen deze artikelen als uitgangspunt dienen. Raadpleging van de veelheid aan literatuur op het gebied van Big Data is ondoenlijk. Daarnaast is het efficiënter om gebruik te maken van de al bestaande uiteenzettingen van de verschillende definities van Big Data.

Traditioneel wordt Big Data omschreven met zijn karakteristieken: de 'drie V's': *velocity*, *volume* en *variety*. *Velocity* duidt op de verwerkingssnelheid van de data, *volume* op de grote hoeveelheid data en *variety* op de diversiteit aan data.[16] In de loop der tijd zijn aan deze drie V's nog andere karakteristieken toegevoegd, waaronder twee aanvullende V's: *veracity* en *value*.[17]

Veracity, waarheidsgetrouwheid, maakt duidelijk dat bij een groot volume, een grote variëteit en een hoge verwerkingssnelheid de kans op volledig correcte data niet bestaat.[18] Het gedeelte van de data dat incorrect is, 'vervuilt' de rest van de data, hetgeen kan leiden tot een incorrect resultaat van het algoritme. Volgens Khan, Uddin en Gupta is *veracity* niet hetzelfde als *validity*.[19] Zij stellen namelijk dat *validity* (een andere V die onderkend kan worden), in tegenstelling tot *veracity*, afhankelijk is van de mate waarin de gebruiker de data begrijpt en correct gebruikt. De relatie tussen elementen van data dient geverifieerd te worden, ook bij data met een hoge waarheidsgetrouwheid. Als al deze V's in acht worden genomen, dan kan Big Data van grote waarde zijn, gebeurt dat niet, dan is het nutteloos.[20] Dat maakt de laatste V, *value*, zo belangrijk.

Hoewel de traditionele definitie van Big Data bestaande uit verschillende V's breed gedeeld is, wordt ook aandacht besteed aan een meer praktische definitie.[21] Hierbij wordt Big Data veelal gekoppeld aan een digitaal aspect en aan het gebruik of de toepassing ervan. Deze aspecten zijn ook terug te vinden in de definitie van het directoraat-generaal Justitie en Consumentenzaken, welke als volgt luidt: 'grote

15 Zie onder meer De Mauro, Greco & Grimald, 'A formal definition of Big Data based on its essential features', 2016; Favaretto e.a., 'What is your definition of Big Data? Researchers' understanding of the phenomenon of the decade', 25 februari 2020, PLoS ONE 15(2): e0228987. doi.org/10.1371/journal.pone.0228987; Emmanuel & Stanier, 'Defining Big Data', 10 november 2016; Ward & Barker, *Undefined By Data: A Survey of Big Data Definitions,* 20 september 2013, ArXiv, abs/1309.5821; Gandomi & Haider, 'Beyond the hype: Big data concepts, methods, and analytics', *International Journal of Information Management*, april 2015, vol. 35, iss. 2, p. 137-144; en Ylijoki, & Porras, 'Perspectives to Definition of Big Data: A Mapping Study and Discussion', *Journal of Innovation Management* 2016, vol. 4, no. 1, p. 69-91.

16 Favaretto e.a. 2020, p. 2.

17 Ishwarappa & Anuradha 2015, p. 320-321.

18 Ishwarappa & Anuradha 2015, p. 321.

19 Khan, Uddin & Gupta 2014.

20 Ishwarappa & Anuradha 2015, p. 321.

21 Favaretto e.a. 25 februari 2020.

hoeveelheden uiteenlopende gegevens die worden ontleend aan verschillende soorten bronnen, zoals personen, machines of sensoren'.[22] Het kan daarbij gaan om 'klimaatgegevens, satellietbeelden, digitale afbeeldingen en video's, gegevens over transacties of GPS-signalen. Big Data kan persoonsgegevens bevatten: dat wil zeggen, gegevens die betrekking hebben op een persoon, zoals een naam, een foto, een e-mailadres, bankgegevens, posts op online sociale netwerken, medische gegevens of het IP-adres van een computer.'

Ook De Mauro, Greco en Grimaldi verwerken in hun definitie van Big Data de toepassing en het doel ervan: 'Big Data is the Information asset characterised by such a High Volume, Velocity and Variety to require specific Technology and Analytical Methods for its transformation into Value'.[23] Zij vinden dat de definitie van Big Data zou moeten verwijzen naar de meest pure karakteristiek ervan, namelijk informatievoorziening. De toevoeging *Technology* duidt op het feit dat niet alle data die tegenwoordig wordt beschouwd als Big Data ook echt een grote omvang betreft. Zo worden berichten op Instagram, Twitter, TikTok of andere sociale media veelal beschouwd als Big Data, terwijl hun omvang, per afzonderlijk bericht, relatief beperkt is.[24] Big Data gaat vanuit die gedachte veel meer over 'een cultureel, technologisch en wetenschappelijk fenomeen' en veel minder over de grote omvang van data.[25] *Analytical Methods* verwijst naar de wijze waarop de data wordt verwerkt. Eerder werd inzichtelijk dat de wijze waarop informatie wordt verwerkt de mate van validiteit, of *validity*, bepaalt en dat dit is onderkend als een karakteristiek van Big Data.

Op deze laatstgenoemde definitie, dat Big Data informatiemiddelen zijn van een bepaald volume, snelheid en verscheidenheid waardoor specifieke technologieën en analytische methoden vereist zijn om waarden te creëren, is echter ook commentaar gekomen.[26] Kritiek is onder meer dat ook deze definitie nog steeds grotendeels gebouwd is op de drie V's, en daardoor onvoldoende praktisch in gebruik is. Om de drie V's goed te kunnen doorgronden is namelijk een bepaalde voorkennis van ICT vereist. Het gebruik van de drie V's als bouwstenen voor de definitie van Big Data is hierdoor niet praktisch toepasbaar. Veel gebruikers van Big Data hebben namelijk niet de technische (voor)kennis om de drie V's direct te doorgronden. Big Data wordt bovendien op heel veel verschillende manieren ingezet en heeft daardoor niet altijd dezelfde karakteristieken.[27] Zo concluderen Kitchen en McArdle dat Big Data, om tot een definitie te komen, verdeeld moet worden in kleinere subcategorieën gesorteerd op basis van de inzet en de verschillende doeleinden van de Big Data.[28]

Door de gevarieerde inzet zal het begrip nimmer gevat kunnen worden in algemeenheden, ofwel in één algemeen, erkende definitie. Favaretto en anderen stellen

22 European Commission 7 juni 2022.
23 De Mauro, Greco & Grimaldi 2016.
24 Boyd & Crawford 2012, p. 2-3.
25 Boyd & Crawford 2012, p. 2-3.
26 Zie voor een uitgebreide toelichting hierop Favaretto e.a. 25 februari 2020, p. 3-4.
27 Kitchen & McArdle 2016, p. 9.
28 Kitchen & McArdle 2016, p. 9.

daarom: 'In order to correctly capture the essence and characteristics of Big Data, it might be necessary to deconstruct or unfold the term into its different constituents, thus shifting from broad generalities to specific qualities relevant not only for scientists, but also for ethics committees and regulators'.[29] Zij geven aan dat naar hun mening verder onderzoek nodig is om tot conceptuele overeenstemming te komen over wat Big Data nu precies is.

Desondanks, zal voor dit onderzoek een definitie van Big Data gehanteerd moeten worden. Aangezien dit een juridisch onderzoek betreft dat gericht is op Big Data verwerking door belastingadministraties is een technische definitie van het woord niet noodzakelijk. Zodoende is de definitie van Big Data van het directoraat-generaal Justitie en Consumentenzaken, door zijn juridische en praktische karakter, het meest passend voor dit onderzoek. Het woord 'groot' uit deze definitie is een relatief begrip. Wat de één als groot beschouwt, beschouwt de ander wellicht als klein. De definitie hiervan verschilt zodoende van persoon tot persoon en is bovendien afhankelijk van tijd. Wat nu als groot wordt beschouwd, kan, in het licht van technologische ontwikkelingen, over een tijd als klein worden beschouwd.[30] Om deze reden is 'grote hoeveelheden' vervangen door 'enorme hoeveelheden'. Het begrip enorm heeft een massaler karakter en is daarom minder subjectief.

In aanvulling zal nog verwezen worden naar de meest pure karakteristiek van Big Data, informatievoorziening, welke De Mauro, Greco en Grimaldi cruciaal achten voor de definiëring van Big Data.

Big Data wordt hier daarom gedefinieerd als 'enorme hoeveelheden uiteenlopende gegevens die worden ontleend aan verschillende soorten bronnen, zoals personen, machines of sensoren, waarbij het kan gaan om een verscheidenheid aan soorten gegevens', die dienen ter informatievoorziening.[31]

2.3.2 *Wat is Big Data-analyse?*

Big Data-analyse is het zoeken naar clusters, regelmatigheden of patronen in grote hoeveelheden, verschillende data die vrijwel altijd constant en actueel zijn. Dat was vroeger anders. Bij traditionele data-analyse werd veelal gebruikgemaakt van op een specifiek tijdstip verzamelde data, tegenwoordig is echter vrijwel altijd een constante stroom aan actuele data beschikbaar die direct wordt verzameld en geanalyseerd.[32]

Ook bij de analyse van Big Data speelt het al aangehaalde subjectieve karakter van het begrip 'groot' een rol. Een zogenaamd kantelpunt bestaat waarop traditionele data-analyses niet langer in staat zijn om de hoeveelheden data te verwerken. Vanaf

29 Favaretto e.a. 25 februari 2020, p. 17.
30 Dit wordt ook erkent door Vetzo, Gerards & Nehmelman 2018, p. 17.
31 Directorate-General for Justice and Consumers januari 2018.
32 Vetzo, Gerards & Nehmelman 2018, p. 17.

dat kantelpunt – welke verschilt per toepassingsgebied – vindt de omslag plaats van traditionele data-analyse naar Big Data-analyse.

Volgens Zwenne, Steenbruggen en Reker wordt Big Data-analyse in algemene zin gebruikt om verbanden of patronen te vinden in grote hoeveelheden data die moeilijk te analyseren zijn op basis van vooraf opgestelde hypotheses en vraagstellingen.[33] Vetzo, Gerards en Nehmelman maken een vergelijkbare constatering. Zij geven aan dat het doel van data-analyse vroeger het bevestigen van een vooraf opgestelde hypothese betrof, waarbij de uitkomst van de data-analyse binnen de kaders van die vooraf opgestelde hypothese bleef, terwijl algoritmen tegenwoordig ook zoeken naar nog onontdekte patronen en verbanden.[34] Hierdoor blijft de uitkomst van de data-analyse niet binnen het bereik van de door de mens opgestelde hypothese en kunnen veel meer patronen en verbanden geconstateerd worden. Zo kan nieuwe, relevante informatie worden gedestilleerd uit de beschikbare data.[35] De capaciteit, in rekenkracht, van algoritmen om te zoeken naar patronen en verbanden is immers vele malen groter dan die van de mens.

De gevonden statistische verbanden of correlaties zijn niet altijd te verklaren of aantoonbaar causaal, wel kan er doorgaans een patroon in gevonden worden waardoor zij een voorspellende waarde krijgen.[36] De gevonden voorspellende waarde kan dan worden vertaald naar bijvoorbeeld een risicoprofiel. Toezichthoudende organen en andere instanties, welke veelal beschikken over veel persoonlijke gegevens, maken bij de uitvoering van hun opsporende en toezichthoudende taak steeds frequenter gebruik van deze techniek van Big Data-analyse, zo ook de Belastingdienst.

2.4 **Profiling**

2.4.1 ***Wat is profiling?***

Profiling is de Engelse term voor profileren. Profileren is een ander woord voor karakteriseren. Men kan zichzelf profileren, in dat geval schetst men een beeld van zichzelf en over zijn of haar karakteristieken. Profiling kan ook generiek plaatsvinden. In dat geval worden algemene profielen opgesteld die een bepaald beeld schetsen. Een profiel is in dit verband een set aan karakteristieken. Dat kunnen uiterlijke of innerlijke karakteristieken zijn, waarbij de laatste zien op het doen en laten van een persoon, op de keuzes die hij of zij (heeft ge)maakt.

De door de Europese Commissie voorgestelde General Data Protection Regulation geeft in art. 4, lid 4 een definitie van profiling. Volgens dit artikel betekent profiling ‘any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular

33 Zwenne, Steenbrugen & Reker 2016, p. 34.
34 Vetzo, Gerards & Nehmelman 2018, p. 18.
35 Vetzo, Gerards & Nehmelman 2018, p. 18.
36 Zwenne, Steenbrugen & Reker 2016, p. 35.

to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements'.

Belangrijke aspecten van deze definitie zijn dat het moet gaan om 'persoonlijke gegevens' van een 'natuurlijk persoon' en om een 'persoonlijk optreden' op basis waarvan een 'voorspelling' gemaakt kan worden. Persoonlijke gegevens zijn volgens de General Data Protection Regulation gegevens die terug te leiden zijn naar een natuurlijk persoon welke direct of indirect identificeerbaar is.

Deze identificatie geschiedt voornamelijk op basis van een identificator zoals naam, locatiegegevens of meer specifieke gegevens over de identiteit van de natuurlijke persoon zoals fysiologische, genetische, psychische, economische, culturele of sociale kenmerken van die natuurlijk persoon.[37]

Verder heeft profilering een voorspellende werking op basis van persoonlijk handelen. Dat persoonlijk handelen is gebaseerd op de gemaakte keuzes van een individu en valt daarmee terug op de karakteristieken van een persoon.

Er worden door verschillende (overheids)organisaties tal van profielen opgesteld. In zekere zin zijn zij te vergelijken met stereotypen. Als men denkt aan een boer, dan denkt men, bewust of onbewust, aan bepaalde eigenschappen, karakteristieken, die kenmerkend zijn voor een boer. Bijvoorbeeld het dragen van een overall en klompen. Voldoet iemand aan zulke kenmerkende of typerende karakteristieken, dan valt diegene binnen het opgestelde profiel. De kans blijft echter altijd bestaan dat iemand die voldoet aan deze karakteristieken geen boer is.

Met de komst van Big Data en Big Data-analyse worden gemakkelijker en meer kenmerkende of typerende karakteristieken, met een voorspellende waarde, gevonden. Profiling in de context van Big Data kan volgens Hildebrandt omschreven worden als: 'a set of technologies, which share at least one common characteristic: the use of algorithms or other techniques to create, discover or construct knowledge from huge sets of data'.[38] Het gaat om automatische profilering, profilering zonder tussenkomst van de mens, waarbij zelflerende algoritmen worden gebruikt. Cruciaal hiervoor is de eerder besproken Big Data-analyse waarbij algoritmen in grote hoeveelheden data op zoek gaan naar nog onontdekte verbanden en patronen met een voorspellende waarde. Deze vorm van Big Data-analyse noemt men *data mining*.[39] Profileren is dan het voorspellen van de kans dat iets zich voordoet bij de aanwezigheid van bepaalde verbanden en/of patronen, die zijn aangetroffen in vergelijkbare situaties uit het verleden. Een belangrijke constatering is dat daarbij niets wordt gezegd over waarom die kans zich voordoet. Profielen zijn in dat licht hypotheses die niet zijn gegrond op

37 Art. 4 lid 1 van de General Data Protection Regulation.
38 Hildebrandt 2008, p. 17.
39 Hildebrandt 2008, p. 18.

een theoretische of logische verklaring, maar slechts op dat wat de data voorspellen, zonder een verklaring waarom.[40]

2.4.2 *Risicoprofielen*

Het voorspellen van een kans dat iets zich voordoet is een belangrijk doel van profileren. Bij belastingadministraties is het doel van profileren bijvoorbeeld het voorspellen van de kans dat een natuurlijk- of rechtspersoon een onjuiste aangifte indient. Abdul-Aliyeva en Van Eijk noemen dit het 'identificeren van potentiële regel- of wetsovertredingen'.[41] Hiervoor worden risicoprofielen gebruikt. Die risicoprofielen bevatten bepaalde kenmerken, ook wel selectiecriteria genoemd. De ontwikkelaar van het risicoprofiel heeft de overtuiging dat de selectiecriteria verband houden met een grotere kans om een norm, voorschrift of wet te overtreden.[42] Als aan een selectiecriteria is voldaan, levert dat een bepaalde score op. De hoogte van de score bepaalt het risico op een onjuist ingediende aangifte. Een dergelijke risicoschifting is noodzakelijk, omdat het voor belastingadministraties onmogelijk is om alle aangiften handmatig te controleren. Een belangrijk kenmerk van risicoprofielen is dat rechtshandhavingsinstanties de profielen *proactief* inzetten, dat houdt in 'zonder concrete, geïndividualiseerde verdenking van normovertreding jegens een persoon' (cursivering door auteur).[43]

Ondanks de noodzaak van risicoprofilering dient zorgvuldig omgegaan te worden met het opstellen van de risicoprofielen. Geabstraheerd dient te worden van *racial profiling*, ook wel vertaald naar etnisch profileren.[44] Etnisch profileren is aan de orde wanneer rechtshandhavingsinstanties profileren op grond van (een combinatie van) ras, huidskleur, afkomst, of nationale of etnische oorsprong of andere persoonlijke kenmerken zoals godsdienst, geslacht of gender, seksuele gerichtheid, handicap, leeftijd of migratie- of werkstatus, zonder objectieve criteria of redelijke rechtvaardiging in een specifieke context zoals het controleren van fouten in de belastingaangiften.[45]

2.5 Tussenconclusie: slimme opsporingstechnieken

In dit hoofdstuk zijn de begrippen algoritmen, Big Data-analyse en profiling gedefinieerd. Dit zijn drie verschillende technieken die allemaal ingezet kunnen worden bij opsporing. Bij belastingadministraties is dat veelal de opsporing van risicovolle aangiften. Het huidige tijdperk geeft deze technieken een digitaal en groots karakter. Door de inzet van de technieken met computers gaat het opsporen van risico's in de aangiften veel sneller. Daarnaast wordt door de inzet van de verschillende

40 Hildebrandt 2008, p. 18.
41 Abdul-Aliyeva & Van Eijk januari 2023, p. 291.
42 Abdul-Aliyeva & Van Eijk januari 2023, p. 292.
43 Abdul-Aliyeva & Van Eijk januari 2023, p. 291.
44 Abdul-Aliyeva & Van Eijk januari 2023, p. 291.
45 UN Committee on the Elimination of Racial Discrimination 17 december 2020, p. 3-4.

technieken veel slimmer omgegaan met de capaciteit van de belastingadministraties.[46] Zodoende zal in het vervolg van dit onderzoek voortaan voornamelijk naar deze drie technieken, algoritmen, Big Data-analyse en profiling, verwezen worden met de overkoepelende term 'slimme opsporingstechnieken'.

46 Tijdens het algemeen overleg op 8 oktober 2014 noemde toenmalig Staatssecretaris Wiebes van Financiën de nieuwe werkwijze ook slim. Zie hiervoor *Kamerstukken II* 2014/15, 31066, nr. 222, p. 20.

3 Het gebruik van slimme opsporingstechnieken – Toen en nu

In het vorige hoofdstuk is antwoord gegeven op deelvraag 1: 'Wat is de definitie van algoritmen, Big Data-analyse en profiling?' Algoritmen zijn gedefinieerd als 'een eindige reeks aan opvolgende instructies die moeten leiden tot het bereiken van een bepaald doel'. Big Data-analyse als 'het zoeken naar clusters, regelmatigheden of patronen in grote hoeveelheden, verschillende data die vrijwel altijd constant en actueel is'. En profiling als 'het voorspellen van de kans dat iets zich voordoet bij de aanwezigheid van bepaalde verbanden en/of patronen tussen karakteristieken, die zijn getrokken uit vergelijkbare situaties uit het verleden'. De drie technieken zijn vervat onder de algemeen overkoepelende term 'slimme opsporingstechnieken'.

In dit hoofdstuk zal kort het (historisch) gebruik van deze slimme opsporingstechnieken binnen de Nederlandse Belastingdienst gegeven worden.

3.1 De Nederlandse Belastingdienst

De belastingheffing heeft in Nederland niet altijd centraal plaatsgevonden.[1] Pas in 1806 kwam daar onder leiding van toenmalige minister van Financiën Isaäc Gogel verandering in.[2] Gogel richtte een centrale belastingadministratie op. Vanaf die oprichting beschikt de belastingadministratie over verscheidene gegevens van belastingplichtigen. Het aantal gegevensstromen neemt alsmaar toe en daarmee ook het belang van de kwaliteit van de verzamelde gegevens.[3] In de twintigste eeuw wordt een belastinginformatiesysteem ontwikkeld en vanaf de jaren dertig worden, om redenen van doelmatigheid, delen van administratieve processen gemechaniseerd. Nog een aantal jaren later, in 1966, is de eerste geautomatiseerde database van de belastingadministratie geboren. Sindsdien vindt de verwerking van gegevens van belastingplichtigen automatisch plaats. Vanaf 1975 gaat deze verbetering van de informatievoorziening en de automatisering alsmaar door en vindt, zoals Arendsen dat noemt, innovatie van de administratieve organisatie van de Belastingdienst plaats.[4]

1 Er zal hier niet uitvoerig in worden gegaan op de geschiedenis van de wijze van belastingheffing in Nederland. Arendsen 2016, p. 27 verwijst voor een uitvoerige uiteenzetting van de geschiedenis van de Nederlandse belastingdienst naar het boek *Op gelijke voet* van Pfeil uit 2009.
2 Dusarduijn, in: *Inleiding belastingheffing ondernemingen en particulieren* 2012, p. 12.
3 Zie voor de hier geschetste ontwikkelingen Arendsen 2016, p. 27.
4 Arendsen 2016, p. 27.

De trend van verdergaande automatisering en informatisering zet zich voort, evenals het gebruik van computers. In 2005 stellen de Belastingdienst en het Centraal Bureau Statistiek het voor een aantal berichtenstromen verplicht om gegevens ten behoeve van de belastingheffing digitaal aan de Nederlandse Belastingdienst aan te leveren.[5] Tegenwoordig maakt de Belastingdienst gebruik van digitale gegevensportalen. 'Het gegevensportaal is bedoeld voor het aanleveren van gegevens door: kinderopvangorganisaties, gastouderbureaus, autoleasebedrijven, financiële instellingen, zoals banken, verzekeraars en beleggingsinstellingen, bedrijven, stichtingen, verenigingen en anderen die bedragen aan derden hebben betaald en OV-bedrijven'.[6]

Arendsen omschrijft deze ontwikkeling als volgt: 'Door de jaren heen groeit zo een door middel van digitale gegevensstromen en gegevensverzamelingen verknoopte samenleving, de informatiesamenleving, ofwel iSamenleving met een iOverheid[7] en een iBelastingdienst'.[8]

Inmiddels heeft deze ontwikkeling geleid tot het inzetten van slimme opsporingstechnieken waar de Belastingdienst voor de uitoefening van zijn taken steeds vaker gebruik van maakt. Dat doet hij (onder meer) bij de controle op de aangiften inkomstenbelasting en bij de btw-teruggaven. Het is een data gedreven aanpak die het selectieproces van de Belastingdienst dient te ondersteunen.[9] Hier worden risicomodellen en selectieregels voor ontwikkeld en ingezet.

De Algemene Rekenkamer omschrijft een risicomodel als 'een berekening op basis van data die de kans op een fout in de aangifte weergeeft met een percentage'.[10] Selectieregels sporen afwijkingen van normbedragen en inconsistenties in de aangifte op.[11] Hierbij wordt een onderscheid gemaakt tussen 'gladde' en 'niet-gladde' gevallen.[12] Als een afwijking wordt geconstateerd of als de kans op een fout in de aangifte hoog is, dan is sprake van een niet-glad geval, de aangifte komt dan in de 'uitworp' terecht. De uitworp is een advies aan de inspecteur of controleur om de betreffende aangifte, of btw-teruggave, handmatig te controleren. Het staat de inspecteur of controleur vrij om van dit advies af te wijken.[13] Recentelijk is door de Hoge Raad bevestigd dat het afwijken van een uitworp geen ambtelijk verzuim oplevert indien de niet-onwaarschijnlijke mogelijkheid zich voordoet dat de aangifte juist is.[14] Het uitwerpen van niet-gladde gevallen wordt aangeduid met de term *triaging*.

5 Arendsen 2008, p. 20.
6 Zie hiervoor 'Gegevensportaal', raadpleegbaar via belastingdienst.nl/wps/wcm/connect/bldcontentnl/belastingdienst/zakelijk/gegevensportalen/kinderopvanginstellingen_autoleasebedrijven_en_banken/kinderopvanginstellingen_autoleasebedrijven_en_banken2.
7 Arendsen verwijst naar De Wetenschappelijke Raad voor het Regeringsbeleid die in 2011 de term iOverheid heeft geïntroduceerd.
8 Arendsen 2016, p. 28.
9 Algemene Rekenkamer juni 2019, p. 8.
10 Algemene Rekenkamer juni 2019, p. 8.
11 Algemene Rekenkamer juni 2019, p. 9.
12 Eck, Van Hout & Weijers 10 juni 2022, p. 1607.
13 Algemene Rekenkamer januari 2021, p. 20.
14 HR 18 maart 2022, ECLI:NL:HR:2022:379, *NTFR* 2022/1207 m.nt. V.S. Huygen van Dyck-Jagersma.

3.1.1 *Triaging bij de inzet van slimme opsporingstechnieken*

De term triaging wordt veelal gebruikt in de medische wereld. Het is het proces waarbij een eerste, snelle beoordeling wordt gemaakt over de urgentie van een patiënt voor medische zorg.[15] Binnen automatische besluitvorming wordt triaging gedefinieerd als 'Determining which cases get to a human decision maker or passed to another automated process'.[16] Bij de Belastingdienst vindt dit proces getrapt plaats.[17] Zo maakte de applicatie FSV gebruik van drie stappen: 'onderzoek door middel van query's aan de poort, analyse aan de poort en een selectiemodule'.[18] In het onderzoeksrapport van PwC *Query's aan de Poort* wordt met de term query's aan de poort 'een verzameling van zoekopdrachten en selectieregels (query's) op de binnenkomende belastingaangiften bedoeld, op basis waarvan aangiften met afwijkingen ten opzichte van de norm; bijvoorbeeld hoge aftrekposten in verhouding tot het opgegeven inkomen, worden uitgeworpen en geanalyseerd door analisten aan de Poort'.[19] De term query wordt als synoniem van selectieregel gebruikt, desalniettemin bestaan query's niet slechts uit selectieregels, maar ook uit zoekopdrachten.[20]

Na deze querystap vindt een analyse, ofwel detectie, aan de poort plaats. Bij deze stap beoordelen analisten 'op basis van de uitvoer van de verschillende query's of de binnengekomen aangiften inkomstenbelasting een verhoogd risico op systeemfraude[21] bevatten, onbewuste fouten bevatten, of direct kunnen worden aangeboden aan de selectiemodule'.[22] De selectiemodule is de laatste stap van de triage en bestaat uit selectieregels opgesteld voor het specifieke aangifte jaar van de ingediende aangifte.[23] De selectieregels zijn voornamelijk vergelijkingen tussen waarden uit voorgaande aangiften of waarden uit de betreffende aangifte zoals loon-, bank-, en hypotheek- en verzekeringsgegevens. Er bestaan ook selectieregels die een bepaalde drempelwaarde vergelijken met de informatie uit de te controleren aangifte.

3.1.2 *Selectieregels en risicomodellen*

Het grootste verschil tussen de selectieregels en de risicomodellen is de basis waarop zij werken. De selectieregels zijn gebaseerd op geldende fiscale wet- en regelgeving, terwijl de risicomodellen gebaseerd zijn op inputdata, ofwel gecontroleerde

15 Cambridge Dictionary, 'Meaning of triage', raadpleegbaar via https://dictionary.cambridge.org/dictionary/english/triage
16 Binns & Veale 2021, p. 322.
17 Van Eck, Van Hout en Weijers 10 juni 2022, p. 1607.
18 Van Eck, Van Hout en Weijers 10 juni 2022, p. 1607.
19 PwC 22 maart 2022, p. 5.
20 PwC 22 maart 2022, p. 7.
21 Voetnoot uit onderzoeksverslag van PwC: 'De Belastingdienst bedoelt met systeemfraude het misbruik maken van het systeem om ten onrechte geldbedragen in de vorm van voorlopige aanslagen of definitieve aanslagen te ontvangen, door het opzettelijk opnemen van onjuiste gegevens in aangiften en verzoeken. Zie ook Feitenrelaas projectcode 1043 stand oktober 2020.'
22 PwC 22 maart 2022, p. 5.
23 PwC 22 maart 2022, p. 15.

aangiften en de resultaten daarvan.[24] Geldende fiscale wet- en regelgeving zijn vaste gegevens, zij wijzigingen slechts bij wetswijzigingen. Gecontroleerde aangiften en de resultaten daarvan, oftewel de inputdata, zijn daarentegen variabel en kunnen gemakkelijk wijzigen. Bij de selectieregels is het 'als dit, dan dat'-karakter van niet-zelflerende algoritmen te herkennen. De algoritmen in risicomodellen, die werken op basis van inputdata, zijn juist zelflerend. Zij verfijnen zichzelf. Als de inputdata verandert, dan verandert het stappenplan van het algoritme mee. Als in 2020 aangiften met name gecorrigeerd zijn op de 'posten' groene beleggingen in box 3 en rente-inkomsten als resultaat uit overige werkzaamheden, dan bevatten de data van de zelflerende algoritme voornamelijk aangiften met correcties op deze posten. Het zelflerende algoritme constateert dan dat bij belastingplichtigen met groene beleggingen en rente-inkomsten een verhoogd risico is op fouten in de aangiften, doordat het zelflerende algoritme, als gevolg van de controle, voornamelijk hier fouten heeft gezien. Als in 2021 juist met name wordt gecorrigeerd bij de post gewone beleggingen, dan past het algoritme hierop zelf zijn risicoselectie aan. Gewone beleggingen zullen door de verandering in controle vanaf dan aangemerkt worden als een risico. De zelflerende algoritmen signaleren daarom op basis van grote hoeveelheden gecontroleerde aangiften en de resultaten daarvan, waar de risico's op fouten in de aangiften liggen.[25] Na constatering van deze risico's wordt automatisch een risicomodel opgesteld dat bepaalde aangiften met een verhoogd risico op fouten of te hoge aftrekposten selecteert. Doordat steeds een nieuwe stroom aan data wordt toegevoegd en wordt geanalyseerd door het algoritme blijft het algoritme leren en zichzelf steeds weer verbeteren. Het risicomodel is zodoende dynamisch.

De selectieregels en de risicomodellen worden tegenwoordig gecombineerd tot een risicomatrix.[26] Vroeger werd uitsluitend gewerkt met de selectieregels. Bij de risicomatrix wordt gebruikgemaakt van de uitkomsten van beide technieken. De resultaten worden onderling met elkaar vergeleken in een matrix. Een hoge score betekent een hoge kans op een correctie. De score van de risicoselectie kan anders zijn dan de score van het risicomodel. Een aangifte kan op basis van de selectieregel niet uitgeworpen worden, maar op basis van het risicomodel juist wel. In de risicomatrix worden de scores met elkaar vergeleken. Op basis hiervan wordt bepaald of de aangifte al dan niet wordt uitgeworpen.

3.2 Tussenconclusie: het gebruik van slimme opsporingstechnieken

De Nederlandse Belastingdienst maakt al geruime tijd gebruik van slimme opsporingstechnieken. De Belastingdienst richt zich vooral op risicoselectie door gebruik te maken van een risicomatrix. De risicomatrix combineert de uitkomsten van selectieregels en risicomodellen. Niet-gladde gevallen worden via triaging uitgeworpen. Een uitworp is een advies voor handmatige controle door een inspecteur. Op de website van de Belastingdienst is relatief gemakkelijk informatie te vinden over de inzet van

24 Algemene Rekenkamer juni 2019, p. 9.
25 Olsthoorn 2016, p. 57-58.
26 Algemene Rekenkamer 2019, p. 9.

de slimme opsporingstechnieken. Door de opheffing over het gebruik van de FSV en de hierdoor gedane onderzoeken naar deze techniek is meer bekend geworden over de inzet van slimme opsporingstechnieken bij de Belastingdienst.

4 Het begrip transparantie

In het tweede hoofdstuk is duidelijk geworden dat slimme opsporingstechnieken niet gemakkelijk te begrijpen zijn. (Enige mate van) studie is vereist om de werking hiervan goed te doorgronden. Wanneer slimme algoritmen worden gecombineerd met Big Data-analyse wordt een en ander alsmaar complexer, en wordt het doorgronden van de werkwijze van de slimme algoritmen lastiger. In die gevallen is het zelfs voor computerexperts niet gemakkelijk om de werkwijze en de bijbehorende uitkomst van het algoritme te begrijpen.[1] Het wordt nog complexer wanneer verschillende algoritmen in verband staan met elkaar. Dit licht ik in een voorbeeld toe. Als algoritme A de onjuistheid van het urencriterium als voorwaarde voor de zelfstandigenaftrek beoordeelt en algoritme B die beoordeling, zonder deze inzichtelijk te maken, gebruikt om een risico-indicatie te geven over de vraag of de zelfstandigenaftrek al dan niet terecht is toegepast, dan is het lastig, zo niet onmogelijk, te achterhalen waarop de risico-indicatie van algoritme B gebaseerd is. Immers, – in dit voorbeeld – is de beoordeling van algoritme A niet inzichtelijk, waardoor onduidelijk, althans niet volledig duidelijk, is op basis waarvan algoritme B tot de risico-indicatie is gekomen. Als niet bekend is in hoeverre is afgeweken van het urencriterium (de uitkomst van algoritme A), is het bovendien lastiger te controleren of het risico op het al dan niet correct toepassen van de zelfstandigenaftrek terecht is gesignaleerd. Door deze onzichtbaarheid wordt het begrijpen en doorgronden van een algoritme alsmaar complexer.

(Geautomatiseerde) ketenbesluiten kennen een dergelijke complexiteit. Het besluitvormingssysteem bij (geautomatiseerde) ketenbesluiten is namelijk afhankelijk van gegevens die afkomstig zijn uit een keten. Hierbij is het genomen besluit op zijn beurt van invloed op een ander besluit van een ander bestuursorgaan uit de keten.[2] Dergelijke besluiten die invloed uitoefenen op een nieuw te nemen besluit zouden zich evenwel voor kunnen doen binnen één bestuursorgaan. Het zal dan gaan om gegevens en besluiten van de ene afdeling binnen één bestuursorgaan die invloed uitoefenen op een te nemen besluit bij een andere afdeling binnen hetzelfde bestuursorgaan. Gedacht kan worden aan een besluit over de hoogte van de verkrijgingsprijs van een aanmerkelijk belang dat van invloed is op de hoogte van de aanslag schenk- en erfbelasting.

Slimme algoritmen hebben een ondoorzichtig karakter en lijken daardoor op een *black box*. Een veel gehoorde uitspraak bij het gebruik van slimme opsporingstechnieken is daarom ‘from black box to glass box’ of ‘opening up the black box’. Wat

1 Vetzo, Gerards & Nehmelman 2018, p. 49.
2 Van Eck 2018, p. 23.

een *black box* en een *glass box* precies zijn en wat exact met deze uitspraak wordt bedoeld, zal in dit hoofdstuk duidelijk worden.

In dit hoofdstuk zal de derde deelvraag 'Welke vormen van transparantie zijn relevant bij het gebruik van algoritmen, Big Data-analyse en profiling?' beantwoord worden.

4.1 Transparantie in relatie tot het gebruik van slimme opsporingstechnieken

Transparantie is doorzichtigheid, iets kunnen inzien en doorgronden. In het geval van het gebruik van slimme opsporingstechnieken gaat het om het kunnen inzien en doorgronden van de systematiek en het proces achter de slimme opsporingstechnieken. Hierdoor is het mogelijk om afwegingen te maken om tot een gefundeerde beslissing te komen. Ook biedt transparantie van de slimme opsporingstechnieken de mogelijkheid om verantwoording te vragen en een gegeven verantwoording te beoordelen.

Eerder is aangegeven dat slimme opsporingstechnieken doorgaans (erg) complex zijn en niet gemakkelijk te doorgronden. Rouvroy omschreef dit idee van ondoorgrondbaarheid met behulp van de term *black box*: 'we know what goes in on one side and we see what comes out the other, but we do not know what goes on between the two'. Oftewel, de werkwijze van het algoritme is onduidelijk, ondoorzichtig. Het algoritme zit in een zwarte doos waar niet in gekeken kan worden. Met een voorbeeld van een simpel algoritme van een recept voor een appeltaart kan dit principe uitgelegd worden. Als de ingrediënten van een appeltaart (appels, suiker, bloem en boter) in een zwarte doos worden gestopt zonder dat zichtbaar of duidelijk is wat in die zwarte doos met de ingrediënten gebeurt en na enige tijd een appeltaart uit de doos komt, dan is het onduidelijk op welke wijze de ingrediënten tot een appeltaart zijn omgetoverd. Hetzelfde gebeurt bij slimme, complexere algoritmen. De inputdata en de outputdata zijn bekend, maar de stappen om van de inputdata tot de outputdata te komen zijn onbekend en onzichtbaar. Inhoudelijke transparantie vereist juist dat het duidelijk is op welke wijze een algoritme tot een beslissing is gekomen. Het 'stappenplan' van het algoritme – dat ten grondslag ligt aan de slimme opsporingstechniek – moet te doorgronden zijn en ook inzichtelijk en begrijpelijk. Van belang is dat niet enkel de programmeur van het algoritme de stappen kent en kan inzien, maar ook de gebruiker – in het geval van belastingheffing, de inspecteur – en diegene wiens data wordt gebruikt – in het geval van belastingheffing, de belastingplichtige. Deze inhoudelijke transparantie is ook van belang voor de controlerende functie van de wetgevende en controlerende macht binnen het systeem van checks and balances. Dit zal uitvoeriger besproken worden in par. 5.3. Daarnaast zal duidelijk worden dat deze vormen van transparantie ook van belang zijn voor de vaststelling van de oorzaak van een eventuele discriminerende werking van de slimme opsporingstechnieken, hetgeen van belang is bij het bepalen van de mate van rechtvaardiging van de discriminatie.[3] Kreten als 'from black box to glass box' of 'opening up the black

3 Hacker 2019, p. 27.

box' doelen op de verandering van een onbekend en onzichtbaar stappenplan naar een bekend en zichtbaar stappenplan. Een stappenplan dat te doorgronden is door de gemiddelde belastingplichtige die hier geringe moeite voor doet.

In de navolgende paragrafen zal duidelijk worden dat inhoudelijke transparantie niet de enige vorm is van transparantie die van belang is voor het waarborgen van een rechtsstatelijke inzet van slimme opsporingstechnieken. Transparantie van de gebruikte inputdata (inputtransparantie) is bijvoorbeeld van groot belang voor het kunnen duiden van eventueel aanwezige bias in de inputdata. Een en ander zal hierna duidelijker worden uitgelegd.

4.1.1 *Rechtspraak over transparantie in relatie tot het gebruik van slimme opsporingstechnieken*

De Raad van State heeft op 17 mei 2017 een uitspraak gedaan over transparantie in relatie tot het gebruik van slimme opsporingstechnieken.[4] In deze zaak stond de besluitvorming van vergunningverlening voor een stikstof verhogende activiteit (zoals het uitbreiden van een veehouderij) centraal. De aangevochten beschikking was gebaseerd op het gebruik van een programma dat vanuit het burgerperspectief slechts te zien was als een *black box*. De Raad oordeelde dat in zulke gevallen op de betrokken ministers en staatsecretaris de verplichting rust om 'de gemaakte keuzes en de gebruikte gegevens en aannames volledig, tijdig en uit eigen beweging openbaar te maken op een passende wijze zodat deze keuzes, gegevens en aannames voor derden toegankelijk zijn'.[5]

Het inzicht in de gemaakte keuzes en de gebruikte gegevens en aannames moet het mogelijk maken om de beslissing te (laten) beoordelen en zo nodig gemotiveerd te betwisten, ten einde effectieve rechtsbescherming tegen dergelijke besluiten te kunnen effectueren. Het toegankelijk maken van de gemaakte keuzes en de gebruikte gegevens en aannames is eveneens noodzakelijk om de rechter in staat te stellen de rechtmatigheid van de genomen beslissing te toetsen en om te voldoen aan zijn motiveringsplicht voor zijn uitspraak.

In de WOZ-zaak van augustus 2018 verwijst de Belastingkamer van de Hoge Raad naar voornoemde uitspraak van de Raad van State.[6] Belanghebbende in deze zaak had bezwaar aangetekend tegen de bij beschikking vastgestelde waarde van een onroerende zaak. Tijdens de bezwaarprocedure heeft belanghebbende verzocht tot inzage in de grondstaffels.[7] Het is een modelmatige taxatie die wordt uitgevoerd op basis van een grote database. Deze modelmatige aanpak lijkt op de risicomodellen die de Belastingdienst hanteert bij de controle van de belastingaangifte (zie par. 3.1.). Het gaat hier echter niet om de berekening van een kans, maar van een berekening

4 RvS 17 mei 2017, ECLI:NL:RVS:2017:1259.
5 RvS 17 mei 2017, ECLI:NL:RVS:2017:1259, r.o. 14.3.
6 HR 17 augustus 2018, ECLI:NL:HR:2018:1316.
7 Voor het taxeren van woninggrond wordt een kavelmodel gebruikt, dit wordt ook wel grondstaffel genoemd.

van een waarde. In dat opzicht is het geen slimme *opsporing*stechniek. Desalniettemin is het een techniek die gebruikmaakt van Big Data-analyse en waar derhalve ook gevaren van non-transparantie aan kunnen kleven, zoals ook het geval was in deze zaak. De heffingsambtenaar weigerde de inzage in de grondstaffels. Dit leverde volgens belanghebbende een schending op van het inzagerecht uit art. 7:4 lid 2 Algemene wet bestuursrecht. Het College van Burgemeester en Wethouders heeft betoogd in hoger beroep 'dat het in de bezwaarfase technisch niet mogelijk was de grondstaffels te herleiden uit het door de heffingsambtenaar gehanteerde softwareprogramma dat voorziet in een op grond van modelmatige analyses tot stand gekomen taxatiemodel'.[8] Uit dit betoog blijkt een gebrek aan inputtransparantie. De Hoge Raad heeft geoordeeld: 'Gegevens die worden opgeslagen, bewerkt, verwerkt of beheerd in systematische gegevensverzamelingen (databases) hebben in beginsel op de zaak betrekking voor zover zij van belang zijn voor, en voor het bestuursorgaan raadpleegbaar zijn met het oog op de aan de orde zijnde zaak'.[9]

Vervolgens heeft de Hoge Raad geoordeeld 'dat de in artikel 7:4, lid 2, Awb opgenomen verplichting tot het ter inzage leggen van de op de zaak betrekking hebbende stukken zich niet kan uitstrekken tot informatie die het bestuursorgaan zelf niet kan raadplegen'.[10] Echter, de Hoge Raad heeft geoordeeld dat hier een uitzondering voor geldt wanneer een 'bestuursbesluit geheel of ten dele het resultaat is van een geautomatiseerd proces'.[11] In die gevallen dienen de genomen stappen inzichtelijk en controleerbaar te worden gemaakt. Dit geldt ook voor de gebruikte inputdata. Deze inhoudelijke transparantie en inputtransparantie, dient te gelden jegens zowel de programmeur, gebruiker, diegene wiens data wordt gebruikt en jegens de wetgevende en controlerende macht. De inhoudelijke transparantie en inputtransparantie dienen te bewerkstelligen dat de processen navolgbaar zijn en gecontroleerd kunnen worden.

Ook in het socialezekerheidsrecht is geoordeeld door de Centrale Raad van Beroep dat het gebruik van risicoprofielen op transparante wijze dient plaats te vinden. Dit kwam aan de orde in een zaak waarin een door de Gemeente Eindhoven opgestelde lijst van 'verwonderadressen' ter discussie stond. De lijst stond ter discussie nadat een van de bijstandsgerechtigden een besluit aanvocht dat was genomen nadat zij op een verwonderadres een huisbezoek had gehad. De bijstandsgerechtigde uitte het vermoeden dat de lijst van verwonderadressen gebaseerd was op discriminatoire gronden. Naar aanleiding deze zaak oordeelde de Centrale Raad van Beroep over de geldigheid van de gehanteerde lijst van verwonderadressen: 'de bijstandsverlenende instantie dient bij het toepassen van risicoprofielen op transparante wijze en niet in strijd met andere beginselen, zoals het verbod van willekeur of het rechtszekerheidsbeginsel en het verbod van détournement de pouvoir, te handelen'.[12]

8 HR 17 augustus 2018, ECLI:NL:HR:2018:1316, r.o. 2.3.1.
9 HR 17 augustus 2018, ECLI:NL:HR:2018:1316, r.o. 2.3.2.
10 HR 17 augustus 2018, ECLI:NL:HR:2018:1316, r.o. 2.3.3.
11 HR 17 augustus 2018, ECLI:NL:HR:2018:1316, r.o. 2.3.3.
12 CRvB 8 december 2020, ECLI:NL:CRVB:3294, r.o. 4.4.

Van Eck, Van Hout en Weijers stellen op grond van deze uitspraak dat een zwaardere bewijslast lijkt te rusten op bestuursorganen in het socialezekerheidsrecht.[13] Uit de hiervoor genoemde uitspraak van de Belastingkamer van de Hoge Raad volgt namelijk dat (slechts) in gevallen waarin een bestuursbesluit geheel of ten dele het resultaat is van een geautomatiseerd proces de stappen inzichtelijk en controleerbaar gemaakt dienen te worden. De Centrale Raad van Beroep lijkt echter van oordeel te zijn dat deze eis van transparantie ook dient te gelden in gevallen van niet-volledig automatische besluitvorming. Zij past de eis, zo lijkt het, breder toe.

Desondanks kan op basis van bovenstaand geconcludeerd worden dat sprake dient te zijn van inhoudelijke transparantie (het kunnen doorgronden van de data*verwerking* in de black box) en inputtransparantie (het kunnen doorgronden van de data die in de black box gaat).

4.2 Transparantie in de fiscaliteit

In de vorige paragraaf is transparantie besproken in relatie tot het gebruik van slimme opsporingstechnieken. Deze bespreking is niet specifiek toegespitst op de fiscaliteit. Het principe van *opening up the black box* is toepasbaar op elk handelen waarbij gebruik wordt gemaakt van een vanuit een buitenstaander geziene black box. Om tot een meer specifieke duiding van transparantie in relatie tot het gebruik van slimme opsporingstechnieken door de Nederlandse Belastingdienst te komen, zal in deze paragraaf aandacht worden besteed aan transparantie in de fiscaliteit met een koppeling naar transparantie van (de inzet van) slimme opsporingstechnieken.

4.2.1 *Transparantie als pijler van Good Tax Governance*

Transparantie is een steeds vaker gehoorde term in de fiscaliteit als het aankomt op bestuur, ofwel *Governance* en dan met name *Good Governance*. In de fiscaliteit zijn twee hoofdvormen van *Governance* te onderscheiden: *Public Governance* en *Corporate Governance*. *Public Governance* gaat over de *Governance* van publieke organen, in het geval van *Public Tax Governance* zijn dat de belastingautoriteit en de fiscale wetgever van een land. *Corporate Governance* gaat over het bestuur van private ondernemingen. *Governance* wordt gedefinieerd als 'toezicht, sturen en beheersen gericht op efficiëntie en effectieve realisatie van beleidsdoelstellingen, en daarover verantwoording afleggen door open te communiceren naar belanghebbenden'.[14] Bij *Public Tax Governance* zijn de belanghebbenden de belastingplichtige burgers en ondernemers. Bij *Corporate Tax Governance* zijn dat (met name) de belastingautoriteit, investeerders en de consumenten. Het woord *Good* in *Good Tax Governance* geeft waarden aan de *Governance*. Een belangrijke waarde is transparantie. Door transparantie wordt relevante informatie beschikbaar gesteld aan belanghebbenden en kan de dialoog

13 Van Eck, Van Hout & Weijers 10 juni 2022, p. 1610.
14 Bossert 2002, p. 245.

worden aangegaan met hen. Zij krijgen inzicht in de fiscale keuzes van de publieke dienstverlener of de private onderneming.[15]

4.2.2 *Soorten transparantie*

Als gezegd is een tweedeling te maken binnen *Good Tax Governance*. Aan de ene kant van het spectrum spreekt men over *Public Good Tax Governance* en aan de andere kant over *Corporate Good Tax Governance*. Binnen transparantie in de fiscaliteit is dat onderscheid ook te maken. Het maken van dit onderscheid is van belang, omdat de doelen van transparantie binnen de publieke en private sector verschillen.

Gribnau onderscheidt vijf verschillende soorten transparantie: procedurele transparantie, transparantie als voorwaarde voor democratische verantwoording en transparantie van fundamentele (rechts)beginselen in de belastingwetgeving, transparantie van de uitkomst van een beslissingsproces en inhoudelijke transparantie.[16] Deze vijf vormen van transparantie zullen hier kort behandeld worden in de context van slimme opsporingstechnieken.

Van procedurele transparantie is bij slimme opsporingstechnieken sprake wanneer inzicht wordt gegeven in de afspraken die worden gemaakt over (de inzet van) slimme opsporingstechnieken.

Transparantie als voorwaarde voor democratische verantwoording houdt in dat door inzicht te geven in (de inzet van) de slimme opsporingstechniek democratische verantwoording aan de burger afgelegd kan worden. De gedachte hierachter is dat de Belastingdienst bepaalt op welke wijze geselecteerd wordt met de slimme opsporingstechniek en zo uitvoering en invulling geeft aan de fiscale wet- en regelgeving zonder dat zij democratisch is gekozen waardoor het in beginsel ontbreekt aan democratische legitimatie en verantwoording. Transparantie kan deze verantwoording mogelijk maken. Van belang is daarbij wel te waken voor een wirwar aan inhoudelijk complexe, openbaar toegankelijke documentatie waardoor de burger door de bomen het bos niet meer ziet. Naast het afleggen van verantwoording aan de burger is deze vorm van transparantie eveneens noodzakelijk voor het afleggen van verantwoording aan de wetgevende en controlerende macht. Dit zal uitvoeriger besproken worden in par. 5.3.3.

Transparantie van fundamentele (rechts)beginselen in de belastingwetgeving houdt in dat 'de belastingwetgever in zijn argumentatie fundamentele beginselen als het draagkrachtbeginsel, het gelijkheidsbeginsel en het rechtszekerheidsbeginsel niet stiefmoederlijk dient te behandelen omdat hij dan aan overtuigingskracht verliest'.[17] Deze vorm van transparantie dient, mijns inziens, niet enkel te gelden voor de belastingwetgever. Ook in andere wet- en regelgeving dient aandacht uit te gaan naar

15 Gribnau & Jallai 2017 p. 83.
16 Gribnau 2006, p. 58-60.
17 Gribnau 2006, p. 59-60

fundamentele beginselen. Gelet op de geconstateerde risico's van (de inzet van) slimme opsporingstechnieken is aandacht voor fundamentele beginselen in de wet- en regelgeving hiervoor eveneens van groot belang.

Transparantie van de uitkomst van een beslissingsproces ziet bij (de inzet van) slimme opsporingstechnieken door de Belastingdienst voornamelijk op transparantie van de beslissing tot het al dan niet uitwerpen van een aangifte. Deze vorm van transparantie ziet slechts op inzicht in de uitkomst van een beslissing en niet op inzicht in de weg daarnaartoe. Bij slimme opsporingstechnieken houdt deze vorm van transparantie echter zeer nauw verband met het stappenplan van de slimme opsporingstechniek, ofwel met inhoudelijke transparantie. Van inhoudelijke transparantie is sprake wanneer eenieder, die daarvoor geringe moeite doet, de werkwijze van de slimme opsporingstechniek kan begrijpen. Om de werkwijze van de slimme opsporingstechniek volledig te begrijpen, is eveneens transparantie van de inputdata vereist. Door het nauwe verband tussen deze drie vormen van transparantie zal ik hen vatten onder één hoofdvorm van transparantie, inhoudelijke transparantie. Deze vorm valt dan uiteen in drie subvormen van transparantie, te weten inputtransparantie, transparantie van de werkwijze van de slimme opsporingstechniek en outputtransparantie.

4.3 Tussenconclusie: het begrip transparantie

In dit hoofdstuk stond de derde deelvraag centraal: 'Welke vormen van transparantie zijn relevant bij het gebruik van algoritmen, Big Data-analyse en profiling?' In zijn algemeenheid kan gesteld worden dat transparantie bij het gebruik van deze slimme opsporingstechnieken aan te duiden is met de term glass box. Vier verschillende vormen van transparantie kunnen worden onderscheiden, deze dienen alle vier te gelden jegens de programmeur, de inspecteur, de belastingplichtige, de rechter en de wetgever. De eerste vorm is inhoudelijke transparantie. Deze vorm van transparantie valt uiteen in inputtransparantie (welke data wordt gebruikt?), outputtransparantie (wat is de uitkomst of de beslissing?) en transparantie van de stappen die doorlopen worden om tot de output te komen. De tweede vorm van transparantie is procedurele transparantie welke inzicht dient te geven in de keuzes en afspraken over (de inzet van) de slimme opsporingstechnieken. Als derde vorm kan transparantie over de wijze waarop fundamentele rechten bij de inzet van slimme opsporingstechnieken worden gewaarborgd, onderkend worden. Tot slot kan als vierde vorm transparantie als voorwaarde voor het afleggen van (democratische) verantwoording erkend worden.

In het navolgende hoofdstuk zal aandacht besteed worden aan de vraag *waarom* transparantie van (de inzet van) slimme opsporingstechnieken van belang is.

5 Het belang van transparantie

In het vorige hoofdstuk is het begrip transparantie in relatie tot het gebruik van slimme opsporingstechnieken geduid. Transparantie is een voorwaarde voor het kunnen afleggen van verantwoording. Het kunnen afleggen van verantwoording is onder meer nodig om te zorgen dat de belastingadministraties de in dit onderzoek te formuleren aanbevelingen respecteren en opvolgen. Daarnaast zal blijken dat transparantie ook van belang is voor het kunnen constateren en daarmee mitigeren van risico's die kleven aan (de inzet van) slimme opsporingstechnieken.

Zodoende zal in dit hoofdstuk ingegaan worden op die risico's. Vervolgens zal na de constatering van deze risico's de rol die transparantie kan vervullen bij het mitigeren van deze risico's aangegeven worden. De deelvraag die in dit hoofdstuk centraal staat, luidt als volgt: 'Welke risico's kleven aan (de inzet van) algoritmen, Big Data-analyse en profiling en wat is voor het mitigeren van deze risico's het belang van transparantie?'

5.1 Risico's van (de inzet van) slimme opsporingstechnieken

De inzet van slimme opsporingstechnieken komt de doelmatigheid van de belastingcontrole ten gunste. Echter, aan de inzet hiervan kleven ook risico's, zoals het verlies van rechtsbescherming, schending van het recht op non-discriminatie en het verlies van rechtszekerheid.

5.1.1 *Beperkingen en risico's van data en Big Data-analyse*

In deze paragraaf zal ingegaan worden op de beperkingen die kleven aan het gebruik van data en (de inzet van) Big Data-analyse[1]. Die beperkingen zijn *biased data*, *selffulfilling prophecy* en de vicieuze cirkel', 'het niet noodzakelijkerwijs causale verband van verbanden uit big-data-analyse' en 'het risico op valse resultaten'. Alvorens deze beperkingen nader toe te lichten, zal nadere aandacht besteed worden aan (Big) data-analyse.

Er zijn grofweg twee vormen van data-analyse te onderscheiden van elkaar: bepaalde gegevens worden met elkaar vergeleken om te verifiëren of de bekende informatie klopt of gezocht wordt naar nog onbekende verbanden of patronen. Het verifiëren van gegevensbestanden kan, zo stelt de Raad van State, objectief gebeuren

1 De hier genoemde beperkingen van Big Data-analyse zijn ook beperkingen van data-analyse.

of 'aanleiding geven voor twijfel of verdenking'.[2] Als voorbeeld van een objectieve reden voor verificatie wordt de situatie gegeven waarin 'betrokkene uit een opdracht meer verdient dan het jaarinkomen dat hij heeft opgegeven'. Bij een aanleiding voor twijfel of verdenking kan gedacht worden aan de situatie dat 'het waterverbruik op het opgegeven woonadres zo laag is dat het adres onbewoond lijkt te zijn'. Bij deze vorm van data-analyse worden kleine hoeveelheden data gebruikt en geeft de computer slechts antwoord op een specifiek door een mens gestelde vraag.[3] Een bepaalde hypothese of een bepaald gegevensbestand wordt dan geverifieerd.

Zoals eerder is gesteld, wordt Big Data-analyse in algemene zin gebruikt voor het vinden van verbanden of patronen in grote hoeveelheden data die moeilijk te analyseren zijn op basis van vooraf opgestelde hypotheses en vraagstellingen. De gevonden statistische verbanden of correlaties zijn niet altijd te verklaren of aantoonbaar causaal, wel kan doorgaans een patroon in de data gevonden worden waardoor zij een voorspellende waarde krijgen. Dit brengt enkele beperkingen met zich mee. Dat zijn *biased data*, '*selffulfilling prophecy* en de vicieuze cirkel' en 'het niet noodzakelijkerwijs causale verband van verbanden uit Big Data-analyse'. Hieronder zullen deze beperkingen achtereenvolgend behandeld worden.

5.1.2 ***Biased data***

Het biasprobleem, dat ten grondslag ligt aan *biased data*, houdt in dat alle data wordt verzameld vanuit een bepaald perspectief en daardoor een zekere mate van vooringenomenheid bevat – vandaar het Engelse woord *bias*. Doordat het hebben van vooroordelen onderdeel uitmaakt van onze socialisatie, heeft ieder mens bepaalde vooroordelen. Vooroordelen verwijzen naar interne overtuigingen, gevoelens, houdingen en veronderstellingen, afhankelijk van de groepen waartoe individuen behoren en is aangeleerd voor-oordelend gedrag over andere sociale groepen.[4] Sommige auteurs koppelen voordelen slechts aan negatieve emoties variërend van irritatie tot haat.[5] Andere auteurs onderscheiden zowel negatieve als positieve vooroordelen.[6] Hierbij wordt onderkend dat vooroordelen altijd oneerlijk zijn, omdat zij niet zijn verdiend door het individu zelf, maar door de groep waartoe de individu geacht wordt te behoren.[7]

Vooroordelen komen zowel in impliciete als in expliciete vorm voor. Impliciete vooroordelen zijn onbewust aanwezig en stemmen niet per se overeen met onze expliciete waarden en intenties.[8] Door de aanwezigheid van deze impliciete vooroordelen kunnen individuen die bewust nadenken over het eerlijk behandelen van anderen, onbewust handelen vanuit hun impliciete vooroordelen, waardoor toch een

2 Raad van State 2018, par. 3.2 '*Zelflerende systemen*'.
3 Raad van State 2018, par. 3.2 '*Zelflerende systemen*'.
4 Sensoy & DiAngelo 2017, p. 75.
5 Kinder, in: *Oxford University Press* 2013, p. 814.
6 Sensoy & DiAngelo 2017, p. 75.
7 Sensoy & DiAngelo 2017, p. 75.
8 Staats 17 juli 2020.

ongelijke behandelingen voor bepaalde groepen kan ontstaan. Doordat impliciete vooroordelen onbewust ontstaan, weet men veelal niet dat de vooroordelen bestaan. Desalniettemin heeft eenieder (impliciete) vooroordelen. Dit is inherent aan de wijze waarop het menselijk brein functioneert.[9]

Naast deze impliciete vooroordelen bestaan ook meer generieke vooroordelen die onderdeel lijken te zijn van een bepaalde cultuur op een bepaald tijdstip.[10] Dit blijkt bijvoorbeeld uit het schoonheidsideaal dat sterk is veranderd over de tijd. In de middeleeuwen werd een mollig lichaam geassocieerd met rijkdom en sensualiteit en slankheid als ziekelijk en afstotelijk.[11] Tegenwoordig is dit eerder andersom.

Deze vooroordelen die worden gevoed door cultuur en sociale standaarden, beginnen veelal als stereotypen.[12] Hoewel de termen vooroordelen en stereotypen veelal worden gebruikt als synoniemen, zijn er belangrijke nuances.

Stereotypen zijn toegeschreven eigenschappen die tot een groep zijn geworden, denk bijvoorbeeld aan het eerder gegeven voorbeeld van boeren. Wanneer waarden gekoppeld worden aan stereotypen ontstaan vooroordelen. Sensoy en DiAngelo illustreren dit aan de hand van een voorbeeld van mannelijke basisschoolleerkrachten[13]: wanneer iemand verwacht een vrouwelijke basisschool leerkracht te ontmoeten (omdat de meeste basisschoolleerkrachten vrouwelijk zijn), maar in plaats daarvan een mannelijke ontmoet, zich vervolgens afvraagt of de persoon homoseksueel is (een veel voorkomend stereotype van mannelijke basisschoolleerkrachten) en zich daarna zorgen maakt of de leerkracht wel een geschikt rolmodel is voor zijn of haar zoon (een veel voorkomend vooroordeel van homoseksuele mannen), dan is deze zorg voortgekomen uit de interactie tussen stereotypen over mannelijke basisschoolleerkrachten en de waarden geassocieerd met die stereotypen in onze cultuur. Hetgeen leidt tot een vooroordeel dat de homoseksuele leerkracht een ongeschikt rolmodel zal zijn voor de zoon.

Een groot gevaar van vooroordelen is dat zij veelal zijn genormaliseerd en worden aangenomen als waarheden. Hierdoor is het lastig om vooroordelen te erkennen en correct mee om te gaan.[14] Doordat het hebben van vooroordelen wordt veroordeeld in de maatschappij, wordt het erkennen ervan verder bemoeilijkt. Het gevaar van discriminatie ligt dan op de loer. Discriminatie treedt op wanneer gehandeld wordt vanuit vooroordelen en op basis hiervan een ongerechtvaardigd onderscheid wordt gemaakt.[15] Vooroordelen worden daarnaast gevoed doordat zij ook leven in de directe omgeving, bijvoorbeeld bij collega's, of wanneer bevestiging van de vooroordelen is gevonden in mediaberichten of een terechte controle. Het is als een vicieuze

9 Staats 17 juli 2020.
10 Sensoy & DiAngelo 2017, p. 76.
11 Luzón 27 juli 2020.
12 Sensoy & DiAngelo 2017, p. 76.
13 Sensoy & DiAngelo 2017, p. 76.
14 Sensoy & DiAngelo 2017, p. 77.
15 Sensoy & DiAngelo 2017, p. 78.

cirkel; men heeft het idee dat bijvoorbeeld mensen met een dubbele nationaliteit meer of eerder frauderen en/of crimineel zijn, daardoor wordt deze groep meer gecontroleerd, door onder meer politieambtenaren, douaneambtenaren en inspecteurs. Doordat deze groep meer gecontroleerd wordt, worden automatisch ook meer gevallen van fraude of criminaliteit aangetroffen in deze groep dan in een groep die minder vaak gecontroleerd wordt. Dit bevestigt de gedachte dat mensen met een dubbele nationaliteit meer of eerder frauderen en/of crimineel zijn. Op deze manier blijft de vicieuze cirkel, en derhalve de vooroordelen, in stand.

Om risicoprofielen meer objectief, althans meer statistisch deugdelijk, te laten zijn dan menselijke, handmatige selectie, is vereist dat zij zijn opgesteld met gebruikmaking van de juiste, schone, data. Een belangrijk vereiste daarvoor is de kwaliteit van de trainingsdata. Zoals eerder is genoemd, gebruiken slimme algoritmen de gedane observaties uit de trainingsdata om zelf slimmer te worden, ze leren van de gedane observaties, verfijnen en ontwikkeling zich verder en passen zichzelf aan. De kwaliteit van de trainingsdata hangt af van de selectie uit de gedane observaties. Als de gedane observaties zijn gevoed door vooroordelen en stereotypen, dan zijn de getrainde algoritmen dat indirect ook. Dergelijke data worden *biased* genoemd. Het maken van een goede selectie uit de gedane observaties vereist goed geschoolde data-analisten en transparantie voor belanghebbenden en externe experts in de ontwikkeling en het gebruik van algoritmen en de daarmee verband houdende trainingsdata.[16]

Na het trainen van de slimme algoritmen is het van belang om de juistheid van de algoritmen na te gaan door de getrainde algoritmen te testen en/of te valideren.[17] Het testen en valideren van algoritmen gebeurt met een andere, nieuwe set aan data met gedane observaties, welke het algoritme nog niet eerder heeft gezien. Zo kan worden gecontroleerd of het algoritme de gewenste resultaten geeft, casu quo de gewenste aangiften als risicovol selecteert.

5.1.3 *Verschillende soorten biased trainingsdata*

Vooroordelen kunnen op verschillende wijzen in de trainingsdata terechtkomen. Biased (trainings)data worden ook wel 'vervuild' genoemd.[18] Trainingsdata kunnen vanaf het begin af aan vervuild zijn of later vervuild raken. Geschikte trainingsdata kan, bewust of onbewust, biased zijn.[19] Dit kan bijvoorbeeld het geval zijn bij trainingsdata afkomstig van beveiligingscontroles waarbij met name een bepaalde groep mensen veelal gestopt wordt voor controle. Als deze dataset gebruikt wordt als trainingsdata dan zal deze (onbewust) een vertekend beeld geven van de representatie van de bevolking. Een eventuele bias kan ook aanwezig zijn doordat objectieve kenmerken sterk verbonden zijn aan discriminerende kenmerken. Calders

16 Boon 2020.
17 Council of Europe 2022, p. 9-10.
18 Richardson, Schultz & Crawford 13 februari 2019, p. 195.
19 Calders & Žliobaitė, in: *Springer* 2013, p. 5.

en Žliobaitė geven als voorbeeld een postcode die sterk verbonden kan zijn aan de etniciteit van een persoon, doordat mensen vaak kiezen om bij familieleden of mensen met dezelfde afkomst te gaan wonen.[20] Bovendien is het lastig om bij verbonden variabelen te identificeren welke variabele heeft geleid tot de uiteindelijke beslissing. Door deze correlatiebias kan verborgen informatie de data binnenkomen via andere karakteristieken (in het voorbeeld kwam de etniciteit de data in via de postcode).[21]

Trainingsdata kunnen ook vervuild zijn doordat zij incompleet zijn. Trainingsdata kan incompleet zijn doordat zij te weinig representatief is. De trainingsdata bij het eerder gebruikte voorbeeld voor het herkennen van pennen zijn bijvoorbeeld onvoldoende representatief, en dus incompleet, wanneer enkel foto's van balpennen aan het algoritme worden getoond. Het algoritme zal dan niet in staat om bijvoorbeeld vulpennen te herkennen. De incompleetheid kan zich echter ook voordoen in het laten zien van te weinig karakteristieken.[22] Bij de pennen zou dat bijvoorbeeld het geval zijn als op de foto's uit de trainingsdata slechts de punten van de pennen zichtbaar zijn. Als het algoritme dan de achterkant van de pen te zien krijgt op een nieuwe foto bestaat een reële kans dat het dit object niet zal herkennen als pen, terwijl het onderschrift van de foto wel correct was en de database zelfs representatief kan zijn geweest. In het belastingrecht is het ook denkbaar dat bepaalde karakteristieken niet terugkomen in de trainingsdata, bijvoorbeeld door privacy redenen.

Naast een het hebben van vervuilde oorsprong, kunnen trainingsdata vervuild raken. Dat kan allereest door een verkeerd gebruik van de trainingsdata.[23] Eerder is uitgelegd dat algoritmen worden getraind met trainingsdata; een algoritme dat pennen dient te herkennen krijgt verschillende foto's van pennen en potloden te zien met onderschriften als 'pen' of 'geen pen'. Het algoritme leert hiervan. Als deze onderschriften echter fout zijn, dus als een foto van een potlood het onderschrift 'pen' heeft, dan leert het algoritme het verkeerde aan. Bij het onderscheiden van pennen en potloden zal dat waarschijnlijk geen problemen opleveren. Wanneer het echter gaat over meer serieuzere zaken zoals het herkennen van een groter risico op fouten in de aangiften, dan kan dit vergaande (discriminerende) gevolgen hebben.

Uit het voorbeeld van Engelsman over het veranderende spoorwegennetwerk blijkt verder dat labels op data na verloop van tijd wijzigen. Waar een bepaald stuk spoor eerst naar links afsloeg, kan het na een wijziging naar rechts afslaan, waardoor het label is veranderd. De data dienen hierop aangepast te worden. Gebeurt dat niet, dan worden de data verkeerd gebruikt

Een andere vorm van verkeerd gebruik van trainingsdata is *sample bias* of steekproefbias.[24] Steekproefbias ontstaat wanneer data van een menselijke steekproefcontrole wordt gebruikt als trainingsdata voor een algoritme. Calders en Žliobaitė geven als

20 Calders & Žliobaitė, in: *Springer* 2013, p. 5.
21 Calders & Žliobaitė, in: *Springer* 2013, p. 6.
22 Calders & Žliobaitė, in: *Springer* 2013, p. 10.
23 Hacker 2019, p. 5.
24 Calders & Žliobaitė, in: *Springer* 2013, p. 9.

voorbeeld trainingsdata afkomstig van een fuik. Zij stellen dat wanneer politieagenten zijn geïnstrueerd om alle jonge bestuurders onder de veertig jaar aan te houden ter controle, omdat uit onderzoek is gebleken dat met name jonge bestuurders autoongelukken veroorzaken, en bestuurders boven de veertig jaar slechts aan te houden wanneer een groot vermoeden bestaat op alcoholgebruik, bijvoorbeeld door het hebben van rode ogen, dan zal uit de steekproefdata kunnen blijken dat misbruik van alcohol onder bestuurders boven de veertig jaar procentueel vaker voorkomt.[25] Bij het trekken van dit verband wordt genegeerd dat een klein absoluut aantal bestuurders boven de veertig jaar is gecontroleerd en dat slechts die bestuurders waarvan een groot vermoeden op alcoholmisbruik bestond, zijn gecontroleerd. Hierdoor zijn de data biased.

5.1.4 *De discriminerende gevolgen van biased data*

De vooroordelen die zijn verankerd in de samenleving zijn terug te vinden in de data. De oorzaak van de discriminerende werking van slimme opsporingstechnieken is hierdoor, zoals hiervoor is omschreven, veelal gelegen in de gebruikte trainingsdata. Als deze vervuilde data vervolgens worden gebruikt om risicoprofielen op te stellen, dan kunnen de eenzijdigheid en/of de vooroordelen van de trainingsdata doorwerken in de opgestelde risicoprofielen. Dit kan leiden tot onjuiste of anderszins problematische uitkomsten van de slimme opsporingstechnieken. Door de bias kan een specifieke doelgroep namelijk, onterecht, extra gecontroleerd worden. Dit heeft een versterkend effect en werkt, zoals hiervoor is genoemd, als een vicieuze cirkel. Zo wordt de discriminerende werking voortdurend versterkt (zie par. 5.1.).

Dit versterkende effect wordt ook wel aangeduid met de term *feedback loop*. Een feedback loop ontstaat wanneer beslissingen die zijn gebaseerd op voorspellingen van algoritmen worden gebruikt als data om de slimme opsporingstechniek te updaten.[26] Met andere woorden: voorspellingen die zijn gemaakt door het algoritme worden via de data, gebaseerd op die voorspellingen, weer gebruikt voor het trainen van het algoritme. Door deze feedback loops blijft de bias van het algoritme in stand en kan de bias zelfs verergeren over tijd.[27]

Custers en Zwenne, Steenbruggen en Reker spreken over het principe van *selffulfilling prophecy*.[28] Custers stelt in zijn voorbeeld van *selffulfilling prophecy* dat uit een willekeurige analyse van politiegegevens blijkt dat brildragers vaker misdrijven plegen dan niet-brildragers. De politie begint dan brildragers in de gaten te houden; als gevolg daarvan worden brildragers vaker gearresteerd op de plaatsen waar toezicht wordt gehouden. Hierdoor komen meer gevallen van arrestaties van brildragers in de data terecht, waardoor zij alleen maar vaker gecontroleerd zullen worden.[29] Doordat meer gecontroleerd wordt op het geselecteerde risico, wordt dat risico dus

25 Calders & Žliobaitė, in: *Springer* 2013, p. 10.
26 Council of Europe 2022, p. 29-30.
27 Council of Europe 2022, p. 29-30.
28 Custers 2016 en Zwenne, Steenbruggen & Reker 2016, p. 37.
29 Custers 2016, p. 17.

voortdurend versterkt, daardoor wordt (in het geval van een politiecontrole) criminaliteit bij die specifiek, vaker gecontroleerde risicogroep meer geconstateerd. Het voorbeeld laat zien dat de kwaliteit van de data van invloed is op de werkwijze bij risicoselectie en dat eenzijdige data negatieve gevolgen kunnen hebben, zoals discriminatie.

Voorbeelden waarbij algoritmen een discriminerende werking hebben, zijn vertaalfuncties, offensieve spraakdetectie[30] en gezichtsherkenningstools. De discriminerende werking van deze algoritmen ontstaat veelal doordat de gebruikte data vooroordelen bevatten of te weinig gevarieerd zijn en daardoor niet representatief zijn.

Om deze discriminerende werking te kunnen voorkomen, dient allereerst achterhaald te kunnen worden of sprake is van bevooroordeelde en/of te eenzijdige data. Om dit te kunnen bewerkstelligen is transparantie van de gebruikte data vereist, ofwel inputtransparantie. Inzicht in de gebruikte data geeft een helderder beeld van het probleem, hierdoor kan gerichter gezocht worden naar een geschikte oplossing voor het elimineren van vervuilde data. Hiervoor dienen de eventueel achterhaalde vooroordelen en/of eenzijdigheid uit de data gefilterd te worden. Dat is helaas niet gemakkelijk, met name niet wanneer gebruik is gemaakt van Big Data waarbij vaak allerlei verschillende soorten data en databronnen door elkaar heen zijn gebruikt.

5.1.5 *De gevolgen van discriminerende proxies*

Van proxy discriminatie is sprake wanneer een besluitvormer de gewenste parameter vervangt door een gemakkelijk waarneembare parameter, zoals (de gemiddelde prestatie van een bepaald) ras, geslacht, enzovoort, omdat er onvoldoende precieze informatie is over de gewenste parameter (bijvoorbeeld arbeidsprestatie).[31] Een proxy kan gezien worden als een gegeneraliseerde en gesimplificeerde assumptie van een bepaalde sociale groep. Zo kan een proxy zijn dat mannelijke bestuurders, over het algemeen, agressiever rijden dan vrouwelijke bestuurders.[32] Als een verzekeringsmaatschappij deze proxy hanteert in zijn berekening voor verzekeringspremie, dan kan dit ertoe leiden dat een rustige, mannelijke bestuurder een hogere premie betaalt dan een agressieve vrouwelijke bestuurder van dezelfde leeftijd, dezelfde auto en even lang in het bezit is van een rijbewijs. De mannelijke bestuurder wordt nu gediscrimineerd, omdat hij op basis van het stereotype 'mannelijke bestuurders zijn agressiever' anders wordt behandeld en niet op basis van hoe hij als individu is.

Tegenwoordig beschikt de besluitvormer veelal over zeer gedetailleerde informatie waaruit een doelvariabele wordt geconstrueerd. Deze doelvariabele kan in verband staan met lidmaatschap van een beschermde groep.[33] Hacker geeft een voorbeeld van een algoritme voor verzekeringsprijzen: 'Als een algoritme voor verzekerings-

30 Het rapport van de Raad van Europa gaat uitgebreid in op het voorbeeld van 'ethnic and gender bias in offensive speech detection', p. 29-48.
31 Hacker 2019, p. 6-7.
32 Calders & Žliobaitė, in: *Springer* 2013, p. 11.
33 Hacker 2019, p. 7.

prijzen vaststelt dat mensen in rode sportwagens meer risico lopen om betrokken te raken bij ongevallen en daarom een hogere premie suggereren, maar rode sportwagens ook voornamelijk eigendom zijn van mannelijke bestuurders, betalen mannen uiteindelijk gemiddeld hogere premies dan vergelijkbare vrouwelijke bestuurders.'[34] De discriminatie was echter niet gericht op geslacht, maar doordat met name mannen lid zijn van de groep waarop werd geselecteerd (het hebben van een rode sportwagen) werd er, onbewust, ook gediscrimineerd op geslacht. Hieruit blijkt dat het weghalen van een gevoelige risicoselectie geen garantie geeft voor non-discriminatie.

Voorspellende risicofactoren, die leiden tot indirecte proxy discriminatie, zijn waardevol voor de besluitvormer, omdat zij vaak accuraat zijn. In deze gevallen staan de belangen van de besluitvormer en de mensen van de beschermde groep veelal lijnrecht tegenover elkaar.[35] Vaak wordt indirecte proxy discriminatie gerechtvaardigd doordat een reële noodzaak voor het gebruik van de proxy bestaat.[36] De keuze van de besluitvormer is relevant voor de (mate van) rechtvaardiging. Dit onderscheid in rechtvaardiging van de verschillende soorten discriminatie geeft het belang aan van het kunnen vaststellen van de wijze waarop de discriminatie is ontstaan. Om dit vast te kunnen stellen, zijn met name inhoudelijke, input- en outputtransparantie vereist.

5.1.6 *Het niet noodzakelijkerwijs causale verband*

De derde beperking van Big Data-analyse is dat verbanden die volgen uit Big Data-analyse niet causaal van aard zijn, maar statistische correlaties.[37] Een illustratief voorbeeld dat het onderscheid tussen een causaal verband en een correlatie duidelijk maakt, is dat van de aanwezigheid van studieboeken bij studenten thuis en de behaalde examenresultaten. Het feit dat studenten studieboeken in huis hebben kan gecorreleerd zijn aan het behalen van goede examenresultaten. Echter, het leidt niet per definitie tot het behalen van goede examenresultaten. Hiervoor is meer vereist dan slechts het in bezit hebben van de studieboeken.

Bovendien is bij het analyseren van Big Data altijd wel een correlatie te vinden. Dit verschijnsel wordt *data dredging* of *fishing expedition* genoemd. Wanneer men een bepaald verband ontdekt in een grote hoeveelheid data, wordt nagegaan of dit verband bij toeval is ontstaan. In het geval van data dredging of fishing expeditions wordt doorgaans geen gebruikgemaakt van een theoretische basis. Data worden geanalyseerd zonder dat de onderzoeker zich heeft ingelezen of vooraf een model of hypothese heeft opgesteld. Op deze wijze worden nieuwe verbanden ontdekt. Deze methode van onderzoek maakt traditionele wetenschappelijke onderzoekers nerveus, omdat een wetenschappelijke, theoretische onderbouwing ontbreekt.

34 Hacker 2019, p. 7.

35 Hacker 2019, p. 20.

36 Hacker haalt op p. 20 de volgende zaken aan: CJEU, Case 96/80, *Jenkins*, EU:C:1981:80, par. 12. en CJEU, Case 170/84, *Bilka-Kaufhaus*, EU:C:1986:204, par. 36; see also Tobler, op. cit. supra note 94, pp. 248 et seq.

37 Zwenne, Steenbruggen & Reker 2016, p. 36.

Traditioneel dient een hypothese of model geverifieerd te worden. Zo is een theoretische grondslag gewaarborgd.

Als binnen een grote hoeveelheid data meerdere verbanden zijn ontdekt, dan kan het zogenoemde *multiple-comparisons problem* zich voordoen. Bepaalde correlaties kunnen optreden, zonder dat een causaal verband bestaat tussen de twee gegevens. Het kan toeval zijn of indirect verband houden. Het feit dat iemand binnen een risicoprofiel past, wil derhalve niet zeggen dat diegene ook het gedrag dat past bij het risicoprofiel vertoont. Om deze reden dienen data dredging of fishing expeditions bij het opstellen van risicoprofielen vermeden te worden. Gezocht dient te worden naar verbanden gebaseerd op een gedegen theoretische grondslag en niet naar louter statische verbanden. Daarbij moet ook het causale verband goed onderbouwd worden.

5.1.7 *Valse resultaten*

Bij Big Data-analyse, waar wordt gezocht naar verbanden en patronen, zullen áltijd verbanden en patronen gevonden worden. Die verbanden en patronen zijn statistisch vastgesteld. Hierdoor bestaat een verhoogde kans dat het verband of patroon ook feitelijk bestaat, dát hoeft – zoals blijkt uit het hiervoor behandelde voorbeeld over de aanwezigheid van studieboeken bij studenten – echter niet zo te zijn. Zoals al is vastgesteld in par. 5.1, is derhalve niet noodzakelijkerwijs sprake van een causaal verband. Daarnaast weerspiegelen de opgestelde profielen nooit de volledig correcte werkelijkheid. Dit komt doordat risicoprofielen foutmarges bevatten en daarnaast verouderen doordat zij in enige mate statisch zijn. Hierdoor kunnen bepaalde personen onder een risicoprofiel vallen, terwijl het risico bij hen niet intreedt.

Dit fenomeen, waardoor een bepaalde conclusie onterecht wel of onterecht niet wordt getrokken, wordt respectievelijk vals positief en vals negatief genoemd. Ik zal dit met een voorbeeld nader toelichten.

Als uit Big Data-analyse blijkt dat een verhoogd risico op fraude in de eigenwoningrenteaftrekregeling bestaat bij belastingplichtigen met een rode auto, een Nederlands paspoort en een eengezinswoning, dan zal, belastingplichtige A die voldoet aan dit profiel, gecontroleerd worden. Uit die controle blijkt vervolgens dat belastingplichtige A de eigenwoningrenteaftrekregeling correct heeft toegepast. Belastingplichtige B daarentegen, die niet voldoet aan het profiel en hierdoor niet is gecontroleerd, heeft de eigenwoningrenteaftrekregeling niet correct toegepast. Hierdoor is belastingplichtige A in overvloede gecontroleerd en is belastingplichtige B, terwijl een controle hier wel tot een correctie zou hebben geleid, niet gecontroleerd.

Bijgevolg kan iemand die voldoet aan het opgestelde risicoprofiel de eigenwoningrenteaftrekregeling correct toepassen, terwijl iemand die niet voldoet aan het opgestelde risicoprofiel, de eigenwoningrenteaftrekregeling incorrect toepast.

Dit risico op valse resultaten zorgt voor een ongelijke behandeling. Doordat belastingplichtige A, onder meer, een rode auto heeft, wordt hij eerder gecontroleerd dan

zijn buurman die een grijze auto heeft. Zelfs al blijkt uit de Big Data-analyse dat een verband bestaat, het lijkt uiterst onlogisch dat het hebben van een rode auto een causaal verband houdt met de eigenwoningrenteaftrekregeling.

Bij Big Data-analyse wordt alleen de relatie tussen, in dit geval, getallen bepaald, zonder de inhoud van de verschillende componenten te beoordelen. Als de risicofactor nauw verband houdt met de te controleren bepaling, dan is de kans groter dat het vastgestelde verband aannemelijk is. Zoals bijvoorbeeld de hoogte van de hypotheekrente in de eigenwoningrenteaftrekregeling. Deze twee factoren zijn verbonden met elkaar; de hypotheekrente bepaalt de hoogte van de eigenwoningrenteaftrek. Door deze verbondenheid is het aannemelijker dat een geconstateerd verband hiertussen causaal is. Bovendien, zou fraude in de hypotheekrente een financieel voordeel op kunnen leveren, waardoor de aannemelijkheid van de aanwezigheid van een causaal verband verder wordt versterkt. Een financieel voordeel ontstaat door fraude wanneer een belastingplichtige een hogere hypotheekrente invult, dan de werkelijke hypotheekrente. De valse hogere hypotheekrente leidt tot een hogere eigenwoningrenteaftrek.

Zoiets doet zich niet voor bij de kleur van een auto. De eigenwoningrenteaftrekregeling wordt niet beïnvloed door de kleur van de auto. Zodoende zou gesteld kunnen worden dat de voorkeur uit dient te gaan naar selectiecriteria die (nauw) verband houden met, ofwel onderdeel uitmaken van, de te controleren bepaling.

Verbanden die ontdekt worden door Big Data-analyse kunnen daarnaast subjectief of zelfs discriminerend van aard zijn. In het voorbeeld hierboven ging het om een relatief onschuldige factor als de kleur van een auto. Het kan echter ook gaan om factoren als nationaliteit en afkomst of handicap en opleidingsniveau. Het gebied van discriminatie is dan al snel betreden. Als door Big Data-analyse een verband geconstateerd wordt tussen het hebben van een handicap en fraude in de zorgkostenaftrek, kan dat tot situaties van discriminatie leiden. Als belastingplichtige A met handicap en zorgkostenaftrek van 500 euro, wel wordt gecontroleerd op fraude in zijn zorgkostenaftrek en belastingplichtige B zonder handicap met eenzelfde zorgkostenaftrek van 500 euro en overige, gelijke omstandigheden, niet wordt gecontroleerd op fraude in zijn zorgkostenaftrek, dan is sprake van discriminatie. Als een meer objectieve risicofactor zoals de hoogte van de zorgkostenaftrek, gehanteerd zou zijn, dan zou de discriminatie zich in dit geval niet hebben voorgedaan. Beide belastingplichtigen zouden dan namelijk gecontroleerd zijn.

Risicoprofielen kunnen nooit volledig accuraat zijn. Met andere woorden, wanneer gebruik wordt gemaakt van slimme opsporingstechnieken zal altijd een kans zijn op vals positieven en vals negatieven. Daarom dient beslist te worden waar de meeste waarde aan gehecht wordt. Is dit bijvoorbeeld het onterecht aanmerken van een aangifte als risicovol of is dit het onterecht *niet* aanmerken van een aangifte als risicovol? Dit is een keuze die gemaakt dient te worden alvorens de slimme opsporingstechnieken ingezet kunnen worden. Door het testen van de slimme opsporingstechnieken

met trainingsdata kan bijvoorbeeld achterhaald worden wanneer de kans op vals positieven en negatieven het kleinst is.

5.2 Beperkingen en risico's van risicoprofielen

In de vorige paragraaf zijn met name risico's van data en Big Data-analyse behandeld. In de laatste subparagraaf is al een risico van risicoprofielen genoemd. In deze paragraaf zullen andere risico's van, met name, (de inzet van) risicoprofielen behandeld worden.

5.2.1 *Social sorting*

Social sorting is het fenomeen dat toezicht is gericht op sociale, economische categorieën die worden opgesteld door de computer op basis van persoonlijke data met als doel het beïnvloeden en beheren van individuen en bevolkingsgroepen.[38] Lyon geeft hierbij het volgende voorbeeld: 'after the "terrorist" attacks of 11 September 2001, many feared that persons with "Arab" or "Muslim" backgrounds would be profiled at airport or border checkpoints. Such categories would carry consequences'.[39]

Door social sorting kunnen bijvoorbeeld bepaalde negatieve stereotypen ontstaan, wat discriminatie in de hand kan werken. Dit fenomeen hangt nauw samen met het eerder in par. 5.1 genoemde biasprobleem. Das en Schuilenburg geven aan dat 'het creëren van transparantie en inzichtelijkheid in de voorspellingen'[40] bij kan dragen aan het voorkomen van het ontstaan van stereotypen en daarmee aan het vermijden van het risico op *social sorting*.

5.2.2 *Het benaderen van de werkelijkheid en de onjuistheid of onvolledigheid van risicoprofielen*

Risicoprofielen weerspiegelen altijd een benadering van de werkelijkheid, hierdoor bevatten zij per definitie foutmarges. Door de aanwezigheid van de foutmarges kunnen personen onterecht niet of juist wel onder een bepaald profiel vallen. Dat kan nadelige gevolgen hebben. Bovendien, kunnen risicoprofielen uitgewerkt raken, omdat zij door de tijd achterhaald zijn.[41] Na verloop van tijd zijn de opgestelde risicoprofielen niet langer actueel en accuraat, zoals ook bleek uit het in par. 2.2.1 aangehaalde

38 Lyon omschreef dit fenomeen voor het eerst in 2003 in *Surveillance as Social Sorting. Privacy, Risk and Digital Discrimination*, New York: Routledge. Later is hier door verscheidene auteurs aandacht aan besteed, zie onder meer Van der Hof & Leenes, 'Gedeelde en samengestelde identiteiten in de publieke dienstverlening', 2010, p. 33; Das & Schuilenburg, 'Predictive policing: waarom bestrijding van criminaliteit op basis van algoritmen vraagt om aanpassing van het strafprocesrecht', *Strafblad: het nieuwe tijdschrift voor strafrecht*, vol. 2018, no. 4, 33, p. 19-26; en Wetenschappelijke Raad voor het Regeringsbeleid, *Big Data in een vrije en veilige samenleving*, Den Haag: Amsterdam University Press 2016, p. 89-90.

39 Lyon 2003, p. 2.

40 Das & Schuilenburg 2018, p. 24.

41 Zwenne, Steenbruggen & Reker 2016, p. 37.

voorbeeld van Engelsman over het achterhaald worden van zelflerende algoritmen bij de treindienstregeling. Het is daarom noodzakelijk de gebruikte profielen met regelmaat te actualiseren. Ook de Algemene Rekenkamer erkent dit risico op het gebruik van verouderde data.[42]

Zwenne, Steenbruggen en Reker merken daarnaast op dat de computer geen 'morele afweging' maakt bij het opstellen van risicoprofielen, waardoor, ongewenst, geselecteerd kan worden op gronden die op gespannen voet staan met het discriminatieverbod.[43] Zij betogen dat toezichthouders zich bewust dienen te zijn van dit gevaar en ervoor moeten waken dat discriminatie optreedt. Het bewust zijn van en het erkennen van risico's is derhalve van belang voor de rechtsstatelijke inzet van slimme opsporingstechnieken.

5.3 Rechtsstatelijke beginselen en (de inzet van) slimme opsporingstechnieken

In de vorige twee paragrafen zijn risico's die kleven aan (de inzet van) slimme opsporingstechnieken inzichtelijk gemaakt. Het betreft de volgende risico's: *biased data*, *selffulfilling prophecy* en de vicieuze cirkel, het niet noodzakelijkerwijs causale verband, valse resultaten, social sorting en het benaderen van de werkelijkheid en de onjuistheid of onvolledigheid van risicoprofielen. In deze paragraaf zal aangetoond worden welke rechtsstatelijke beginselen deze risico's mogelijk kunnen schenden en hoe dit beperkt kan worden.

5.3.1 *Fiscale rechtsbescherming*

'Rechtsbescherming is het geheel van mogelijkheden in een samenleving om (achteraf) op te komen tegen besluiten en handelingen van overheidsorganen'.[44] Deze definitie van rechtsbescherming is een enge definitie. Rechtsbescherming dient immers niet enkel aan de orde te zijn bij het op komen tegen besluiten en handelingen van overheidsorganen. Rechtsbescherming dient veel meer gedragen te worden doorheen de gehele samenleving en de rechtsstaat. Hierbij hoort een principieel dienstbare houding van de wetgevende en de uitvoerende macht waarbij rechtsbescherming een ware norm is, in plaats van een abstracte term.[45] Burgers dienen het gevoel te hebben dat de overheid voor hen klaarstaat, ook wanneer een geschil zich voordoet. Wanneer de overheid dit idee van rechtsbescherming openlijk uitstraalt en omarmd, dan zal rechtsbescherming inhoud krijgen en tastbaar worden voor de gewone burger.

42 Algemene Rekenkamer januari 2021, p. 40.
43 Zwenne, Steenbruggen & Reker 2016, p. 37.
44 Raad van State 15 september 2015.
45 Heij & De Vries 6 december 2020.

5.3.2 *Fiscale rechtsbescherming en de rol van de trias politica*

Happé onderscheidt drie beginselen van fiscale rechtsbescherming: 'het legaliteitsbeginsel en de belastingheffing, het gelijkheidsbeginsel als fundament van de plichten van de fiscus en de rechtsbescherming door de belastingrechter'.[46] In deze driedeling is de trias politica – één van de benoemde kernelementen van rechtsstatelijkheid[47] – van Montesquieu te herkennen; de wetgevende macht, de uitvoerende macht en de controlerende of rechtsprekende macht. In de klassieke opvatting van de trias politica vervullen zij ieder hun eigen taak en zijn zij strikt gescheiden van elkaar. In de huidige sociale verzorgingsstaat dienen alle drie de machten bij te dragen aan (fiscale) rechtsbescherming, vervullen zij meerdere taken en bestaat een evenwicht der machten. Deze bijdragen aan (fiscale) rechtsbescherming dient zichtbaar en voelbaar te zijn doorheen de gehele samenleving. Hierdoor zal rechtsbescherming tot een tastbare norm verworden en zullen burgers daadwerkelijk een gevoel van rechtsbescherming ervaren, ook gekregen vanuit de overheid.

De uitvoerende macht heeft in de huidige sociale verzorgingsstaat een ruimere discretionaire bevoegdheid gekregen. Hierdoor zijn de uitvoerende en wetgevende macht voor een deel in één hand komen te liggen en is in bepaalde mate een disbalans in de klassieke trias waarneembaar. De bestuursorganen voeren niet langer enkel het beleid uit, maar vormen dat ook zelf. Deze ruimere discretionaire bevoegdheid heeft geresulteerd in een verandering van de rechtsbescherming zoals is neergelegd in het grondwettelijke legaliteitsbeginsel.
In de woorden van Happé voldeed deze vorm van rechtsbescherming niet meer 'in een maatschappij waarin de overheid zijn nachtwakerstatus had afgelegd'.[48], [49] Aldus Happé dient de ruimere discretionaire bevoegdheid gecompenseerd te worden door de rechter met de algemene beginselen van behoorlijk bestuur.

Door de technologische ontwikkelingen en met name de verdeling van het gebruik hiervan, komt de trias politica verder onder druk te staan. Het is met name de uitvoerende instantie die veelvuldig gebruikmaakt van de technologische ontwikkelingen.[50] De kennis van de uitvoerende macht op dit gebied is dan ook groter dan de kennis op dit gebied van de wetgevende en controlerende macht.[51] Hierdoor wordt de uitvoerende macht sterker en wordt het lastiger voor de wetgevende en controlerende macht om hun functie binnen het stelsel van checks and balances te blijven

46 Happé 1969.
47 Gribnau 1998, p. 13.
48 Happé 1996, par. 1.1.2 'De moderne opvatting: de idee van de sociale verzorgingsstaat' en par. 1.2.4 'Toezicht op het handelen van de fiscus'.
49 Ook de fiscale rechtsbescherming in de zin van het fiscale legaliteitsbeginsel is veranderd. Gribnau en Pauwels becommentariëren deze verandering. Zie hiervoor J.L.M. Gribnau & M.R.T Pauwels, 'Artikel 104 – Belastingheffing. Wetenschappelijk commentaar', raadpleegbaar via nederlandrechtsstaat.nl/grondwet/inleiding-hoofdstuk-5-wetgeving-en-bestuur/artikel-104-belastingheffing/##artikel104.
50 Zweistra & Poort juni 2022, p. 457.
51 Passchier 2020, p. 919-920.

vervullen, waardoor de balans binnen de trias (verder) verstoord raakt.[52] Een andere oorzaak voor de verstoring van de balans, en met name de effectiviteit van rechterlijke en parlementaire controle, is aldus Passchier gelegen in de ondoorzichtigheid van digitalisering. Voor de rechter is het nagenoeg onmogelijk om te beoordelen of een besluit rechtmatig is genomen indien niet navolgbaar is hoe het besluit tot stand is gekomen en voor het parlement is het doorgronden van de technische en sociale werking van de digitale technologieën lastig door een gebrek aan kennis.[53] Uit deze gevaren blijkt het belang van de verschillende vormen van transparantie, met name dat van output- of beslissingstransparantie, inhoudelijke transparantie, inputtransparantie en transparantie als voorwaarde voor (democratische) verantwoording. Zonder deze vormen van transparantie geraakt de trias politica in disbalans en mindert het mechanisme van checks and balances aan functionaliteit.

Technologie begint de overhand te nemen en wordt, in de woorden van Zweistra en Poort, een 'dominante medespeler in het netwerk van de overheid'.[54] Door de verandering die Happé waarnam, kwamen meer rechten en bevoegdheden toe aan de afzonderlijke drie machten. Het is nu de technologie aan wie die macht toekomt. Algoritmen bepalen mede de invulling en uitvoering van de uitvoerende taak, hierdoor verliest de mens aan grip en macht.[55] De zorg bestaat dat technologie een vierde macht kan worden in de trias.[56] Door de vergevorderde complexiteit van met elkaar verweven algoritmen neemt transparantie af en raakt de mens de controle kwijt. Zweistra en Poort pleiten voor een betere samenwerking tussen politiek, ethiek, recht en technologie om de machtsbalans – waarin de technologie thans het zwaarst begint te wegen – te kunnen herstellen en bewaken.

Ook hier vervult het legaliteitsbeginsel een belangrijke rol. Hoewel het legaliteitsbeginsel bepaalt dat belastingen slechts bij wet geheven mogen worden, dient de letter van de wet altijd geïnterpreteerd te worden.[57] Zodoende is een nadere normering van het legaliteitsbeginsel vereist. De veranderlijke maatschappij en de gecompliceerdheid van de fiscale wetgeving maken het lastig de fiscale wet te vervatten in algemeenheden. Primair dient de belastingadministratie haar wetsinterpretatie, en daarmee ook de wetstoepassing, op voorhand kenbaar te maken, zodat de belastingplichtige weet waar hij aan toe is. In gevallen waarin een strikte uitleg van de wettelijke bepaling geen recht doet aan doel en strekking van de wet, is het de belastingadministratie toegestaan om af te wijken van de wet. Mits, zij daarbij het legaliteits- en gelijkheidsbeginsel in acht neemt en het meeste gewicht toekent aan het gelijkheidsbeginsel.[58] In de paragrafen 5.1.2 en 5.1.3 zal nader stilgestaan worden bij deze beginselen van gelijkheid en rechtszekerheid.

52 Passchier 2020, p. 920.
53 Passchier 2020, p. 919-920.
54 Zweistra & Poort juni 2022, p. 460.
55 Zweistra & Poort juni 2022, p. 460.
56 Zweistra & Poort juni 2022.
57 Happé 1996, par. 1.1.3.4 'Legaliteitsbeginsel en de eis van nadere normering'.
58 Happé 1996, par. 1.1 'Het legaliteitsbeginsel en de belastingheffing'.

De eis van de nadere normering van het legaliteitsbeginsel kan gekoppeld worden aan het huidige beloop van de technologie. Slimme opsporingstechnieken kunnen een onvoldoende geëvalueerde standaard zetten, een gezette norm is dan onvoldoende gereflecteerd door 'de domeinen politiek, ethiek en recht'.[59] Het gevaar hiervan is dat één staatsmacht ontstaat. Het mechanisme van checks and balances verzwakt, waardoor de macht van de uitvoerende macht alsmaar toeneemt. Zo kan zij uiteindelijk verworden tot één staatsmacht. Bovendien doen dergelijke onvoldoende geëvalueerde normen afbreuk aan de rechtsbescherming die voortvloeit uit het legaliteitsbeginsel.

Aldus Zweistra en Poort is de invloed van de slimme opsporingstechnieken concreet zichtbaar in 'het aandeel van algoritmen in de toeslagenaffaire'.[60], [61] De wijze waarop de technologie werkte, bemoeilijkte het maken van individuele afwegingen. Nadat een aantal individuen opkwamen tegen de werkwijze van de technologie is hieraan een nieuwe grens gesteld. 'Die grens werd gesteld door de politieke gemeenschap en lag niet besloten in wat technologisch mogelijk was.'[62] Het voorbeeld geeft aan dat technologie onvoldoende geëvalueerd een weg kan banen in de samenleving en een steeds dominantere positie inneemt. Zweistra en Poort dragen als oplossing van deze dominantere rol van technologie 'een specifiek samenwerkingsverband aan tussen de domeinen politiek, ethiek en recht', met als doel 'technologische ontwikkelingen in de greep te krijgen en te houden van de trias'.[63] In het samenwerkingsverband dient ook ruimte te zijn voor het domein van de technologie. Dit wordt ook erkend door Zweistra en Poort. Zij stellen echter niet specifiek dat kennis van experts uit de techniekhoek een belangrijke meerwaarde zal geven aan het na te streven samenwerkingsverband. Met kennis van programmeurs en data-analisten zal de werkwijze van de slimme opsporingstechnieken beter begrepen kunnen worden. Inhoudelijke, input- en outputtransparantie en transparantie als voorwaarde voor het afleggen van democratische verantwoording dragen hier ook aan bij en zijn bovendien noodzakelijk voor het daadwerkelijk intomen van de technologie.

Deze vormen van transparantie maken het mechanisme van checks and balances weer mogelijk en dragen tevens bij aan een begrijpelijke inzet van de slimme opsporingstechnieken wat evaluatie mogelijk maak. Door transparantie in de technieken en kennis uit de vier domeinen kan de 'dominante rol' van de slimme opsporingstechnieken gefundeerd op de juiste kennis door de gehele samenleving doorgrond worden. Het kunnen doorgronden door de gehele samenleving vergt naast transparantie ook een zekere mate van voorlichting aan de samenleving. Zonder deze voorlichting of wijze van informatieverschaffing zal het voor de gemiddelde burger nog

59 Zweistra & Poort juni 2022, p. 458.
60 Zweistra & Poort juni 2022, p.458.
61 Hoewel de toeslagenaffaire zich niet af heeft gespeeld binnen de Belastingdienst zoals in dit onderzoek bedoeld, toont het wel de kracht en gevaren van de inzet van slimme opsporingstechnieken. Zodoende is ervoor gekozen om dit voorbeeld van Zweistra en Poort hier te noemen.
62 Zweistra & Poort juni 2022, p. 461.
63 Zweistra & Poort juni 2022, p. 458.

steeds onmogelijk zijn om de slimme opsporingstechnieken te kunnen begrijpen, laat staan te kunnen doorgronden.

5.3.3 *Fiscale rechtsbescherming achteraf*

Het is de taak van de rechter om, achteraf, te toetsen of de wetten en de uitvoering daarvan in zijn algemeenheid voldoende rechtsbescherming bieden en om in het individuele geval rechtsbescherming te bieden aan de individuele belastingplichtige door de verschillende belangen af te wegen. De fiscale rechter kadert het handelen van de belastingadministratie af met de algemene beginselen van behoorlijk bestuur, hiermee biedt hij rechtsbescherming.[64]

In de Nederlandse fiscaliteit kan (achteraf) opgekomen worden tegen de belastingaanslag en -verrekening en de voor bezwaar vatbare beschikking, zoals is bedoeld in art. 26 van de Algemene wet inzake rijksbelastingen. Hiertegen staat de mogelijkheid tot bezwaar en beroep open. Het bezwaar wordt behandeld door de inspecteur en het beroep door de rechter. Om een weloverwogen beslissing te kunnen nemen, dienen de inspecteur en de rechter van alle feiten en omstandigheden op de hoogte te zijn. De inspecteur en de rechter dienen inzicht te hebben in de overwegingen die ten grondslag liggen aan het genomen besluit. Bij een besluit dat is genomen met slimme opsporingstechnieken dient daarom inzicht te zijn in de werking van die slimme opsporingstechnieken. Het is zodoende van belang dat de inspecteur tijdens de bezwaarfase en de rechter tijdens de beroepsfase de selectieregels kunnen doorgronden. Daarvoor is transparantie vereist.

Ook voor de controle op de naleving van algemene beginselen van behoorlijk bestuur is inzicht in de werkwijze van de slimme opsporingstechnieken vereist. Als geen inzicht is of wordt gegeven in de gebruikte data en de wijze waarop de risicoprofielen worden opgesteld, dan kan niet gecontroleerd worden of fundamentele beginselen, zoals het gelijkheidsbeginsel, verbod op discriminatie en de algemene beginselen van behoorlijk bestuur, wel in acht zijn genomen.

In de jurisprudentie zijn weinig zaken gevonden waarin een beroep werd gedaan op schending van een Algemeen beginsel van behoorlijk bestuur. Als hierop al een beroep wordt gedaan dan is dat voornamelijk op het zorgvuldigheids- of motiveringsbeginsel. In de hoger-beroepzaak op 2 september 2021 bij de Centrale Raad van Beroep vroeg appellant zich zorgwekkend af ‘of het hoofdbesluit en het bestreden besluit uitsluitend door algoritmen tot stand zijn gekomen, zonder tussenkomst van extra personeel’.[65] Volgens appellant waren ook algoritmen gebruikt.

De Raad las deze vraag als een beroep op schending van het zorgvuldigheidsbeginsel en oordeelde dat dit beroep ongegrond was, omdat geen sprake was van een ‘open

64 Happé 1996, par. 1.1.2 ‘De moderne opvatting: de idee van de sociale verzorgingsstaat’ en par. 1.2.4 ‘Toezicht op het handelen van de fiscus’.

65 CRvB 2 september 2021, zaaknummer: 21/1171 AOW, ECLI:NL:CRVB:2021:2244, r.o. 4.5.

norm waarvan de toepassing afhankelijk is van een weging van de omstandigheden van het geval of een afweging van belangen, maar om een wettelijke leeftijdsgrens'.[66] Hieruit volgt dat een beroep op schending van het zorgvuldigheidsbeginsel niet snel gegrond wordt verklaard bij gesloten normen.

Transparantie maakt het in eerste instantie mogelijk dat belastingplichtigen een opgelegde aanslag of beschikking kunnen begrijpen en vervolgens een weloverwogen keuze maken om hiertegen in bezwaar of beroep te gaan. Zonder transparantie is sprake van een zekere mate van informatieasymmetrie tussen burger en toezichthoudend orgaan.

Die informatieasymmetrie is veelal groter in procedures waarbij slimme opsporingstechnieken, in de vorm van een black box, zijn ingezet. Belastingplichtigen hebben dan namelijk geen inzicht in de keuzes die ten grondslag liggen aan het genomen besluit. Hierdoor kunnen zij het genomen besluit minder goed begrijpen en zich hiertegen minder (gericht) verdedigen.

Gebrek aan transparantie leidt ertoe dat het beginsel van fair play in het gedrang komt. Het fair play beginsel is een algemeen beginsel van behoorlijk bestuur en in Nederland wettelijk verankerd in art. 2:4 van de Algemene wet bestuursrecht. Het fair play beginsel behelst onder meer dat partijen op een gelijkwaardige, eerlijke wijze het 'spel spelen'.[67] Hierdoor beschermt het fair play beginsel zowel de belangen van de inspecteur als die van de belastingplichtige. De inspecteur en belastingplichtige dienen beiden zicht te (kunnen) hebben op de basale overwegingen die ten grondslag liggen aan het aangevochten besluit. Hoewel het fair play beginsel vanuit die gedachte openheid bevordert, stelt het ook grenzen aan het delen van informatie. Zo is het opvragen door de inspecteur van informatie over de advisering van de fiscale positie van belastingplichtige strijdig met het fair play beginsel.[68] Andersom hoeft de Belastingdienst zijn controle- en opsporingsbeleid – en de in dat kader gebruikte algoritmen – niet volledig prijs te geven aan de belastingplichtigen, dit omdat de inspecteur dan veel van zijn argumenten zichtbaar maakt voor de wederpartij. Hier kan derhalve een spanningsveld geconstateerd worden tussen het geven en niet geven van informatie aan de wederpartij.[69] Toch, kan ook vastgesteld worden dat transparantie van de gebruikte algoritmen en data kan bijdragen aan het opheffen van de informatieasymmetrie tussen de burger en de gebruiker van de algoritmen, waardoor een level playing field wordt gestimuleerd. Dit blijkt ook uit de in par. 4.1 behandelde stikstofzaak van de Raad van State waar het fair play beginsel aan bod kwam.[70] De Raad heeft dit beginsel niet als dusdanig genoemd, maar noemt wel de elementen van het beginsel; het voorkomen van ongelijkwaardige procesposities.[71]

66 CRvB 2 september 2021, zaaknummer: 21/1171 AOW, ECLI:NL:CRVB:2021:2244, r.o. 4.5.
67 Van Eijsden 2007.
68 HR 23 september 2005, ECLI:NL:HR:2005:AU3140, *BNB* 2006/21.
69 Dit spanningsveld komt ook aan de orde in par. 5.1.4 waarin *gaming the system* centraal staat.
70 RvS 17 mei 2017, ECLI:NL:RVS:2017:1259.
71 RvS 17 mei 2017, ECLI:NL:RVS:2017:1259, r.o. 14.3 en 14.4.

5.3.4 *Rechtsgelijkheid en het recht op non-discriminatie*

Het recht op non-discriminatie is, net als het gelijkheidsbeginsel, een fundamenteel en breed erkend recht.[72], [73] Het hiermee verband houdende verbod op discriminatie geldt voor eenieder, ook voor belastingadministraties. Bij de gebruikmaking van risicoprofielen in de opsporing van belastingfraude of fouten in de aangiften, kan dit verbod overtreden worden. In deze paragraaf zal worden ingegaan op de elementen van het gelijkheidsbeginsel en het verbod op discriminatie. Ook zullen enkele concrete voorbeelden van strijdigheden worden genoemd.

Uit de politiek-filosofische beschouwing van Happé volgt dat het gelijkheidsbeginsel fundamenteel is voor de fiscale rechtsbescherming.[74] Hierdoor is de belastingadministratie – Happé spreekt over de fiscus – in bepaalde situaties verplicht om, binnen de rechtskaders, af te wijken van de wettelijke bepalingen. Doet hij dat niet, dan is de rechter verdragsrechtelijk bevoegd om de uitvoering van én de invulling van de wetten te toetsen aan het gelijkheidsbeginsel.[75] Deze plicht van de belastingadministratie en de verdragsrechtelijke bevoegdheid van de rechter volgen uit de wettelijke bepaling zoals is neergelegd in art. 26 van het Internationaal Verdrag inzake burgerrechten en politieke rechten.[76] Voor zowel de rechter als de belastingadministratie is het perspectief van het gelijkheidsbeginsel de rechtsbescherming. Voor de belastingadministratie is dat de rechtsbescherming in zijn algemeenheid, bepaald door 'de algemene norm van de wettelijke bepaling' en voor de rechter is dat de rechtsbescherming in het individuele geval.[77]

Strijdigheid met het gelijkheidsbeginsel ontstaat wanneer sprake is van ongelijke behandeling van gelijke gevallen of een te ver gaande ongelijke behandeling van ongelijke gevallen.[78] Met andere woorden, wanneer ongelijke gevallen niet slechts ongelijk worden behandeld voor zover zij ongelijk zijn. (Ten minste) twee vormen van gelijkheid kunnen onderscheiden worden: gelijkheid *in* de wet (het formele gelijkheidsbeginsel) en gelijkheid *voor* de wet (het materiële gelijkheidsbeginsel).[79] In het eerste geval gaat het om de verplichting van de wetgever om zorg te dragen dat geen onterecht onderscheid wordt gemaakt in wettelijke bepalingen. In het tweede geval gaat het om de toepassing van de wettelijke bepaling, ofwel zorgdragen voor een gelijke behandeling of gerechtvaardigde ongelijke behandeling. De eerste vorm van gelijkheid valt onder de beginselen van behoorlijke wetgeving. De tweede vorm komt tot uitdrukking als een beginsel van behoorlijk bestuur. Bij de toetsing aan het gelijkheidsbeginsel bij (de inzet van) slimme opsporingstechnieken is de tweede

72 Gerards, in: *Gelijkheid en (andere) Grondrechten* 2004, p. 45.
73 Zie onder meer: art. 1 van de Nederlandse Grondwet; art. 7 van de UVRM; art. 26 van het IVBPR; art. 14 van het EVRM; art. 1 van Protocol nr. 12 bij het EVRM; en art. 21 van het HGEU.
74 Happé 1996, par. 1.2.
75 Happé 1996, par. 1.2.2. 'Juridische fundering van de plicht tot standpuntbepalingen'.
76 Nederland is partij bij dit Verdrag.
77 Happé 1996, par. 1.2.4 'Toezicht op het handelen van de fiscus'.
78 Zie bijvoorbeeld HR 4 oktober 2002, nr. 37 439, *BNB* 2002/406, r.o. 3.5.
79 Gerards, in: *Gelijkheid en (andere) Grondrechten* 2004, p. 49.

vorm van gelijkheid van belang. Strijdigheid kan ontstaan door een ongerechtvaardigde, ongelijke behandeling in de uitvoering van de wet. Deze ongerechtvaardigde, ongelijke behandeling kan het gevolg zijn van *biased data* of proxy discriminatie zoals zichtbaar is geworden in par. 5.1.

Daarnaast is zichtbaar geworden dat de wijzigingen in de uitvoering van de wet door de inzet van slimme opsporingstechnieken zorgen voor een verandering in het mechanisme van checks and balances en zorgt voor een disbalans tussen de drie machten van de trias. Onvoldoende geëvalueerde normen gezet door slimme opsporingstechnieken kunnen leiden tot een schending van het gelijkheidsbeginsel. Zoals al is genoemd, kan een specifiek samenwerkingsverband tussen de domeinen politiek, ethiek en recht bijdragen aan het minimaliseren van de macht van slimme opsporingstechnieken.

Zoals al geconstateerd is, wordt bij profiling geselecteerd op basis van bepaalde (persoons)kenmerken. Wanneer deze kenmerken een discriminerend karakter hebben, ontstaat strijdigheid met het verbod op discriminatie. Van een discriminerend karakter is sprake wanneer mensen of groepen mensen ongelijk worden behandeld op basis van (persoons)kenmerken, zonder dat hier een (objectieve) rechtvaardigingsgrond voor bestaat.

Concreet is een ongelijke behandeling op basis van godsdienst, levensovertuiging, ras, geslacht/sekse, nationaliteit, seksuele gerichtheid, handicap of chronische ziekte, leeftijd, politieke gezindheid, nationaliteit of burgerlijke staat niet toegestaan. Discriminatie kent verschillende vormen. Een bekende vorm is racisme. Bij deze vorm van discriminatie worden (groepen) mensen uitgesloten of anders behandeld op basis van hun ras. Ras wordt hier gekenmerkt door huidskleur, nationaliteit en/of etniciteit. Die andere behandeling en uitsluiting vindt zijn grondslag in de gedachte dat een biologisch onderscheid bestaat tussen rassen en dat hierdoor het ene ras superieur is aan het andere ras. Tegenwoordig is racisme meer geënt op een cultureel onderscheid, dan op een biologisch onderscheid.[80] Ook overheden kunnen, onbewust, racistisch optreden. Deze structurele vorm van racisme wordt institutioneel racisme genoemd.

Er kan ook sprake zijn van een onrechtvaardige, ongelijke behandeling waarbij onduidelijk is of een of meerdere discriminatiegronden worden geschonden, omdat zij zich gelijktijdig en onafscheidelijk van elkaar voordoen. Dit wordt intersectionele discriminatie genoemd. Intersectionele discriminatie doet zich bijvoorbeeld voor wanneer een vrouw van kleur gediscrimineerd wordt. Deze discriminatie kan of het gevolg zijn van rassendiscriminatie of van genderdiscriminatie, of van allebei.[81] Het is niet mogelijk om vast te stellen op welke grond precies gediscrimineerd is, omdat de twee kenmerken die deel uitmaken van haar identiteit of die door anderen aan

80 Blokland & Hondius 2003, p. 77-78.
81 Xythali 2018, p. 12.

haar worden toegewezen (het vrouw zijn en een kleur hebben) niet van elkaar gescheiden kunnen worden.

Ook het optreden van de Belastingdienst kan discriminerend zijn. Bijvoorbeeld wanneer voor de controle op een aangifte is geselecteerd op een discriminatiegrond en dit heeft geleid tot een uitworp. Volgens de Hoge Raad kan aan een dergelijke controle de conclusie worden verbonden dat 'de controle van de aangifte van de belastingplichtige heeft plaatsgevonden op een wijze die zozeer indruist tegen hetgeen van een behoorlijk handelende overheid mag worden verwacht, dat het gebruik van hetgeen bij die controle aan het licht is gekomen onder alle omstandigheden ontoelaatbaar moet worden geacht'.[82]

Selectiecriteria worden hiermee niet volledig in de ban gedaan. In een latere zaak bij het gerechtshof Den Haag voerde een belastingplichtige aan dat hij ten onterechte was aangemerkt als een fraudeur, omdat hij wegens een onderzoek naar zijn adviseur de projectcode '1043' heeft gekregen en daarom mogelijk eveneens is opgenomen in de zogenoemde FSV. Het hof oordeelde dat een dergelijke uitworp op grond van een ingesteld onderzoek naar de gemachtigde niet zozeer indruist tegen hetgeen wat van een behoorlijk handelende overheid mag worden verwacht en dat derhalve de navorderingsaanslag niet vernietigd hoefde te worden.[83]

Binnen het kader van risicoselectie dient de rechter, bij zijn beoordeling of sprake is van discriminatie op grond van het Europees Verdrag van de Rechten van de Mens (EVRM), na te gaan of de betrokkene op dezelfde wijze behandeld zou zijn geweest indien hij niet een bepaald persoonskenmerk had gehad zoals is bedoeld in art. 14 van het EVRM.[84] Indien de behandeling anders zou zijn geweest, dan is sprake van ongelijke behandeling op grond van één van de in art. 14 verboden gronden.

5.3.5 *Rechtszekerheid*

Het beginsel van rechtszekerheid houdt in dat burgers dienen te weten waar zij aan toe zijn. Enerzijds dient de geldende wet- en regelgeving, evenals de gevolgen hiervan, ondubbelzinnig, duidelijk en kenbaar te zijn (het formele rechtszekerheidsbeginsel), en anderzijds geldt voor deze geldende wet- en regelgeving het verbod van terugwerkende kracht (het materiële rechtszekerheidsbeginsel).[85] In relatie tot de toepassing van slimme opsporingstechnieken is met name het formele rechtszekerheidsbeginsel van belang. Burgers dienen niet enkel de letter van de wet te kunnen raadplegen, zij dienen evenzo te kunnen achterhalen op welke wijze zij wordt toegepast. Zoals in par. 5.1 is genoemd, wordt met de inzet van slimme opsporingstechnieken de wetstoepassing beïnvloed door, onder meer en met name, de gebruikte

82 HR 10 december 2021, nr. 20/02304, ECLI:NL:HR:2021:1748, BNB 2022/41, r.o. 5.3.
83 Gerechtshof Den Haag 1 maart 2022, 21/00378-80, ECLI:NL:GHDHA:2022:309, *NTFR* 2022/1630, r.o. 5.3.2.
84 Gerechtshof Den Haag 14 februari 2023, 200.304.295/01, ECLI:NL:GHDHA:2023:173, r.o. 8.5.
85 Nicolaï 2016.

algoritmen. Zelflerende algoritmen ontwikkelen zichzelf, hierdoor veranderen de algoritmen in de loop der tijd. De wijze van selectie evolueert hierdoor mee.

Door deze verandering kan de rechtszekerheid ten aanzien van de wetstoepassing in het gedrang komen. Doordat de wijze van selectie continue wijzigt, weet de burger niet langer goed waar hij aan toe is. Een en ander betekent niet dat de belastingadministratie haar volledige controlestrategie dient te onthullen, wel dient zij inhoudelijke transparantie te verschaffen.[86] Ingevolge art. 3:47 en 3:48 van de Algemene wet bestuursrecht is een bestuursorgaan verplicht om de belanghebbenden inzicht te verschaffen in de wijze waarop een besluit tot stand is gekomen. Hier wordt, aldus Van Hout, geen nieuwe vorm van rechtsbescherming beoogd, het gaat om een concretisering – afgestemd op (de inzet van) de slimme opsporingstechnieken – van wat de Algemene wet bestuursrecht al voorschrijft.[87]

Bij de traditionele risico- en controletechnieken weet de burger ook niet of nauwelijks de controlestrategie. Het (volledig) inzichtelijk maken van de controlestrategie is gevoelig voor *gaming the systeem*. Kwaadwillende belastingplichtigen kunnen gemakkelijk inspelen op de publiekelijk, bekende risicoselectie en zo onder de radar blijven. Transparantie is vanuit die gedachte minder wenselijk.

Daarentegen kan een trend waargenomen worden die meer uitgaat van een wederzijdse vertrouwensrelatie. Vanuit die vertrouwensrelatie ziet de belastingadministratie de burger als een welwillende belastingplichtige en de belastingplichtige andersom de belastingadministratie als welwillend bestuursorgaan. Van Hout stelt bovendien dat het inzichtelijk maken van de wijze waarop een beslissing tot stand is gekomen de voorzienbaarheid en de rechtszekerheid doen toenemen. Hierdoor zal, in de woorden van Hout: het vertrouwen in de belastingadministratie[88] stijgen; 'hoe ambivalent dat wellicht voor sommigen zal voelen'.[89] Deze afname van wantrouwen geldt echter niet per definitie voor iedere belastingplichtige. De ene belastingplichtige zal inderdaad gerustgesteld worden als hij weet wat de belastingadministratie verzamelt en wat zij daarmee doet. Echter, bij andere belastingplichtige zal het wantrouwen juist toenemen. Bijvoorbeeld omdat hij niet besefte dat de belastingadministratie zó veel gegevens van hem verzamelde.

Kortom, gezocht zal moeten worden naar een balans tussen het voorkomen van gaming the system, wan-/vertrouwen en (de mogelijkheid tot) transparantie die ten goede komt aan de rechtszekerheid. Dit is een lastige afweging die gemaakt dient te worden. Het is aanbevolen om nader te onderzoeken op welke wijze deze afweging het beste gemaakt kan worden.

86 Van Hout 29 augustus 2017, p. 1043.
87 Van Hout 29 augustus 2017, p. 1043.
88 Van Hout spreekt over de Belastingdienst, mijns inziens kan haar stellingname ook op andere belastingadministraties toegepast worden.
89 Van Hout 29 augustus 2017, p. 1043.

5.4 Tussenconclusie: het belang van transparantie

In dit hoofdstuk zijn de risico's die kleven aan het gebruik van algoritmen, Big Data-analyse en profiling onderzocht. In dat licht is ook aandacht besteed aan het belang van transparantie hiervan. Verder is het belang van rechtsbescherming voor de burger die te maken krijgt met deze slimme opsporingstechnieken inzichtelijk geworden. Om rechtsbescherming in brede zin te verzekeren dient allereerst en vooral verantwoord omgegaan te worden met de slimme opsporingstechnieken. Hiervoor zijn bewustheid van en het erkennen van de nadelen en risico's van de slimme opsporingstechnieken vereist. Voor een effectieve rechtsbescherming achteraf is tevens het opheffen, of in ieder geval het verkleinen, van de informatieasymmetrie tussen de burger en de gebruiker van de algoritmen van belang. Dit om een schending van het fair play beginsel te voorkomen. Om dit te bewerkstelligen zijn met name input-transparantie en inhoudelijke transparantie noodzakelijk. Deze vormen van transparantie zijn ook noodzakelijk voor een gemotiveerd oordeel in een bezwaar- of beroepsfase.

Ten derde is transparantie vereist om een eventuele discriminerende werking van slimme opsporingstechnieken te voorkomen. Inzicht in de trainingsdata maakt het namelijk mogelijk om eventueel aanwezige vooroordelen in en/of eenzijdigheid van de trainingsdata uit die trainingsdata te filteren.

Ten vierde kan transparantie bijdragen aan het mitigeren van de geconstateerde risico's van *biased data, selffulfilling prophecy* en de vicieuze cirkel, het niet noodzakelijkerwijs causale verband, valse resultaten, social sorting en het benaderen van de werkelijkheid en de onjuistheid of onvolledigheid van risicoprofielen. Doorslaggevend hiervoor is de rol die transparantie vervult bij het afleggen van verantwoording.

6 Bestaande richtinggevende kaders

Het gebruik van slimme opsporingstechnieken neemt alsmaar toe. Zoals is geconstateerd, kleven hieraan risico's waar rechtsbescherming voor moet gelden. Momenteel bestaat voornamelijk wet- en regelgeving op het gebied van privacybescherming.[1] Zoals al is gesteld, valt privacybescherming buiten de reikwijdte van dit onderzoek, derhalve zal daar ook hier geen aandacht aan besteed worden. In Nederland geldt momenteel – afgezien van de privacywetgeving – geen wet- of regelgeving voor het gebruik en de inzet van slimme opsporingstechnieken. Dit gebrek aan positief recht houdt uiteraard niet in dat de inzet en het gebruik van slimme opsporingstechnieken door overheidsorganen onbegrensd is. De algemene beginselen van behoorlijk bestuur en de grond- en mensenrechten, waar overheidsorganen zich aan dienen te houden, zorgen voor een begrenzing. Naast deze alom geldende rechten en beginselen, zijn ook een tal van kaders, richtlijnen en hulpmiddelen opgesteld voor de inzet van slimme opsporingstechnieken. In dit hoofdstuk zullen een aantal hiervan nader toegelicht worden.

Het Toetsingskader van de Algemene Rekenkamer, Richtlijnen voor het toepassen van algoritmen door overheden en publieksvoorlichting over data-analyses en de Toolbox Ethisch Verantwoorde Innovatie zullen behandeld worden vanwege hun algemene karakter en omdat zij ingaan op meerdere risicoaspecten. Daarnaast zal aandacht besteed worden aan de visie van de Nationale ombudsman op het gebruik van data en algoritmen door de overheid. Ook zal het Algoritme Register van de stad Amsterdam als good practice toegelicht worden.

Omwille van de beperkte omvang van dit onderzoek kunnen niet alle al bestaande richtinggevende kaders behandeld worden. Hierdoor is ervoor gekozen om de Handreiking non-discriminatie by design[2] en de Impact Assessment Mensenrechten en Algoritmes[3] niet toe te lichten. In deze twee kaders wordt namelijk enkel aandacht besteed aan het risico op schending van mensenrechten, zoals het verbod op

1 Zie onder meer de Algemene verordening gegevensbescherming (Verordening (EU) 2016/679 van het Europees Parlement en de Raad) 27 april 2016; Rijksdienst 'Model Data Protection Impact Assessment' 19 november 2021, raadpleegbaar via kcbr.nl/beleid-en-regelgeving-ontwikkelen/integraal-afwegingskader-voor-beleid-en-regelgeving/verplichte-kwaliteitseisen/data-protection-impact-assessment; Centrum Informatiebeveiliging en Privacybescherming, De Privacy Baseline 2020; Koers & de Bruijn, Handleiding Privacy by Design, 2017.

2 *De Handreiking non-discriminatie by design* juni 2021, raadpleegbaar via rijksoverheid.nl/documenten/rapporten/2021/06/10/handreiking-non-discriminatie-by-design.

3 *De Impact Assessment Mensenrechten en Algoritmes* juli 2021, raadpleegbaar via rijksoverheid.nl/documenten/rapporten/2021/02/25/impact-assessment-mensenrechten-en-algoritmes.

discriminatie en dit risico wordt al behandeld in het Toetsingskader van de Algemene Rekenkamer, Richtlijnen voor het toepassen van algoritmen door overheden en publieksvoorlichting over data-analyses en de Toolbox Ethisch Verantwoorde Innovatie.

6.1 Toetsingskader Algemene Rekenkamer

De Algemene Rekenkamer heeft, na constatering van een gebrek aan een instrument voor het toetsen en analyseren van algoritmen, in 2020 het digitale Toetsingskader 'Aandacht voor algoritmen' ontwikkeld. Het betreft een gemakkelijk te vinden en te gebruiken overzicht van risico's die zich kunnen voordoen bij de gebruikmaking van algoritmen. In deze paragraaf zal een algemene analyse van dit Toetsingskader gegeven worden. Extra aandacht zal besteed worden aan de aanwezigheid van transparantie in het Toetsingskader.

6.1.1 *Het Toetsingskader in het algemeen*

Zoals al is genoemd, geeft het Toetsingskader een overzicht van risico's die zich kunnen voordoen bij de gebruikmaking van algoritmen. Per risico zijn een onderzoeksvraag en beheersmaatregel(en) genoteerd om het risico te detecteren en te beheren. Sommige beheermaatregelen zijn eenduidig en concreet, bijvoorbeeld 'Zichtbaar gescheiden training-, test- en validatiedata', andere zijn minder concreet en minder direct toepasbaar, zoals 'Maatregelen om bias te beperken, tegen te gaan en/of te compenseren'. Hier worden geen voorbeelden gegeven van dergelijke maatregelen. Hierdoor is het Toetsingskader mijns inziens voldoende toereikend voor de signalering van eventuele gebreken en bevat het een eerste handreiking voor te nemen beheermaatregelen, maar is het – door het ontbreken van voorbeelden – onvoldoende toereikend om de geconstateerde gebreken direct met de gegeven beheermaatregelen te herstellen. Hiervoor is vereist dat het bestuursorgaan dat de gebreken wil herstellen nader onderzoek verricht. Zo is in het geval van geconstateerde bias, onderzoek nodig naar maatregelen voor het beperken, tegengaan en/of compenseren van de bias.

Met andere woorden, het Toetsingskader is mijns inziens voldoende toereikend voor het vaststellen van risico's van het gebruik van algoritmen. Echter, het schort mijns inziens aan concrete handvatten om geconstateerde risico's (op voorhand) te mitigeren. Dit heeft de Algemene Rekenkamer zelf ook aangegeven. Het opgestelde Toetsingskader is bedoeld voor controle na de ontwikkeling van de algoritmen en niet voor het inperken of zelfs mitigeren van de risico's tijdens de ontwikkeling van en tijdens de inzet van de algoritmen. Daarvoor is een 'hanteerbaar normenkader aan de voorkant' nodig of 'kwaliteitseisen voor de ontwikkeling van algoritmes'. Met 'als doel dat de bruikbaarheid van de kwaliteitseisen omhooggaat en al aan de voorkant, bij de ontwikkeling van algoritmes, kan worden toegepast.'[4]

4 Algemene Rekenkamer januari 2021, p. 41.

Het toetsen met het Toetsingskader na de ontwikkeling en tijdens het gebruik van de algoritmen is niettemin waardevol. Zo vindt ICT-expert Marc Gelissen de aanbeveling van de Algemene Rekenkamer om afspraken over de inzet van algoritmen vast te leggen en de continue monitoring goed in te richten[5] 'een goede zaak'.[6] Tijdens het gebruik van de algoritmen wordt dan namelijk voortdurend getoetst op de ethische aspecten. Volgens Gelissen is 'de belangrijkste toets een ethische: wordt er niet gediscrimineerd, en komt de 'menselijke maat' niet in de knel? Ook moet een burger de gebruikte data kunnen opvragen.' Hier besteedt het Toetsingskader ook aandacht aan.

6.1.2 *Het Toetsingskader en transparantie*

Het opvragen van de gebruikte data komt naar voren in één van de vier ethische onderwerpen die zijn verweven in het gehele Toetsingskader, te weten 'Verklaarbaarheid en transparantie'.[7] De Algemene Rekenkamer geeft hier een tweetal geboden: 'Er kan verantwoording worden afgelegd over de gevolgde procedures' en 'De werking van het algoritme is te verklaren en uit te leggen'. Het eerste gebod is onderverdeeld in acht 'subgeboden'. Het tweede gebod is onderverdeeld in zeven subgeboden. In deze (sub)geboden zijn de verschillende vormen van transparantie te herkennen. Hieronder zal genoemd worden welke vorm van transparantie (zie par. 4.2.2) deze subgeboden dienen. Eerst zullen de subgeboden van het eerste gebod besproken worden. Daarna zullen de subgeboden van het tweede gebod besproken worden.

In de eerste twee subgeboden, 'Afwegingen worden gedocumenteerd, waardoor keuzes traceerbaar zijn' en 'Ontwerp van het model is gedocumenteerd', is procedurele transparantie te herkennen. De keuzes en afspraken die ten grondslag liggen aan de inzet van de algoritmen – of breder getrokken de slimme opsporingstechnieken – dienen namelijk gedocumenteerd te worden. Dergelijke, openbaar toegankelijke, documentatie dient de procedurele transparantie. Het derde, vierde en vijfde subgebod, respectievelijk 'Er vindt documentatie plaats over het verkrijgen, selecteren en bewerken van data', 'Keuzes gemaakt bij trainen en testen worden gedocumenteerd' en 'Karakteristieken van de dataset worden gedocumenteerd', dienen de procedurele en inputtransparantie. Met de genoemde documentatie kan inzicht verschaft worden in de inputdata en zijn karakteristieken. Hiermee wordt inputtransparantie gecreëerd. Daarnaast wordt inzicht verschaft in de wijze waarop de inputdata wordt geselecteerd, getraind en getest. Dit laatste dient ook de procedurele transparantie. De subgeboden zes en zeven, 'Methoden om risico's te identificeren worden gedocumenteerd' en 'Maatregelen om risico's tegen te gaan worden gedocumenteerd' dienen de procedurele transparantie, doordat de keuzes en afspraken over de inzet van de algoritmen – en zoals eerder is aangegeven, breder getrokken over de inzet van de

5 Algemene Rekenkamer januari 2021, p. 40.
6 Gelissen 9 februari 2021.
7 Algemene Rekenkamer, *Toetsingskader algoritmes: aan de slag. Ethiek*, raadpleegbaar via rekenkamer.nl/onderwerpen/algoritmes-digitaal-toetsingskader/ethiek.

slimme opsporingstechnieken – inzichtelijk worden gemaakt. In al deze subgeboden is ook transparantie als voorwaarde voor (democratische) verantwoording te herkennen. Door openbare documentatie is het afleggen van verantwoording mogelijk. Deze vorm van transparantie is met name te herkennen in het achtste subgebod 'Het is duidelijk wie verantwoordelijk is als het algoritme fouten maakt'.

Ook in het tweede gebod, 'De werking van het algoritme is te verklaren en uit te leggen', zijn verschillende vormen van transparantie te herkennen. De eerste drie subgeboden zijn 'Technische processen zijn inzichtelijk', 'Het systeem is inzichtelijk' en 'Het is inzichtelijk (te maken) hoe het algoritme keuzes op individueel niveau maakt'. In deze drie subgeboden is inhoudelijke transparantie te herkennen. Deze subgeboden maken het stappenplan inzichtelijk waardoor inhoudelijke transparantie ontstaat. Het vierde, vijfde en zesde subgebod komen met name ten goede aan de procedurele transparantie en aan transparantie als voorwaarde voor (democratische) verantwoording. Respectievelijk zijn dit 'Doel van het algoritme is helder', 'Het is inzichtelijk onder welke voorwaarden het algoritme goed functioneert' en 'Het is inzichtelijk wanneer het algoritme accuraat werkt en wat de prestaties zijn'. Ook deze subgeboden stellen dat keuzes en afspraken over de inzet van de algoritmen – en wederom breder getrokken, de inzet van de slimme opsporingstechnieken – vastgelegd dient te worden. Door deze vastlegging kan vervolgens verantwoording afgelegd worden over de inzet van de algoritmen – of ook breder de slimme opsporingstechnieken. In het laatste subgebod, 'Mensen die te maken hebben met een algoritme moeten hierover heldere informatie kunnen krijgen', is ook transparantie als voorwaarde voor (democratische) verantwoording te herkennen. Door het kunnen krijgen van heldere informatie wordt de mogelijkheid om verantwoording te vragen, geboden.

6.1.3 *Conclusie Toetsingskader van de Algemene Rekenkamer*

Geconcludeerd kan worden dat het Toetsingskader van de Algemene Rekenkamer goede handvatten biedt om risico's van de inzet van algoritmen te constateren en dat daarbij aandacht wordt besteed aan de belangrijke ethische toets. In het vierde ethische onderwerp, 'Verklaarbaarheid en transparantie', wordt ook aandacht besteed aan verschillende vormen van transparantie. Minder toereikend is het Toetsingskader in het bieden van handvatten voor het (vooraf) mitigeren van de geconstateerde risico's.

6.2 Richtlijnen voor het toepassen van algoritmen door overheden en publieksvoorlichting over data-analyses

In deze paragraaf zullen de 'richtlijnen voor het toepassen van algoritmen door overheden en publieksvoorlichting over data-analyses' centraal staan. De richtlijnen zullen geïntroduceerd worden en daarna kort geanalyseerd.

In maart 2021 heeft het Ministerie van Justitie en Veiligheid twee richtlijnen gepubliceerd; één voor het toepassen van algoritmen door overheden en één over

publieksvoorlichting over data-analyses. De opgestelde richtlijnen geven een basis weer over wat gedaan zou moeten worden voor het verantwoord toepassen van algoritmen en waar publieksvoorlichting hierover aan zou moeten voldoen. De richtlijnen zijn echter weinig concreet, geven doorgaans geen invulling aan de te hanteren methode en geven niet aan door wie de handelingen verricht dienen te worden. Hierdoor zijn de richtlijnen mijns inziens niet direct toepasbaar in de praktijk.

6.2.1 *Weinig concreet en niet direct toepasbaar*

Als voorbeeld behandel ik hier de aandachtspunten voor onderzoek naar kwaliteit en kwantiteit van databronnen (vallend onder 'Bewustzijn en inperking van risico's').[8] Deelvraag 3 luidt 'Wordt de data over tijd consistent bijgehouden?' Hierbij wordt niet aangegeven wat consistent is en op welke wijze het consistente bijhouden dient te gebeuren. Daarnaast roepen de genoemde vragen bij mij de vraag op door wie dit onderzoek verricht dient te worden. Zou dit – in het geval van de Belastingdienst – dienen te gebeuren door de Inspecteur, de Ontvanger, de controleur, de data-analist, de modelontwerper, de wetgever, de rechter, een extern toezichthouder, et cetera?

Nu deze richtlijnen zijn bedoeld voor alle overheidsorganen is het uiteraard lastig om gedetailleerde voorschriften te bieden. Dat neemt echter niet weg dat een vraag bestaat naar direct toepasbare richtlijnen.[9] De oppervlakkigheid en openheid van deze richtlijnen staan mijns inziens juist haaks op de behoefte aan gedetailleerde richtlijnen voor specifieke overheidsorganen, zodat zij direct toepasbaar zijn. Wanneer de richtlijnen direct toepasbaar zijn is het aannemelijker dat de aanwijzingen eerder worden opgevolgd. Het kost dan immers minder moeite om dit te doen. Als bijvoorbeeld bij de vraag 'Wordt de data over tijd consistent bijgehouden?' aangegeven zou zijn hoe bepaald kan worden wat consistent is, op welke wijze het consistente bijhouden dient te gebeuren en door wie, zou dit gebod direct opgevolgd kunnen worden.

Het overheidsorgaan zou dan slechts de gegeven aanwijzingen voor het bepalen van consistentie, de wijze van consistent bijhouden dienen op te volgen en zorg te dragen dat de juiste personen dit doen. Doordat het ontbreekt aan deze aanwijzingen dient het overheidsorgaan hier zelf over na te denken, alvorens het gebod uit te kunnen voeren, waardoor die uitvoering meer moeite en tijd kost.

6.2.2 *Transparantie en vastlegging in de richtlijnen*

Onder het kopje 'Transparantie en uitlegbaarheid', wordt nader stilgestaan bij de kwaliteitseisen. Deze kwaliteitseisen zijn mijns inziens nog steeds weinig concreet zijn. Hoewel duidelijke regels worden omschreven over het vastleggen van gemaakte keuzes en het ontwerpproces, ontbreekt het aan een uitleg over de wijze waarop de

8 Ministerie van Justitie en Veiligheid 1 maart 2021, p. 20.

9 Zie Doove & Otten 2018 voor het door hen, namens het CBS, uitgevoerde verkennend onderzoek naar het gebruik van algoritmen binnen overheidsorganen.

kwaliteit gedefinieerd dient te worden en vanaf wanneer sprake is van kwalitatief goede databronnen en kwalitatief minder goede databronnen. Bovendien wordt ook hier niet ingegaan op de vraag wie precies dient te documenteren. Desalniettemin, worden nieuwe inzichten gegeven voor openbaar toegankelijke documentatie en evaluatie mogelijkheden. Uit de geboden 'Organiseer de code in modules welke separaat en gecombineerd kunnen worden geëvalueerd' en 'Test deze modules op correcte functionaliteit zowel afzonderlijk als in combinatie' zou inspiratie ontleend kunnen worden voor het formuleren van de aanbevelingen.[10]

6.2.3 *Tussenconclusie: richtlijnen voor het toepassen van algoritmen door overheden en publieksvoorlichting over data-analyses*

Geconcludeerd kan worden dat de richtlijnen niet direct toepasbaar zijn, omdat de gedefinieerde geboden ruimte over laten voor vragen en dit eist nadere invulling door het overheidsorgaan dat de geboden toe wil passen. De algemeenheid van de richtlijnen is te verklaren doordat zij zijn bedoeld voor alle overheidsorganen. Dit neemt echter niet weg dat direct toepasbare richtlijnen de voorkeur genieten. Toch, kan aan de gestelde richtlijnen in zijn algemeenheid inspiratie ontleend worden voor het formuleren van aanbevelingen voor (de inzet van) rechtsstatelijke slimme opsporingstechnieken voor de Nederlandse Belastingdienst.

6.3 Toolbox Ethisch Verantwoorde Innovatie

De Toolbox Ethisch Verantwoorde Innovatie is te vinden op de website digitaleoverheid.nl. De Digitale Overheid wil een brug slaan tussen 'het beleid en de professionals die werken aan digitalisering van de overheid'.[11] De Toolbox Ethisch Verantwoorde Innovatie helpt ontwikkelaars en biedt bestuurders een handreiking voor ethisch verantwoorde innovatie; dat wil zeggen 'met respect voor belangrijke publieke waarden en grondrechten'. Het gebruik van innovatieve technologieën door de overheid neemt toe en daarmee ook de invloed die deze technieken kunnen hebben 'op belangrijke publieke waarden, zoals privacy, rechtsgelijkheid en autonomie'. Om overheden te helpen hier verantwoord mee om gaan is de Toolbox Ethisch Verantwoorde Innovatie ontwikkeld.[12] Slimme opsporingstechnieken vallen onder de innovatieve technologieën waar de toolbox voor ontwikkeld is. In deze paragraaf zal de opbouw van deze toolbox genoemd worden en zal een globale analyse gegeven worden over de verankering van transparantie in deze toolbox.

10 Ministerie van Justitie en Veiligheid 1 maart 2021, p. 22.

11 Digitale Overheid, *Over ons. Voor professionals*, raadpleegbaar via digitaleoverheid.nl/dossiers/over-ons/.

12 Digitale Overheid, *Over de Toolbox voor Ethisch Verantwoorde Innovatie*, raadpleegbaar via digitaleoverheid.nl/overzicht-van-alle-onderwerpen/nieuwe-technologieen-data-en-ethiek/publieke-waarden/toolbox-voor-ethisch-verantwoorde-innovatie/over-de-toolbox-voor-ethisch-verantwoorde-innovatie/.

6.3.1 *De opbouw van de Toolbox Ethisch Verantwoorde Innovatie*

De toolbox is onderverdeeld in zeven kernprincipes, te weten: 'Kwaliteit data, algoritmes en analyses', 'Belanghebbenden betrekken', 'Transparantie en verantwoording', 'Wet- en regelgeving respecteren', 'Monitoren en evalueren', 'Veiligheid borgen' en 'Publieke waarden centraal'. De toolbox is te benaderen via de website van de Digitale Overheid.[13] De toolbox bestaat uit allerlei *tools* die overzichtelijk en per kernprincipe zijn weergegeven. Per kernprincipe wordt een uitleg gegeven over de risico's van de inzet van de innovatieve technologieën. Ieder kernprincipe heeft een eigen deelpagina. Op iedere pagina wordt doorverwezen naar andere middelen die ook kunnen helpen bij het ethisch verantwoord innoveren. Hierna zal nader worden ingegaan op het kernprincipe 'Transparantie en verantwoording'.

6.3.2 *Het kernprincipe 'Transparantie en verantwoording'.*

Het kernprincipe 'Transparantie en verantwoording' kent drie geboden. Dat zijn 'Houd in het ontwerp al rekening met transparantie', 'Leg verantwoording af over de juiste zaken' en 'Zorg voor effectieve communicatie'. Hierna zullen deze drie geboden geanalyseerd worden.

Bij het eerste gebod ligt de nadruk op inhoudelijke transparantie en transparantie als voorwaarde voor (democratische) verantwoording: 'Systemen en processen moeten in de basis al uitlegbaar en te verantwoorden zijn'.[14] Het gaat hier om de systemen en processen van de innovatieve technologieën. Daarom wordt gedoeld op inhoudelijke transparantie en niet op procedurele transparantie. Die laatste vorm van transparantie ziet namelijk op de keuzes en afspraken die zijn gemaakt voor de inzet van de innovatieve technologieën, maar gaat niet over de uitlegbaarheid van de innovatieve technologie zelf. Bij inhoudelijke transparantie gaat het hier wel om. De toolbox geeft aan dat als het 'technisch niet mogelijk is om een systeem keuzes in 'normale mensentaal' te laten verwoorden, dit aanleiding kan zijn om die keuzes niet door het systeem te laten maken'.[15] Hierin is transparantie als voorwaarde voor (democratische) verantwoording te herkennen. In de toolbox wordt aangeven dat '*open source software* bij uitstek zorgt voor transparantie'. Bij *open source software* is de broncode van het innovatieve programma voor iedereen raadpleegbaar, ofwel publiekelijk toegankelijk. De broncode is de door de programmeur ontwikkelde code die de basis

13 Digitale Overheid, *Toolbox Ethisch Verantwoorde Innovatie*, raadpleegbaar via digitaleoverheid.nl/overzicht-van-alle-onderwerpen/nieuwe-technologieen-data-en-ethiek/publieke-waarden/toolbox-voor-ethisch-verantwoorde-innovatie/.

14 Digitale Overheid, *Transparantie en verantwoording. Wees transparant en leg verantwoording af*, raadpleegbaar via https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/nieuwe-technologieen-data-en-ethiek/publieke-waarden/toolbox-voor-ethisch-verantwoorde-innovatie/transparantie-en-verantwoording/.

15 Digitale Overheid, *Transparantie en verantwoording. Wees transparant en leg verantwoording af*, raadpleegbaar via https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/nieuwe-technologieen-data-en-ethiek/publieke-waarden/toolbox-voor-ethisch-verantwoorde-innovatie/transparantie-en-verantwoording/.

vormt van de software.[16] Bij algoritmen is de broncode het script dat gebruikt wordt om automatisch het stappenplan te volgen. Hoewel open source software bijdraagt aan transparantie is het ook gevoelig voor misbruik. Doordat de broncode beschikbaar is, kunnen hackers relatief eenvoudig fouten ontdekken en de software hacken. Daarnaast kan de broncode, in het geval van slimme opsporingstechnieken bij belastingadministraties, informatie prijsgeven over het gevoerde selectiebeleid en dat kan bijdragen aan het in hoofdstuk 5 behandelde gevaar van *gaming the system*.

Daartegenover staat dat *open source software* innovatie stimuleert doordat verschillende programmeurs gebruik kunnen maken van dezelfde broncode en de *open source software* kunnen controleren. Hierover wordt in de toolbox het volgende aangegeven: 'Andere specialisten kunnen bijvoorbeeld veiligheidsrisico's opmerken. Of foutieve of bevoordeelde patronen of processen identificeren'.[17] Met name het laatste – het onderling controleren van de software – vind ik een waardevolle meerwaarde van open source software. Echter, ik betwijfel of deze meerwaarde zwaarder weegt dan de hiervoor genoemde nadelen. Zodoende gaat mijn voorkeur uit naar een middenweg: stel de broncode beschikbaar in een beveiligde omgeving voor een (beperkte) groep (ethische) programmeurs en voor de rechter[18] die rechtsbescherming en/of rechtsherstel voor de individuele belastingplichtige dient te bieden. In de beveiligde omgeving kan dan onderling getoetst worden op risico's zoals discriminatie, zonder dat iedereen vrijuit de broncode kan raadplegen en gebruiken. Ook de rechter wordt hiermee in staat gesteld om alle relevante feiten en omstandigheden, waaronder de wijze waarop het besluit tot stand is gekomen, te analyseren en hierdoor tot een gemotiveerde beslissing te komen.

In gebod twee wordt hier ook bij stilgestaan. Hierin wordt benoemd dat transparantie niet identiek is aan volledige openbaarheid. Dit sluit aan bij het bovenstaande en tevens ook bij hetgeen in par. 4.2.2. is genoemd over transparantie als voorwaarde voor (democratische) verantwoording. Namelijk dat gewaakt dient te worden dat een wirwar aan informatie ontstaat waardoor de burger door de bomen het bos niet meer ziet.

Het laatste gebod sluit hier ook bij aan. Hier wordt aangegeven dat niet alleen inhoudelijke transparantie is vereist, maar ook procedurele transparantie, 'de reden om

16 Nussbaum 1984, p. 285.

17 Digitale Overheid, *Transparantie en verantwoording. Wees transparant en leg verantwoording af. Tips voor het gebruik van open source software*, raadpleegbaar via digitaleoverheid.nl/overzicht-van-alle-onderwerpen/nieuwe-technologieen-data-en-ethiek/publieke-waarden/toolbox-voor-ethisch-verantwoorde-innovatie/transparantie-en-verantwoording/.

18 Later, zal in par. 7.4. blijken dat deze toegang ook zou moeten gelden voor een gespecialiseerd toezichthoudend orgaan die een aanvullende en ondersteunde rol voor de rechterlijke macht vervult.

technologie in te zetten'.[19] Daarnaast wordt hier benoemd dat informatie gegeven dient te worden in 'duidelijke en eenvoudige taal'.

6.3.3 *Tussenconclusie Toolbox Ethisch Verantwoorde Innovatie*

Geconcludeerd kan worden dat de Toolbox Ethisch Verantwoorde Innovatie omvangrijk is, omdat het zeven onderwerpen aanstipt. De risico's per kernprincipe worden duidelijk omschreven. Tegelijkertijd is geconstateerd dat relatief veel wordt doorverwezen naar andere hulpmiddelen om ethisch verantwoord te kunnen innoveren. Dit is ook logisch gelet op de naam. Het is een toolbox, ofwel gereedschapskist, met daarin gereedschap en uitleg over dat gereedschap om ethisch verantwoord te kunnen innoveren. Het enkele raadplegen van de toolbox is hierdoor niet voldoende om ethisch verantwoord te kunnen innoveren. Hiervoor zullen ook de gereedschappen waarnaar verwezen wordt, geraadpleegd moeten worden. Met andere woorden om direct toepasbare aanwijzingen te vinden is het noodzakelijk om een ander hulpmiddel te raadplegen.

Mijns inziens werkt dit niet optimaal in de praktijk. Medewerkers van de Belastingdienst kunnen zich hierdoor namelijk niet beperken tot het raadplegen van één alles omvattende richtlijn, maar zijn genoodzaakt om meerdere richtlijnen te raadplegen. Ik kan mij voorstellen dat dit niet ten goede komt aan de efficiëntie. Hierbij merk ik op dat deze aanname niet is geverifieerd door middel van empirisch onderzoek, hetgeen zich wellicht leent voor vervolgonderzoek.

6.4 **Visie van de Nationale ombudsman**

De Nationale ombudsman van Nederland heeft zijn visie op het gebruik van data en algoritmen door de overheid vastgelegd in een online beschikbaar gestelde brochure.[20] De brochure begint met een samenvatting. Hierin worden mijns inziens overzichtelijk de belangrijkste aandachtspunten vermeld. Bovendien wordt een praktijkvoorbeeld[21] gegeven aan de hand waarvan de aandachtspunten nader ingevuld worden en staat het burgerperspectief centraal.[22] Dat burgerperspectief is mijns inziens het meest waardevolle van deze visie. Zodoende ligt hier in deze paragraaf het zwaartepunt op.

19 Digitale Overheid, *Transparantie en verantwoording. Wees transparant en leg verantwoording af. Zorg voor effectieve communicatie*, raadpleegbaar via digitaleoverheid.nl/overzicht-van-alle-onderwerpen/nieuwe-technologieen-data-en-ethiek/publieke-waarden/toolbox-voor-ethisch-verantwoorde-innovatie/transparantie-en-verantwoording/.

20 Nationale ombudsman, *Ombudsvisie op gebruik van data en algoritmen door de overheid: stel burgers centraal*, raadpleegbaar via https://www.nationaleombudsman.nl/system/files/bijlage/DEF%202.0%20Rapport%20%E2%80%93%20Een%20burger%20is%20geen%20dataset_0.pdf"https://www.nationaleombudsman.nl/system/files/bijlage/DEF%202.0%20Rapport%20%E2%80%93%20Een%20burger%20is%20geen%20dataset_0.pdf

21 Het praktijkvoorbeeld is te vinden op p. 4 van de brochure en gaat over een burger die meermaals verkeersboetes ontving en motorrijtuigenbelasting dient te betalen voor auto's die niet van haar zijn.

22 Govers e.a. 2021, p. 9.

6.4.1 *Het burgperspectief in de visie van de Nationale ombudsman*

Door het praktijkvoorbeeld gaat het burgerperspectief beter leven, het maakt de risico's tastbaarder. 'Het burgerperspectief centraal stellen, betekent vanuit behoorlijkheid dat de overheid de verantwoordelijkheid neemt door burgers te betrekken bij de ontwikkeling, toepassing en het gebruik van data en algoritmen, betekenisvol menselijk contact borgt en ruimte biedt voor maatwerk.'[23] Dit wordt niet expliciet vermeld in de andere kaders. Verspreid door de brochure heen staan verschillende citaten van burgers over de wijze waarop zij het gebruik van data en algoritmen door de overheid ervaren. Dit geeft het burgerperspectief op een indringende en tastbare wijze weer. Het gevoel en het belang van goede waarborgen gaat hierdoor mijns inziens meer leven. Meer dan bij de Toolbox Ethisch Verantwoorde Innovatie, terwijl de risico's ook daar helder uiteen zijn gezet.

Naast het burgerperspectief, worden ook concrete handvatten gegeven zoals 'Wees toegankelijk door te weten welke burger zich achter de data bevindt en voor hem/haar bereikbaar te zijn'.[24] De aandachtspunten die in de hiervoor behandelde kaders aan bod zijn gekomen worden ook door de Nationale ombudsman benoemd en uitgewerkt. Zo staat de Nationale ombudsman stil bij duidelijkheid.[25] De Nationale ombudsman geeft net als de Algemene Rekenkamer aan dat het doel voor het gebruik van de data en algoritmen in kaart gebracht moet worden. Zo ontstaat duidelijkheid voor de burger. Hierin is procedurele transparantie te herkennen. Hierover is ook een citaat van een burger opgenomen in de brochure: 'Ik weet het eigenlijk niet, er gebeuren wel meer dingen die wij niet weten'.[26] In een ander citaat van een burger is inhoudelijke transparantie te herkennen. Het citaat luidt als volgt: 'Op basis waarvan de machine dan beslissingen maakt moet je wel duidelijk communiceren'.[27] Dit citaat maakt duidelijk dat de burger waarde hecht aan inhoudelijke transparantie. In nog een ander citaat komen beide vormen van transparantie naar voren: 'Wat is dan de procedure, en op basis waarvan beslissen ze dan'.[28] Door het noemen van deze citaten staat ook bij het geven van de concrete handvatten het burgerperspectief centraal.

6.4.2 *Tussenconclusie: Visie van de Nationale ombudsman*

Kortom, in de visie van de Nationale ombudsman staat het burgerperspectief centraal. Deze visie wordt goed geïllustreerd door een praktijkvoorbeeld en het geven van verscheidene citaten van burgers. In de visie zijn handvatten gegeven die bijdragen aan transparantie. Hierbij wordt ook steeds aandacht besteed aan het burgerperspectief waardoor het geheel completer is. Zoals is aangegeven, vind ik het burgerperspectief het meest waardevolle element van de visie. De visie kan gebruikt

23 Govers e.a. 2021, p. 6.
24 Govers e.a. 2021, p. 11.
25 Govers e.a. 2021, p. 11.
26 Govers e.a. 2021, p. 13.
27 Govers e.a. 2021, p. 13.
28 Govers e.a. 2021, p. 13.

worden om belastingambtenaren bewust te maken van dit burgerperspectief en om de impact die de inzet van slimme opsporingstechnieken kan hebben op burgers beter inzichtelijk te maken.

6.5 Het Algoritmeregister van de stad Amsterdam

In deze paragraaf zal het Algoritmeregister van de stad Amsterdam toegelicht worden. Dit Algoritmeregister wordt gezien als een good practice van het vastleggen van de wijze waarop algoritmen worden ingezet, op een manier zodat die voor de burger begrijpelijk is.

6.5.1 *Wat is het Algoritmeregister van de stad Amsterdam?*

De gemeente Amsterdam geeft in zijn zogenaamde Algoritmeregister – welke vrij en gemakkelijk online raadpleegbaar is – een overzicht van de algoritmen die de gemeente bij de uitoefening van zijn dienstverlening gebruikt.[29] Naast dit duidelijke overzicht wordt ook uitleg gegeven over de inzet, het doel en de invloed die de Amsterdamse algoritmen hebben en de bij de inzet van de algoritmen genomen ethische waarborgen. Hiermee worden de procedurele en inhoudelijke transparantie gewaarborgd. Daarnaast wordt per algoritme simpel uitgelegd waar het algoritme voor wordt gebruikt. Het doel van het Algoritmeregister is tweeledig. Enerzijds dient het Algoritmeregister de transparantie van (de inzet) van de algoritmen en fungeert het als informatiebron hierover, anderzijds is het een uitnodiging van de initiatiefnemers aan andere overheidsinstanties om ook een algoritmeregister te introduceren en hierover van gedachten te wisselen.

6.5.2 *Achtergrond en doelstelling van het Algoritmeregister van de stad Amsterdam?*

Een nadere onderbouwing van de doelstelling voor het ontwikkelen en implementeren van het Algoritmeregister is weergeven in de zogenaamde *whitepaper* geschreven door Haataja, Van de Fliert en Rautio. Hierin staat onder meer omschreven wat een algoritmeregister volgens de initiatiefnemers dient te bevatten. De initiatiefnemers zijn de stad Amsterdam en de stad Helsinki (Finland). Zij hebben samen het publiekelijk toegankelijke algoritmeregister ontwikkeld.
Hoewel zij niet de eerste zijn die de idee van een openbaar algoritmeregister hebben bedacht, ‘geloven zij wel de eerste overheidsorganisaties te zijn die een dergelijk algoritmeregister hebben geïmplementeerd’.[30]

29 Gemeente Amsterdam, online geraadpleegd op 7 juni 2022.

30 Haataja, Van de Fliert & Rautio september 2020, p. 6. De auteurs geven aan ‘Over the last year, similar suggestions have been brought into discussion also by civil society organisations. Most recently, AlgorithmWatch and Access Now suggested the similar concept in their responses to the consultation of EU Commission High-Level Expert Group on AI during summer 2020’.

In een algoritmeregister dient volgens hen een overview die voor iedereen begrijpelijk is, gegeven te worden.[31] Verantwoordelijkheid speelt ook hier een rol, het moet duidelijk zijn wie waar verantwoordelijk voor is, op welke wijze de verantwoordelijke partijen gecontacteerd kunnen worden en welke externe partijen betrokken zijn. Hier komt transparantie als voorwaarde voor (democratische) verantwoording naar voren. Andere secties zouden moeten zijn *datasets, dataprocessing, non-discrimination, human oversight, risks, explainability* en *references*.[32] Deze waarborgen komen ook terug in de andere kaders. *Human oversight* wordt hier wel meer benadrukt dan in de andere kaders. In de *whitepaper* wordt namelijk aangegeven dat een algoritmeregister een duidelijke omschrijving van het volgende dient te bevatten: 'Description of the capability and support for human intervention in the system design and development, decision cycles, and in the monitoring of the system's operation. Description of the necessary competencies required for successfully performing the function and the training provided for gaining such skills and competencies.'[33] In de andere kaders is geen, althans niet expliciet, aandacht besteed aan het vastleggen van de vaardigheden die nodig zijn voor de ambtenaren die gebruikmaken van de algoritmen. In het geval van de slimme opsporingstechnieken bij de belastingadministraties zou het dan gaan om het vastleggen van de benodigde vaardigheden van de belastingambtenaren die gebruikmaken van de resultaten van de slimme opsporingstechnieken. Dit kan bijdragen aan het afleggen van verantwoording over de inzet van de slimme opsporingstechnieken aan de burger.

6.5.3 *Tussenconclusie: het Algoritmeregister van de stad Amsterdam*

Geconcludeerd kan worden dat het initiatief tot een openbaar toegankelijk algoritmeregister bijdraagt aan procedurele transparantie, inhoudelijke transparantie en transparantie als voorwaarde voor (democratische) verantwoording. De whitepaper geeft een heldere uitleg over de wijze waarop een algoritmeregister vorm dient te krijgen. Doordat het Algoritmeregister bijdraagt aan de verschillende vormen van transparantie kan het voor belastingadministratie dienen als inspiratiebron om zelf te komen tot een initiatief om deze vormen van transparantie te kunnen waarborgen.

6.6 Tussenconclusie: bestaande richtinggevende kaders

In dit hoofdstuk stond de volgende vraag centraal: 'Welke richtinggevende kaders bestaan al ten aanzien van transparantie van het gebruik van algoritmen, Big Data-analyse en profiling, meer specifiek voor de Nederlandse Belastingdienst?'

Er is in Nederland momenteel nog geen wet- en regelgeving van kracht ten aanzien van transparantie van het gebruik van algoritmen, Big Data-analyse en profiling. Wel zijn meerdere richtinggevende kaders en andere hulpmiddelen ontwikkeld.

31 Haataja, Van de Fliert & Rautio september 2020, p. 7.
32 Haataja, Van de Fliert & Rautio september 2020, p. 8 en 9.
33 Haataja, Van de Fliert & Rautio september 2020, p. 9.

Daar is in dit hoofdstuk bij stilgestaan. Meer specifiek is stilgestaan bij het Toetsingskader van de Algemene Rekenkamer, richtlijnen voor het toepassen van algoritmen door overheden en publieksvoorlichting over data-analyses, de Toolbox Ethisch Verantwoord Innoveren, de visie van de Nationale ombudsman en het Algoritmeregister van de stad Amsterdam.

Geconcludeerd kan worden dat aan alle vijf de behandelde kaders en hulpmiddelen handvatten ontleend kunnen worden voor aanbevelingen voor een nieuw (wettelijk) kader voor de inzet van slimme opsporingstechnieken door de Nederlandse Belastingdienst. Het Toetsingskader van de Algemene Rekenkamer biedt handvatten voor het doorlopend toetsen van gebruikte algoritmen, maar is minder geschikt voor het (vooraf) mitigeren van geconstateerde risico's. Uit de richtlijnen voor het toepassen van algoritmen door overheden en publieksvoorlichting over data-analyses kan in zijn algemeenheid inspiratie ontleend worden voor de te formuleren aanbevelingen. De geboden in de richtlijnen zijn echter mijns inziens niet concreet genoeg om direct door een overheidsorganisatie toegepast te kunnen worden. De Toolbox Ethisch Verantwoorde Innovatie omvat zeven kernprincipes en is daarmee zeer omvangrijk. Een door mij geconstateerd nadeel van deze toolbox is dat veel doorverwezen wordt naar andere hulpmiddelen om ethisch verantwoord te innoveren. Het enkele raadplegen van de toolbox is onvoldoende om de risico's van (de inzet van) slimme opsporingstechnieken te kunnen mitigeren. De visie van de Nationale ombudsman biedt met name een meerwaarde op het gebied van het burgperspectief. De brochure van de visie waarin het burgerperspectief is verweven, kan gebruikt worden om belastingambtenaren bewust te maken van dit burgerperspectief en om de impact die de inzet van slimme opsporingstechnieken kan hebben op burgers beter inzichtelijk te maken. Het Algoritmeregister van de stad Amsterdam is een concreet voorbeeld over de wijze waarop transparantie van het gebruik van slimme opsporingstechnieken gecreëerd kan worden. Tot slot kan geconcludeerd worden dat de geraadpleegde kaders – openbaar toegankelijke – documentatie als belangrijk zien. Deze documentatie draagt bij aan het realiseren van verschillende vormen van transparantie.

7 Aanbevelingen voor een rechtsstatelijk gebruik van slimme opsporingstechnieken

In dit hoofdstuk zal antwoord gegeven worden op de laatste deelvraag: 'Welke aanbevelingen kunnen bijdragen aan een meer rechtsstatelijk gebruik van algoritmen, Big Data-analyse en profiling door de Nederlandse Belastingdienst?' Grofweg kunnen er twee soorten methoden onderscheiden worden om tot een meer rechtsstatelijk gebruik te komen. Dit zijn methoden die 'discriminatie in algoritmische processen *onthullen*' en 'methoden die algoritmische processen *corrigeren*' (cursivering door auteur).[1] 'Algoritmische processen' kan in dit verband gelijkgesteld worden aan slimme opsporingstechnieken. Bij de beantwoording van de deelvraag zullen beide soorten methoden aan bod komen. Uitgangspunt bij de beantwoording van deze deelvraag zijn de in hoofdstuk 5 geconstateerde risico's en belemmeringen van (de inzet van) slimme opsporingstechnieken. Daarnaast is inspiratie ontleend aan de in hoofdstuk 6 behandelde richtinggevende kaders. Op basis hiervan zijn vier aanbevelingen geformuleerd: een controlegroep, verplichte, openbaar toegankelijke documentatie, Big Data-analyse en zelflerende algoritmen als laatste middel met effectieve menselijke tussenkomst en een onafhankelijk toezichthoudend orgaan. Deze aanbevelingen zullen ieder in een afzonderlijke paragraaf behandeld worden.[2] Hierna zal het onderwerp 'sancties bij overtreding' aangestipt worden.

7.1 Een controlegroep voor controle vooraf[3]

In deze paragraaf zal de aanbeveling 'een controlegroep voor controle vooraf' toegelicht worden. Daartoe zal allereerst de noodzaak van deze controlegroep toegelicht worden. Hierna zal aangegeven worden uit wie deze controlegroep dient te bestaan en welke taak deze controlegroep dient te verrichten. Deze aanbeveling om tot een rechtstatelijk gebruik van de slimme opsporingstechnieken te komen, behoort tot

1 Hacker 2019, p. 28.

2 Nota bene, de volgorde van aanbevelingen is willekeurig gekozen en geeft derhalve geen indicatie van prioriteit aan.

3 Na het afronden van deze thesis is op 17 maart 2023 de Adviescommissie Analytics bij Financiën van start gegaan. Deze adviescommissie voldoet in bepaalde mate aan de aanbeveling die hier wordt gegeven. Aangezien de adviescommissie is ingesteld na het afronden van de thesis is hier echter geen aandacht aanbesteed. Zie voor meer informatie over de start van de adviescommissie: rijksoverheid.nl/actueel/nieuws/2023/03/17/adviescommissie-analytics-bij-financien-van-start.

de eerste soort methoden; methoden die discriminatie in de slimme opsporingstechnieken onthullen.

7.1.1 *De noodzaak voor een controlegroep voor controle vooraf*

Aanleiding voor het opstellen van deze aanbeveling zijn de risico's van *biased data*, (indirecte) *proxy* discriminatie en het trekken van subjectieve of zelfs discriminerende verbanden uit Big Data-analyse. Zoals is genoemd in par. 5.1, zijn data veelal biased, vooroordelen gaan schuil in de data. Dit kan ertoe leiden dat slimme opsporingstechnieken een ongerechtvaardigd discriminerend effect hebben. Ook het gebruik van een proxy kan leiden tot (indirecte) discriminatie. Voor het bepalen van de mate van rechtvaardiging van de discriminatie dient de oorzaak van de discriminatie bekend te zijn. (Indirecte) proxy discriminatie wordt vaker gerechtvaardigd dan discriminatie vanwege *biased data*.[4] Het is daarom van belang dat input- en outputdata worden geanalyseerd op indicatoren van discriminatie.[5] De controle voor de inzet van de slimme opsporingstechnieken dient ook een dergelijke analyse te bevatten.

Het zoeken naar verbanden en patronen in grote hoeveelheden data kan eveneens leiden tot discriminatie. Bepaalde verbanden en patronen zullen namelijk altijd gevonden worden, daar zullen ook verbanden en patronen tussen zitten die niet objectief zijn of niet logisch te koppelen zijn aan het te detecteren risico. Sommige verbanden zullen ook subjectief of zelfs discriminerend zijn. In hoofdstuk 5 werden hiervan twee voorbeelden genoemd. Het eerste voorbeeld over de eigenwoningrenteaftrekregeling had betrekking op een relatief onschuldige risicofactor als de kleur van een auto. In het tweede voorbeeld was die risicofactor minder onschuldig. In dit voorbeeld was een verband waargenomen tussen het hebben van een handicap en fraude in de zorgkostenaftrek. Doordat deze verbanden niet logisch te koppelen zijn aan de regeling, bestaat een verhoogde kans op een ongerechtvaardigde, ongelijke behandeling. Zoals is geconstateerd, is dan al snel sprake van discriminatie. Zicht op dit risico en het beperken hiervan is van groot belang. Geconcludeerd is verder dat het hanteren van een meer objectieve risicofactor de kans op het intreden van discriminatie verkleint (zie par. 5.3).

7.1.2 *Strategieën om bias te verminderen*

Als geconstateerd is dat de slimme opsporingstechnieken (ongerechtvaardigd) discrimineren, dan zullen strategieën ter vermindering van de bias een rol moeten gaan spelen.[6] Hacker en Wiedemann verdelen deze strategieën onder in 'vier verschillende soorten benaderingen: *pre-processing* benaderingen die de inputdata bewerken, *in-processing* benaderingen die het pad van input- naar outputdata inzichtelijk pogen te maken en pogen te controleren, *post-processing* benaderingen die de outputdata veranderen naar een eerlijke representatie en *reality check* benaderingen

4 Hacker 2019, p. 20.
5 Hacker 2019, p. 28.
6 Hacker 2019, p. 29.

die beoordelen of de outputdata wel vergelijkbaar is met echte uitkomsten.'[7] Het reikt voor dit onderzoek te ver om de technische werkwijze van al deze verschillende methoden uiteen te zetten. Geconstateerd kan worden dat bias enerzijds effectief geëlimineerd kan worden door wijzigingen aan te brengen in de trainingsdata en anderzijds door het trainingsproces op non-discriminatie aan te sturen. Daarnaast kan bias geëlimineerd worden uit de output, hier zien de post-processing en reality check benaderingen op.

Een voor de hand liggende pre-processing methode om bias weg te halen is het elimineren van gevoelige karakteristieken, zoals etniciteit of geslacht.[8] Echter, zoals duidelijk is geworden in par. 5.1, zal deze ogenschijnlijke simpele oplossing geen profijt bieden wanneer sprake is van correlatiebias. Doordat de *gevoelige* karakteristieken (onbewust) verbonden zijn met *ongevoelige* karakteristieken kunnen zij zichtbaar zijn in de output van de slimme opsporingstechniek. Hierdoor kan de slimme opsporingstechniek een discriminerend effect hebben, ondanks de directe eliminatie van de gevoelige karakteristiek.

Een andere methode voor het elimineren van bias die wellicht voor de hand ligt, maar eveneens niet het gewenste effect zal hebben, is het trainen op enkel trainingsdata van de gevoelige groep. Bij deze methode wordt namelijk geen rekening gehouden met eventuele historische bias. Calders en Žliobaitė omschrijven dit met een voorbeeld van een algoritmisch model voor toelatingen tot een universiteit.[9] Als twee verschillende sets trainingsdata voor mannen en vrouwen worden gebruikt en uit de trainingstest voor mannen blijkt dat zij worden toegelaten met een score van 70 of hoger en vrouwen met een score van 80 of hoger, zal het gehele systeem nog altijd als discriminerend worden beschouwd, ondanks het gebruik van twee verschillende sets aan trainingsdata.

Effectieve methoden om bias uit trainingsdata te halen die Calders en Žliobaitė voordragen zijn het wijzigen van de labels van de trainingsdata, het dupliceren of verwijderen van individuele gevallen, het toevoegen van synthetische gevallen en het aanpassen van data aan de nieuwe representatieve context.[10] Dit is geen uitputtende lijst en combinaties van de verschillende methoden zijn eveneens denkbaar.

Naast het wijzigen van de trainingsdata kan het trainingsproces ook dusdanig worden gestuurd dat het non-discriminatie afdwingt[11], dit zijn de in-processing methoden. In-processing methoden zien op het controleren van het algoritmische proces van input- naar outputdata.[12] In-processing methoden houden nauwverband met de erkende inhoudelijke transparantie die inzicht vereist in de wijze waarop een bepaalde beslissing tot stand is gekomen. Een methode om bias binnen dit proces

7 Hacker & Wiedemann 2017, p. 28.
8 Calders & Žliobaitė, in: *Springer* 2013, p. 12.
9 Calders & Žliobaitė, in: *Springer* 2013, p. 13.
10 Calders & Žliobaitė, in: *Springer* 2013, p. 14.
11 Calders & Žliobaitė, in: *Springer* 2013, p. 14.
12 Hacker & Wiedemann 2017, p. 16.

van input- naar outputdata te beperken is het minimaliseren van de verschillende waarden tussen individuen en groepen.[13]

7.1.3 *De inrichting van een controlegroep voor controle vooraf*

Om de kans op *biased data* en (indirecte) proxy discriminatie te minimaliseren dient de Nederlandse Belastingdienst te investeren in data-analisten die in staat zijn om de hiervoor genoemde technieken ter minimalisatie van bias en proxy discriminatie toe te passen. Om het trekken van subjectieve of zelfs discriminerende verbanden uit Big Data-analyse in te perken, zouden belastingadministraties de volgende regel kunnen hanteren: vóór de inzet van een risicofactor, die is ontleend uit Big Data-analyse, dient door een diverse, inclusieve groep aan experts nagegaan te worden of die risicofactor 1) logischerwijs te koppelen is aan de regeling waarin dat risico zich voor kan doen, 2) een objectief karakter heeft en 3) niet (overduidelijk) tot een ongerechtvaardigde, ongelijke behandeling leidt. Als dit het geval is, dan heeft het gebruik van de risicofactor slechts een kleine kans op ongerechtvaardigde, ongelijke behandeling en is het gebruik van de risicofactor gemakkelijker uit te leggen. Ik licht dit nader toe.

Een risicofactor is logischerwijs te koppelen aan een regeling indien de risicofactor een element is van de regeling of daar inherent mee samenhangt. Bij de eigenwoningrenteaftrekregeling is als voorbeeld de hoogte van de hypotheekrente gegeven en bij de zelfstandigenaftrek de ratio omzet en gemaakte uren. Als de risicofactor (hoogte hypotheekrente respectievelijk omzet en gemaakte uren) logischerwijs te koppelen is aan de regeling waarin het risico zich voor kan doen, dan is de risicofactor gemakkelijker te verklaren en uit te leggen aan de belastingplichtigen. Belastingplichtigen zullen eerder begrijpen dat zij vanwege de hoogte van hun hypotheekrente (extra) worden gecontroleerd, dan vanwege het (toevallig) hebben van een rode auto. De hoogte van de hypotheekrente heeft namelijk invloed op de eigenwoningrenteaftrekregeling. De kleur van een auto heeft dat niet.

Nijssen en Stevens doen een soortgelijke aanbeveling. Volgens hen zouden 'de beslis- en rekenregels en de gegevensmodellen[14] moeten worden omgezet naar een softwarecode op basis waarvan ICT-systemen uitlegbare geautomatiseerde beslissingen kunnen nemen. Om de beslissingen ook echt uitlegbaar te laten zijn, is het nodig dat de beslis- en rekenregels waarop de softwarecode is gebaseerd, te herleiden zijn tot de wettelijke regels in de databank wetten.nl.[15] Dit herleiden komt neer op het logischerwijs kunnen koppelen van een risicofactor aan de regeling.

Als een risicofactor logischerwijs te koppelen is aan de regeling, dan is de risicofactor meteen objectiever. Een element van de regeling is namelijk objectief bepaalbaar. De kleur van een auto is ook objectief bepaalbaar, maar is niet nodig voor het vaststellen van de (on)juistheid van de toepassing van een regeling. Ook het hebben van een

13 Calders & Žliobaitė, in: *Springer* 2013, p. 14.
14 Waar de Belastingdienst gebruik van maakt.
15 Nijssen & Stevens 16 september 2019, p. 1105.

tweede nationaliteit is objectief bepaalbaar, maar kan toch een subjectief karakter hebben als nationaliteit geen enkele rol speelt bij de toepassing van de regeling. Het zou kunnen dat nationaliteit als risicofactor voortvloeit uit een bias die aanwezig is geweest in de dataset waaruit het verband tussen nationaliteit en het risico op fraude is getrokken. Die bias heeft een subjectief karakter en de hieruit voortgevloeide risicofactor indirect ook.

Het selecteren van een geschikte risicofactor is een primaire taak van de programmeur van de slimme opsporingstechniek. Het is echter wenselijk dat het selecteren van een geschikte risicofactor in overleg met verschillende experts plaatsvindt. Eerder is al de meerwaarde van een samenwerkingsverband tussen de domeinen politiek, ethiek, recht en techniek aangekaart. Een dergelijk samenwerkingsverband waarbij ook de Belastingdienst als uitvoerende macht wordt betrokken, is waardevol voor de selectie van geschikte risicofactoren.

Het selecteren van een geschikte risicofactor is een lastige taak. Cruciaal hiervoor is primair het implementeren van de hiervoor genoemde methoden voor het minimaliseren van bias in de data. Secundair zou het geven van voorlichtingen en trainingen over biased risicofactoren aan experts uit de verschillende domeinen aan kunnen zetten tot nadenken over bias en hierdoor eveneens positief kunnen bijdragen aan de minimalisatie van bias. Van belang is hierbij het erkennen en bediscussiëren van vooroordelen. Erkenning en discussie kunnen bijdragen aan het minimaliseren van bias. In par. 5.1.2 is duidelijk geworden dat vooroordelen veelal zijn genormaliseerd in de samenleving en hierdoor vaak onbewust aanwezig zijn. Een eerste stap in het de-normaliseren van vooroordelen is het erkennen ervan. Dit kan gestimuleerd worden door een open dialoog aan te gaan en voorlichting te geven over veelvoorkomende (onbewuste) stereotypen en vooroordelen.

Door daarnaast als extra controlestap de vraag te stellen of de risicofactor (overduidelijk) tot een ongerechtvaardigde, ongelijke behandeling leidt, wordt een menselijke weging toegevoegd en bewustheid gecreëerd. Men kan er, mijns inziens, op vertrouwen dat het merendeel van de mensheid niet discriminerend is ingesteld. Wanneer zij zich tevens bewust zijn van de vooroordelen die aanwezig zijn in hun directe omgeving, dan zal het aannemen van een objectieve houding gemakkelijker zijn. Bij een meer diverse controlegroep zal de mate van non-discriminaliteit bovendien beter gewaarborgd zijn, omdat in iedere cultuur andere vooroordelen leven.

Divers ziet in dit geval op leeftijd, geslacht, levensovertuiging, geloofsovertuiging, ras, etniciteit, geslacht/sekse, nationaliteit, seksuele gerichtheid, handicap of chronische ziekte, politieke gezindheid, nationaliteit en burgerlijke staat. Idealiter is van iedere bevolkingsgroep minimaal één vertegenwoordiger, zodat de groep de gehele samenleving weerspiegelt. Zo is de kans het grootste dat aan de belangen van alle groepen is gedacht. Het realiseren van een zeer diverse controlegroep is lastiger dan het realiseren van een minder diverse controlegroep. Desalniettemin, zou een zeer diverse controlegroep, mijns inziens, wel het streven moeten zijn. Als een (zeer) diverse controlegroep van oordeel is dat de risicofactor niet leidt tot een ongerechtvaardigde,

ongelijke behandeling, dan zou, mijns inziens, gesteld kunnen worden dat de kans op een ongerechtvaardigde, ongelijke behandeling minimaal is.

De mate van non-discriminaliteit zal tevens beter gewaarborgd zijn als ook ethici een oordeel vellen over de te hanteren risicofactor. Zij kunnen vanuit hun expertise de mogelijke ethische gevolgen beter beoordelen dan programmeurs, zelfs al hebben zij hier een cursus voor gevolgd. Deze gedachte sluit aan bij de eerder benoemde visie van Zweistra en Poort om een samenwerking te creëren tussen de domeinen technologie, politiek, ethiek en recht. Zweistra en Poort bepleiten dat ethici en technici de nieuw ontwikkelde technologieën samen dienen 'te toetsen en uiteindelijk bekritiseren'.[16] Ik trek deze samenwerking door naar een verband waarbij ook de uitvoerders – de belastingambtenaren – samenwerken om tot een goede inbedding te komen van de nieuwe technologieën – in dit onderzoek de slimme opsporingstechnieken.

Naast ethische kennis is ook kennis uit het ICT-domein vereist. Nijssen en Stevens pleiten in dit verband voor een nauwe samenwerking tussen beleidsmakers, wetgevingsjuristen, proces- en ICT-ontwerpers en uitvoerders.[17] Experts uit deze disciplines zouden zich moeten verdiepen in elkaars vakgebied. Deze nauwe samenwerking draagt ook bij aan het minimaliseren van subjectieve of zelfs discriminerende risicofactoren.

Tot slot zou ook de politiek, met daaronder begrepen het burgerperspectief – in de zin dat burgers betrokken worden bij de ontwikkeling, toepassing en het gebruik van data en algoritmen – betrokken dienen te zijn bij de totstandkoming en selectie van risicofactoren. De totstandkoming van het recht is hoofdzakelijk gelegen in het politieke debat, zodoende zou ook bij de ontwikkeling van technologieën die invloed uitoefenen op het recht de politiek betrokken dienen te zijn.[18] Via het politieke debat kan het burgerperspectief meegewogen worden in de ontwikkeling van de risicofactoren en de slimme opsporingstechniek in zijn algemeenheid.

7.1.4 *Tussenconclusie: Een controlegroep voor controle vooraf*

In deze paragraaf is het belang van controle voor de inzet van de slimme opsporingstechnieken uiteengezet. Die controle dient voor een belangrijk deel te bestaan uit het toepassen van bias minimaliserende methoden.

Daarnaast dient de controlegroep risicofactoren te selecteren die passen binnen een rechtsstatelijke inzet van slimme opsporingstechnieken, oftewel risicofactoren die blijk geven van gebondenheid aan fundamentele, rechtsstatelijke beginselen en rechtsnormen die niet per definitie juridisch afdwingbaar zijn. Hierdoor draagt deze aanbeveling bij aan een rechtsstatelijke inzet van slimme opsporingstechnieken. De controlegroep voor controle vooraf dient een weerspiegeling te zijn van de gehele

16 Zweistra & Poort juni 2022, p. 464.
17 Nijssen & Stevens 19 september 2019, p. 1105.
18 Zweistra & Poort juni 2022, p. 463.

samenleving en dient derhalve zo veel mogelijk – het liefst alle – bevolkingsgroepen te vertegenwoordigen. Daarnaast dient de controlegroep experts uit verschillende domeinen te bevatten, te weten de politiek (door wie tevens het burgerperspectief behartigd dient te worden), de ICT, de ethiek, de wetgeving en de uitvoering. Een dergelijke controlegroep dient voor de inzet van de risicofactor na te gaan of de risicofactor 1) logischerwijs te koppelen is aan de regeling waarin dat risico zich voor kan doen, 2) een objectief karakter heeft en 3) niet (overduidelijk) tot een ongerechtvaardigde, ongelijke behandeling leidt. Door een dergelijke controle toe te passen vóór de inzet van de risicofactor wordt de kans op het intreden van ongerechtvaardigde, ongelijke behandeling een stuk kleiner. Met de gedachte 'voorkomen is beter dan genezen' zijn controlemechanismen aan de voorkant effectiever dan rechtsherstel achteraf. Bovendien, zal de inzet van deze vooraf gecontroleerde risicofactoren beter uit te leggen zijn, dan de inzet van niet-vooraf-gecontroleerde risicofactoren. Dit draagt bij aan transparantie als voorwaarde voor het afleggen van (democratische) verantwoording.

7.2 Big Data-analyse en zelflerende algoritmen als laatste slimme opsporingstechniek

In deze paragraaf staat de aanbeveling 'Big Data-analyse en zelflerende algoritmen als laatste middel met effectieve menselijke tussenkomst' centraal. Aanleiding voor deze aanbeveling is het in par. 5.3 behandelde risico op valse resultaten. In deze paragraaf zal nader toegelicht worden hoe dit risico gemitigeerd kan worden door middel van de hier gestelde aanbeveling. Daarna zal het belang van effectieve menselijke tussenkomst gespecificeerd worden.

7.2.1 *Het risico van de inzet van Big Data-analyse en zelflerende algoritme*

Bij Big Data-analyse wordt, zoals reeds is gesteld, gezocht naar nieuwe verbanden en die verbanden worden ook gevonden. Dat kunnen verbanden zijn die voor een mens niet logisch te beredeneren zijn en 'toevallig' zijn ontdekt, ofwel zonder de inzet van de slimme opsporingstechnieken niet gevonden zouden zijn. Denk bijvoorbeeld aan de situatie waarin bij de bouw van nieuwe steden het aantal geboortes toenam en eveneens het aantal ooievaren in de stad. Als deze data worden geanalyseerd kan het verband getrokken worden dat ooievaren baby's brengen (of andersom). Dat is natuurlijk niet correct, maar wel een verband dat uit de inputdata afgeleid kan worden. De inzet van risicofactoren die resulteren uit Big Data-analyse zou vanuit die gedachte zo veel mogelijk gemeden moeten worden. Dit is ook naar voren gekomen in par. 7.1.

Daarnaast is het risico op het intreden van discriminatie bij de inzet van zelflerende algoritmen groter, dan bij niet-zelflerende algoritmen. Zelflerende algoritmen verfijnen namelijk zelfstandig hun opsporingsbeleid. Hierdoor kan het algoritme uit zichzelf gaan discrimineren. Bij niet-zelflerende algoritmen dient de discriminatie, voor het intreden hiervan in het stappenplan verankerd te zijn, omdat zij hun opsporingsbeleid niet zelfstandig verfijnen.

Door de inzet van zelflerende algoritmen te beperken zou het risico op het intreden van discriminatie derhalve verkleind kunnen worden. Een andere manier om deze kans op het intreden van discriminatie te kunnen verkleinen, is om de evolutie van zelflerende algoritmen nauwlettend te analyseren.

Met nauwlettend bedoel ik in dit verband het frequent en nauwkeurig controleren van de verfijning van het algoritme; 'vertoont het algoritme nog steeds geen signalen van discriminatie?' Dit is een taak die uitgevoerd dient te worden door een groep experts uit de verschillende domeinen, politiek, ethiek, techniek en recht. De frequentie waarmee die nauwkeurige controle plaats dient te vinden, hangt af van de snelheid waarmee het zelflerend algoritme zichzelf verfijnt. Deze snelheid zal per algoritme verschillen. Zodoende kan frequent niet in het algemeen geconcretiseerd worden, maar dient dit op het algoritme dat ingezet wordt, afgestemd te worden. Een nadeel van deze nauwlettende controle is dat het capaciteit (zowel in mankracht als in tijd) kost. Gelissen geeft aan dat ook de overheidsinstanties de druk ervaren 'dat processen allemaal sneller en goedkoper moeten worden'.[19] Volgens hem kan het automatiseren van beslissingen daarvoor een oplossing zijn, mits het systeem niet-zelflerend is. Het beslissingssysteem is dan beter te controleren, omdat het algoritme de geprogrammeerde stappen volgt en deze niet zelf verder ontwikkelt.

In dat geval is sprake van een glass box in plaats van een black box, omdat het algoritme de stappen volgt zoals die zijn geprogrammeerd en deze stappen bekend zijn, althans te achterhalen zijn.[20] Hierdoor kunnen de stappen die ten grondslag liggen aan de beslissing van het algoritme gecontroleerd worden en is sprake van inhoudelijke transparantie. Evenzo dient inhoudelijke transparantie te gelden voor niet-algoritmische informatie. Bij niet-algoritmische informatie zal de inhoudelijke transparantie gemakkelijker te behalen zijn, doordat niet-algoritmische informatie veelal minder complex is. Binnen algoritmische informatie zal inhoudelijke transparantie van niet-zelflerende algoritmen gemakkelijker te behalen zijn dan inhoudelijke transparantie van zelflerende algoritmen.

Desalniettemin dient ook zorgvuldig omgegaan te worden met de inzet van niet-zelflerende algoritmen. Want, zoals Dusarduijn stelt, kunnen 'algoritmes geen rekening houden met context die *niet* wordt aangeleverd. In het (fiscale) recht kan dat problemen gegeven (cursivering door auteur)'.[21] Het recht is niet rechtlijnig of staccato, maar in sommige gevallen krom en in ieder geval niet gemakkelijk te vatten in

19 Gelissen 9 februari 2021.

20 Sommige particuliere programmeurs geven hun programmering niet vrij. In die gevallen zijn de stappen niet bekend. Echter, zij kunnen wel achterhaald worden, omdat zij door een mens zijn geprogrammeerd. De rechter kan de programmeur dan bijvoorbeeld gebieden om het geprogrammeerde stappenplan vrij te geven.

21 Dusarduijn maart 2019, p. 119.

mathematische formules[22], dat geldt ook voor het fiscale recht. Van Eck concludeert hieruit 'een groot verschil tussen het recht zoals men dat zou willen beoefenen, en de vorm waarin het recht in computertaal en dus in de vorm van het blind toepassen van regels leidt tot besluiten in individuele gevallen'.[23] Volgens Van Eck wordt – althans werd op het moment van schrijven van haar proefschrift – geen rekening gehouden met deze constateringen bij de ontwikkeling van beslisregels in automatische afhandelingssystemen.

Momenteel lijkt hier bij het ontwerp van selectieregels ook onvoldoende aandacht aan gegeven te worden. Selectieregels pogen het recht te vervatten in mathematische 'als dit, dan dat'- formules, hetgeen nu juist haaks lijkt te staan op wat de uitvoering van de fiscale wetgeving behelst.[24] Van Eck draagt het inbouwen van zijpaden in het systeem als oplossing aan voor het gebrek aan het mathematische karakter van de fiscale wetsuitvoering. Het inbouwen van zijpaden leidt tot meer flexibiliteit in het ontwerp van de algoritmen. Als dit wordt gecombineerd met (meer) aandacht en tijd in de uitvoering voor uitzonderingsgevallen, dan kan de asymmetrie tussen hoe men zou willen dat het recht beoefend wordt en hoe het daadwerkelijk beoefend wordt, verkleind worden.[25] Bij het flexibele ontwerp van de slimme opsporingstechnieken dient tevens terugwerkende kracht mogelijk gemaakt te worden.[26]

Gelissen erkent eveneens dat niet alle gevallen die gecontroleerd dienen te worden, zullen vallen 'binnen de parameters van de geautomatiseerde beslissing'.[27] Hetzelfde geldt voor selectieregels. Volgens Gelissen is voor deze onduidelijke gevallen die niet passen binnen de gestelde parameters, een menselijke maat vereist. De menselijke maat vereist dat in uitzonderingsgevallen afgeweken kan worden van de geautomatiseerde beslissing, ofwel van de uitkomst van de slimme opsporingstechniek. Bij selectieregels is ook van belang dat afgeweken kan worden van het door de selectieregel geselecteerde risico. Om dat gegrond te kunnen doen, is het noodzakelijk om de selectieregel te kunnen doorgronden en te weten waarop de selectie is gebaseerd. Dit vereist transparantie.

Nota bene, wanneer slimme opsporingstechnieken op de juiste wijze zijn getraind en wanneer de bias verminderende technieken die zijn genoemd in par. 7.1.2 worden gehanteerd, dan zullen minder gevallen nopen voor afwijking van de beslissing of de uitkomst van de slimme opsporingstechniek. Desondanks, is het bestaan van uitzonderingen inherent aan de gebruikte techniek. Zoals is aangeven, zullen uit het analyseren van data altijd verbanden worden getrokken, hierdoor zullen

22 Gribnau spreekt over 'geen kwestie van eenvoudige subsumptie' en 'geen mathematische bezigheid', p. 62 van J.L.M. Gribnau, 'Heeft de Belastingdienst zijn governance op orde?', in: B. Starink & M. Visser (red.) *Ondernemend met pensioen* (Dietvorst-bundel), Deventer: Wolters Kluwer 2015, p. 55-70.
23 Van Eck 2018, p. 435.
24 Aldus Gribnau, in: *Ondernemend met pensioen* 2015, p. 62.
25 Van Eck 2018, p. 435.
26 Van Eck 2018, p. 435.
27 Gelissen 9 februari 2021.

uitzonderingsgevallen altijd blijven ontstaan. Ongeacht de minimalisatie van bias in de (trainings)data.

7.2.2 *Tussenconclusie: Big Data-analyse en zelflerende algoritmen als laatste slimme opsporingstechniek*

Uit het bovenstaande kan geconcludeerd worden dat het gebruik van Big Data-analyse en zelflerende algoritmen zoveel mogelijk beperkt dient te worden, omdat hiermee de kans op het intreden van discriminatie wordt verkleind. Als wordt gekozen voor de inzet van deze technieken, dan is het gebruik van bias minimalisatie methoden cruciaal. Daarnaast dient bij de ontwikkeling van de techniek ruimte voor flexibiliteit ingebouwd te worden. In uitzonderingsgevallen moet afwijken mogelijk zijn. Tevens dient ruimte geboden te worden voor terugwerkende kracht. Door het minimaliseren van de inzet van deze twee technieken zullen fundamentele, rechtsstatelijke beginselen en rechtsnormen die niet per definitie juridisch afdwingbaar zijn beter gewaarborgd zijn. Verder dragen de ruimte voor afwijkingen in uitzonderingsgevallen en terugwerkende kracht ook bij aan een rechtsstatelijke inzet van slimme opsporingstechnieken.

7.3 Verplichte, openbaar toegankelijke documentatie

In deze paragraaf zal de aanbeveling 'verplichte, openbaar toegankelijke documentatie' toegelicht worden. De drijfveer voor deze aanbeveling is het realiseren van transparantie, met name procedurele transparantie en transparantie als voorwaarde voor (democratische) verantwoording[28].

Het nut van openbaar toegankelijk documenten is (ook) gebleken uit de geraadpleegde kaders. Openbaar toegankelijk wil zeggen dat de documentatie gemakkelijk raadpleegbaar is voor de *stakeholders* van de belastingadministratie. Het houdt ook in dat de documentatie toegankelijk is voor een breed publiek. Bijvoorbeeld door de documentatie te publiceren op de website van de belastingadministratie. De gemiddelde belastingplichtige dient in staat te zijn om de documentatie te vinden en vervolgens te begrijpen. Hiervoor is relatief simpele taal vereist. Gezien de complexiteit van de slimme opsporingstechnieken, kan het lastig zijn om hier simpele taal voor te gebruiken. Als oplossing hiervoor kan gedacht worden aan het online publiceren van een simpele en verkorte versie van de documentatie. Deze simpele samenvatting dient dan naast de uitgebreide en gedetailleerde documentatie beschikbaar te worden gesteld. Hierbij dient evenwel in ogenschouw genomen te worden dat meer transparantie kan ook leiden tot meer vragen, wat juist afbreuk zou kunnen doen aan het vertrouwen (de transparantie-paradox; zie par. 1.2.3).[29] Vervolgonderzoek naar de complexe relatie tussen transparantie en vertrouwen kan bijdragen aan

28 Ik heb hier transparantie als voorwaarde voor (democratische) verantwoording samengevat tot de term verantwoordingstransparantie.

29 Gribnau 2016.

het nemen van een juiste beslissing over de wijze van publicatie (met name over de vraag of die publicatie volledig, beperkt of beide dient te zijn).

De opbouw van deze paragraaf is als volgt: eerst zal stilgestaan worden bij de aspecten die de openbaar toegankelijke documentatie mijns inziens dient te bevatten, daarna zal stilgestaan worden bij de vraag welke experts mijns inziens betrokken dienen te zijn bij de ontwikkeling van deze documentatieverplichting en wie vervolgens betrokken dienen te zijn bij de documentatie zelf.

7.3.1 *De inhoud van de verplichte, openbaar toegankelijke documentatie*

Verplicht, openbaar toegankelijke documentatie is denkbaar voor belastingadministraties ten aanzien van het gebruik van slimme opsporingstechnieken. In deze documentatieverplichting zouden de aanwijzingen uit de verschillende richtlijnen voor de vastlegging terug moeten komen. De verplichte, openbaar toegankelijke documentatie zou sterk gebaseerd kunnen zijn op de suggesties die worden gegeven in de whitepaper van het Algoritmeregister van de stad Amsterdam.

De openbaar, toegankelijke documentatie zou mijns inziens uit een abstract en vier inhoudelijke hoofstukken moeten bestaan.[30] Hierna zal voor het abstract en elk hoofdstuk aangeven worden welke onderdelen zij dienen te bevatten. Daarbij wordt ook aangegeven welke vormen van transparantie hiermee worden gediend.

Een abstract met daarin:
- het doel van de inzet van de slimme opsporingstechnieken *(procedurele en verantwoordingstransparantie)*;
- de wijze waarop de slimme opsporingstechnieken (globaal) werken en in welke gevallen ze worden ingezet *(inhoudelijke, procedurele en verantwoordingstransparantie)*;
- welke belastingplichtigen beïnvloed worden door de inzet en op welke wijze *(uitkomst, procedurele en verantwoordingstransparantie)*; en
- waarom gekozen is voor de inzet van de slimme opsporingstechniek en de noodzaak van de inzet *(procedurele en verantwoordingstransparantie).*

Een hoofdstuk over de ontwikkeling en het implementatieproces van de slimme opsporingstechnieken, waarin wordt besproken:
- welke data zijn gebruikt voor het trainen en ontwikkelen van de slimme opsporingstechnieken en op welke wijze die data zijn verzameld *(input-, inhoudelijke en verantwoordingstransparantie)*;
- de wijze waarop is gewaarborgd dat de gebruikte data zo min mogelijk vooroordelen bevat en zo divers mogelijk is *(procedurele, verantwoordingstransparantie en transparantie van fundamentele (rechts)beginselen)*;

30 Vertoont grote overeenkomsten met de aanbevelingen uit de whitepaper van het Algoritmeregister van de stad Amsterdam, Haataja, Van de Fliert & Rautio, september 2020.

- de wijze waarop de implementatie van de slimme opsporingstechnieken plaatsvindt *(procedurele en verantwoordingstransparantie)*;
- wie betrokken is geweest bij de implementatie (idealiter zijn ook belastingplichtigen via een adviesraad betrokken geweest bij de implementatie, om het burgerperspectief te kunnen waarborgen) *(procedurele en verantwoordingstransparantie)*; en
- wie gebruikmaken van de slimme opsporingstechnieken (welke ambtenaren) en de wijze waarop de slimme opsporingstechnieken hen helpen bij de uitvoering van hun werkzaamheden *(procedurele en verantwoordingstransparantie)*.

Een hoofdstuk over de risico's van (de inzet van) slimme opsporingstechnieken, waarin het volgende wordt besproken:
- de kans op het intreden van risico's bij implementatie *(procedurele, verantwoordingstransparantie en transparantie van fundamentele (rechts)beginselen)*;
- de wijze waarop de kans op het intreden van risico's tijdens het gebruik van de slimme opsporingstechnieken wordt geminimaliseerd *(procedurele, verantwoordingstransparantie en transparantie van fundamentele (rechts)beginselen)*;
- welke risico's zich voordoen en op welke wijze zij zich verhouden tot de voordelen van de inzet van de slimme opsporingstechnieken *(procedurele, verantwoordingstransparantie en transparantie van fundamentele (rechts)beginselen)*; en
- de wijze waarop rechten worden beschermd *(procedurele, verantwoordingstransparantie en transparantie van fundamentele (rechts)beginselen)*.

Een hoofdstuk over de verantwoordelijkheid van de inzet van de slimme opsporingstechnieken, waarin wordt besproken:
- wie waarom verantwoordelijk is indien risico's toch intreden en hoe zij verantwoordelijk gesteld kunnen worden *(procedurele en verantwoordingstransparantie)*; en
- welke externe partijen (bijv. softwareleveranciers) betrokken zijn *(procedurele en verantwoordingstransparantie)*.

Een hoofdstuk over de evaluatie van de inzet van de slimme opsporingstechnieken, waarin wordt besproken:
- de wijze waarop de werkzaamheid van de slimme opsporingstechnieken wordt geëvalueerd *(procedurele en verantwoordingstransparantie)*;
- de frequentie waarmee evaluatie plaatsvindt *(procedurele en verantwoordingstransparantie)*;
- wie betrokken is bij de evaluatie en waarom *(procedurele en verantwoordingstransparantie)*; en
- de wijze waarop belastingplichtigen (voor zover mogelijk) betrokken worden bij de evaluatie *(procedurele en verantwoordingstransparantie)*.

Kort gezegd ben ik van mening dat de verplichte, openbaar toegankelijke documentatie de volgende aspecten dient te bevatten: een abstract en informatie over 1) de ontwikkeling en het implementatieproces van de slimme opsporingstechnieken, 2) de risico's van (de inzet van) slimme opsporingstechnieken, 3) de verantwoordelijkheid

van de inzet van de slimme opsporingstechnieken en 4) de evaluatie van de inzet van de slimme opsporingstechnieken.

7.3.2 *Wie dient betrokken te zijn bij de ontwikkeling van de documentatieverplichting en de documentatie zelf?*

Voor de ontwikkeling en de exacte invulling van een gestandaardiseerde documentatieverplichting zou mijns inziens consultatie plaats moeten vinden met experts uit verschillende domeinen die een rol spelen bij de inzet van de slimme opsporingstechnieken. Ik denk hierbij aan de al in par. 7.1 benoemde domeinen (de politiek (door wie tevens het burgerperspectief behartigd dient te worden), de ICT, de ethiek, de wetgeving en de uitvoering). Per domein zal ik kort toelichten waarom ik consultatie vanuit dit domein wenselijk acht.

Bij de ontwikkeling van de documentatieverplichting en de documentatie zelf geldt wederom het uitgangspunt dat het recht gevormd wordt door het politieke debat, derhalve is ook hier politieke begeleiding, waarbij oog is voor het burgerperspectief, wenselijk. Daarbij dienen ook de Nationale ombudsman en de burger zelf benaderd te worden. Zij zijn immers de uitgelezen personen om het burgerperspectief te vertegenwoordigen en aan te geven op welke wijze zij menen dat dit terug dient te komen in documentatie. Uit de ICT zouden data-analisten, computerwetenschappers, programmeurs en experts op het gebied van algoritmen geraadpleegd kunnen worden. Zij kunnen vertellen op welke wijze de technieken werken en hoe dit gedocumenteerd zou kunnen worden. Ethici kunnen een rol spelen bij het vastleggen van keuzes en afwegingen op het gebied van ethiek door aan te geven wat gedocumenteerd dient te zijn om de waarborg van ethiek (achteraf) te kunnen controleren.

Ook rechters, juristen en advocaten (gespecialiseerd op het gebied van automatische besluitvorming en de inzet van slimme opsporingstechnieken) kunnen hier een rol vervullen door aan te geven hoe verplichte, openbaar toegankelijke documentatie vooraf kan bijdragen aan het bieden van rechtsherstel achteraf. Een belangrijke vraag hierbij luidt als volgt: 'Is de rechter (en de belanghebbende) in staat om te achterhalen op welke wijze tot een beslissing is gekomen en op welke wijze bewijs is verzameld?' Daarnaast zouden ook adviezen van non-discriminatieorganisaties in ogenschouw genomen kunnen worden. Voorts dienen vanuit het wetgevingsdomein experts op het gebied van documentatieverplichtingen geconsulteerd te worden om te zorgen dat de documentatieverplichting eenduidig is, gemakkelijk te gebruiken en zijn doel dient.

Tot slot kunnen uit het uitvoeringsdomein – in dit onderzoek de belastingadministratie – belastingambtenaren die gebruikmaken van de inzet van slimme opsporingstechnieken geconsulteerd worden. De belastingambtenaren kunnen adviezen geven over de wijze waarop de slimme opsporingstechnieken in de praktijk worden ingezet en meedenken over vragen en aanwijzingen die richting dienen te geven aan de documentatie hieromtrent.

De in par. 7.1 voorgestelde controlegroep kan zorgdragen voor deze documentatie. Hiermee zijn de verschillende domeinen ook bij de vastlegging betrokken.

7.3.3 *Tussenconclusie: verplichte, openbaar toegankelijke documentatie*

Verplichte, openbaar toegankelijke documentatie draagt bij aan transparantie, met name procedurele en verantwoordingstransparantie. De verplichte openbare documentatie maakt tevens een controle op de gebondenheid aan fundamentele, rechtsstatelijke beginselen en (niet-juridische afdwingbare) rechtsnormen van (de inzet van) slimme opsporingstechnieken mogelijk. Naar mijn mening dient de verplichte, openbaar toegankelijke documentatie de volgende aspecten te bevatten: een abstract en informatie over 1) de ontwikkeling en het implementatieproces van de slimme opsporingstechnieken, 2) de risico's van (de inzet van) slimme opsporingstechnieken, 3) de verantwoordelijkheid van de inzet van de slimme opsporingstechnieken en 4) de evaluatie van de inzet van de slimme opsporingstechnieken. Voor de exacte invulling en de ontwikkeling van de verplichte, openbaar toegankelijke documentatie dient mijns inziens consultatie plaats te vinden met experts uit verschillende domeinen, te weten de politiek (door wie tevens het burgerperspectief behartigd dient te worden), de ICT, de ethiek en de wetgevende en uitvoerende macht.

7.4 Een gespecialiseerd toezichthoudend orgaan voor de controle op de inzet van de slimme opsporingstechnieken

Volgens de trias politica voert de rechterlijke macht controle uit op de uitvoerende en de wetgevende macht, via individuele geschilbeslechting. Voor de inzet van de slimme opsporingstechnieken is het raadzaam om naast deze controle toezicht uit te laten voeren door een gespecialiseerd orgaan. In deze paragraaf zal uitgelegd worden waarom dit raadzaam is en nuttig kan zijn.

7.4.1 *Een gespecialiseerd toezichthoudend orgaan ondersteunend aan de rechterlijke macht*

De controle door het toezichthoudend orgaan zal plaatsvinden tijdens de inzet van de slimme opsporingstechnieken en niet pas achteraf, als het al is misgegaan en rechtsherstel geboden dient te worden. Het onafhankelijk orgaan zou deskundig moeten zijn 'in het programmeren van wetteksten', aldus van Eck.[31, 32]

Van Eck ziet meerwaarde in een dergelijk orgaan voor de controle op de beslisregels, omdat de rechter dan op het oordeel van dat orgaan zou moeten kunnen vertrouwen gelet op het deskundigheidsniveau. Dit zorgt ervoor dat de rechter niet meer in alle

31 Van Eck 2018, p. 434 en 435.

32 Het programmeren van de wetteksten kan gekoppeld worden aan de in par. 7.1 besproken stellingname van Nijssen en Stevens dat selectie- en beslisregels te herleiden dienen te zijn tot de wettekst.

gevallen de beslisregel hoeft te controleren. Ten aanzien van de controle op de inzet van de slimme opsporingstechnieken kan dit mijns inziens eveneens zinvol zijn.

Het gespecialiseerde orgaan dient de inzet van de slimme opsporingstechnieken met een technisch inhoudelijke visie te beoordelen. Het orgaan vormt een verlengstuk van de controlegroep voor controle vooraf. Samenwerking en kenniswisseling tussen de verschillende domeinen blijft het uitgangspunt. Een extra controle door een gespecialiseerd orgaan kan zorgen voor een frisse blik en mogelijk ook voor een beoordeling vanuit een andere invalshoek op de inzet van de slimme opsporingstechnieken waardoor andere (potentiële) risico's gedetecteerd kunnen worden.

Het gespecialiseerde orgaan kan voor de controle gebruikmaken van de verplichte, openbaar toegankelijke documentatie zoals is bedoeld in par. 7.3. Daarnaast zou het ook toegang kunnen krijgen tot het platform met open source data dat is genoemd in par. 6.3.2.

Met deze informatie zou het orgaan in staat moeten zijn om te toetsen of de beslis- en selectieregels juist zijn geïmplementeerd, ofwel of de wettekst juist is geprogrammeerd. De uitkomst van deze toets kan vervolgens gebruikt worden door de rechter voor zijn oordeel of rechtsherstel geboden dient te worden en op welke wijze.

Daarnaast zou het orgaan de uitkomst gedurende de inzet van de slimme opsporingstechnieken – nog voordat het mis is gegaan – kunnen delen met de belastingadministraties. In samenwerking kan dan gezocht worden naar een oplossing om eventueel geconstateerde risico's (in het vervolg) te mitigeren.

Aanvullend onderzoek is nodig om te onderzoeken of het wenselijk is dat dit orgaan onafhankelijk is of onderdeel uit dient te maken van de belastingadministratie zelf.

7.4.2 *Tussenconclusie: een gespecialiseerd toezichthoudend orgaan voor de controle op de inzet van de slimme opsporingstechnieken*

In deze paragraaf stond de aanbeveling 'een gespecialiseerd toezichthoudend orgaan voor de controle op de inzet van de slimme opsporingstechnieken' centraal. Deze aanbeveling draagt bij aan rechtsstatelijke slimme opsporingstechnieken doordat de aanbeveling pleit voor controle op de gebondenheid aan fundamentele, rechtsstatelijke beginselen en (niet-juridisch afdwingbare) rechtsnormen. Het orgaan zou een ondersteuning kunnen vormen op de rechterlijke macht, door de beslis- en selectieregels te toetsen. Dit is nuttig omdat de rechter dan niet in iedere situatie de beslis- en selectieregels zelf hoeft te toetsen. De uitkomst van deze toets zou gedurende de inzet van de slimme opsporingstechnieken overlegd kunnen worden aan de Belastingdienst, zodat zij tijdig samen kunnen werken aan een oplossing. Om te bepalen of dit orgaan onafhankelijk dient te zijn of onderdeel uit dient te maken van de belastingadministratie zelf is aanvullend onderzoek vereist.

7.5 Sancties bij overtreding?

Het uitgangspunt van de hiervoor gestelde aanbevelingen is samenwerking, voorkomen is beter dan genezen, signalering en tijdig ingrijpen waar nodig. Als toch complicaties optreden en blijkt dat de Belastingdienst zich niet houdt aan de gestelde aanbevelingen, dan zal hij allereerst gewaarschuwd worden door het gespecialiseerde toezichthoudende orgaan en zal alsnog gezamenlijk worden gewerkt aan een verbetering van de situatie. Toezicht wordt krachtiger als sancties bij (voortdurende) overtreding opgelegd kunnen worden. Sancties stimuleren het idee van gebonden zijn aan fundamentele, rechtsstatelijke beginselen en rechtsnormen die niet per definitie juridisch afdwingbaar zijn. In het geval van de Belastingdienst is het opleggen van sancties lastig, omdat het een publiek orgaan betreft dat met publieke middelen bekostigd wordt. Hoewel in het voorjaar van 2022 door de Autoriteit Persoonsgegevens een boete is opgelegd aan de Belastingdienst van 3,7 miljoen euro[33], acht ik een geldelijke sanctie voor een publiek orgaan, zoals de Belastingdienst, niet wenselijk. Het is uiteindelijk de burger die de boete betaalt, zo zal het in ieder geval voelen voor velen.

Een sanctie in de vorm van een gevangenisstraf of taakstraf is ook niet denkbaar bij een publiek orgaan. Derhalve dient gezocht te worden naar een ander niet-geldelijk punitief element.

7.5.1 *Een niet-geldelijke sanctie?*

In deze paragraaf zullen alternatieven voor een geldelijke sanctie aangehaald worden.

Gedacht kan worden aan het nietig verklaren van uitkomsten (bijvoorbeeld een gecorrigeerde aangifte) van slimme opsporingstechnieken wanneer blijkt dat zij onrechtmatig zijn (gebruikt). Het is echter lastig te bepalen in hoeverre de correctie een gevolg is van het onrechtmatig gebruik van de slimme opsporingstechnieken en met name of dit gevolg niet ingetreden zou zijn zonder het onrechtmatige gebruik. Echter, als evident blijkt dat bepaalde rechtsbeginselen zijn geschonden en een controle bijvoorbeeld discriminerend is, dan zou bepleit kunnen worden dat de gevolgen van die controle juist wel in algemene zin ongeldig verklaard dienen te worden. Oftewel, dat een naheffingsaanslag of boete die is opgelegd als gevolg van een onrechtmatig gebruik van slimme opsporingstechnieken, vernietigd zou moeten worden.

Het opleggen van deze sanctie dient desalniettemin vooral van geval tot geval nauwkeurig beoordeeld te worden. Dit is een taak die is weggelegd voor de rechter. Het opleggen van deze sanctie met een preventief doel is hierdoor minder geschikt, omdat de rechter pas een sanctie uitdeelt als het is misgegaan. Een ander nadeel van deze sanctie is dat het geen generieke, maar een individuele sanctie betreft. Ook

33 Zie in dit verband Autoriteit persoonsgegevens 'Boete Belastingdienst voor zwarte lijst FSV' persbericht van 12 april 2022, raadpleegbaar via autoriteitpersoonsgegevens.nl/nl/nieuws/boete-belastingdienst-voor-zwarte-lijst-fsv.

hierdoor werkt het minder preventief. Voor de (verdere) inrichting van deze sanctie dient bovendien onderzoek verricht te worden naar het leerstuk van onrechtmatig verkregen bewijs. Helaas is hier in dit onderzoek geen ruimte meer voor.

Verder kan voorzichtig gedacht worden aan een sanctie in de vorm van publiekelijk leed. In Nederland is veel ophef over de Belastingdienst, omdat de inzet van hun slimme opsporingstechnieken niet voldeed aan belangrijke waarborgen en een discriminerend resultaat had. Hoewel negatieve publiciteit via de media erg vervelend is, kan het ook leiden tot een incentive om de situatie te verbeteren. In dit kader is het interessant om nader onderzoek te verrichten naar het leerstuk van *naming and shaming*.

7.5.2 *Tussenconclusie: sancties bij overtreding?*

Het blijft lastig om een geschikte sanctie te bedenken voor een publiek orgaan zoals de Belastingdienst. Sancties zullen het idee van gebondenheid aan fundamentele, rechtsstatelijke beginselen en (niet-juridisch afdwingbare) rechtsnormen wel versterken. Verder onderzoek naar effectieve sancties voor de Belastingdienst is derhalve wenselijk.

7.6 Tussenconclusie: Aanbevelingen voor een rechtsstatelijk gebruik van slimme opsporingstechnieken

In dit hoofdstuk zijn aanbevelingen gedaan voor een rechtsstatelijke inzet van slimme opsporingstechnieken door de Belastingdienst. Uitgangspunt is om in een zo vroeg mogelijk stadium gebondenheid aan fundamentele, rechtsstatelijke beginselen en (niet-juridisch afdwingbare) rechtsnormen te bewerkstelligen. Een belangrijk mechanisme hiervoor zijn bias minimaliserende methoden. Aanvullend kan gebruikgemaakt worden van een zo divers mogelijk samengestelde controlegroep. Deze groep, bestaande uit experts uit verschillende disciplines, dient controle uit te oefenen op de inzet van de slimme opsporingstechnieken. Bij de inzet daarvan zou het gebruik van Big Data-analyse en zelflerende algoritmen zo veel mogelijk beperkt moeten worden, omdat de risico's daar het grootste zijn. Ten behoeve van transparantie zou openbaar toegankelijke documentatie verplicht gesteld kunnen worden. Daarnaast is het raadzaam om een gespecialiseerd orgaan aan te stellen om de rechter te ondersteunen bij de beoordeling van de inzet van slimme opsporingstechnieken. Tevens kan dit orgaan de spreekwoordelijke vinger aan de pols houden en de belastingadministratie zodoende tijdig informeren als het gebreken heeft geconstateerd. Samen kan dan gezocht worden naar een oplossing. Uitgangspunt van de aanbevelingen is samenwerking tussen de domeinen politiek (door wie tevens het burgerperspectief behartigd dient te worden), ICT, ethiek, wetgeving en uitvoering. Tot slot is nagedacht over de mogelijkheid om sancties op te leggen bij het niet naleven van de gestelde aanbevelingen. Doel van deze sancties is de (idee van) gebondenheid aan fundamentele, rechtsstatelijke beginselen en rechtsnormen die niet per definitie juridisch afdwingbaar, zoals de hier geformuleerde aanbevelingen, te versterken. Geconcludeerd is dat voor het kunnen bepalen van de meerwaarde van en de mogelijkheden tot het opleggen van sancties nader onderzoek vereist is.

8 Conclusie

In dit onderzoek is gezocht naar aanbevelingen voor een rechtsstatelijke inzet van slimme opsporingstechnieken door de Nederlandse Belastingdienst. De vraag 'Hoe kan de rechtsstatelijke inzet van algoritmen, Big Data-analyse en profiling door de Nederlandse Belastingdienst gewaarborgd worden?' stond centraal. Om tot een beantwoording van die vraag te komen zijn een zestal deelvragen beantwoord.

Bij de eerste deelvraag is onderzocht wat algoritmen, Big Data-analyse en profiling zijn. Een algoritme is een eindige reeks opeenvolgende instructies. Tussen niet-zelflerende en zelflerende algoritmen is een onderscheid gemaakt. De eerste soort volgt een vooraf gegeven, vastgestelde set aan instructies op via een 'als dit, dan dat' structuur en de tweede soort verfijnt zichzelf, door telkens een analyse te maken van de inputdata en hierop de set aan de te volgen instructies aan te passen. Vervolgens is het concept Big Data-analyse onderzocht. Geconstateerd is dat tal van definities van Big Data, onderdeel van Big Data-analyse, in omloop zijn. In dit onderzoek is gekozen voor een praktische definitie van Big Data en zo ook van Big Data-analyse. De gekozen definitie luidt als volgt: Big Data-analyse is het zoeken naar clusters, regelmatigheden of patronen in enorme hoeveelheden, verschillende data die vrijwel altijd constant en actueel zijn. Met deze resultaten kunnen profielen opgesteld worden. Profileren is een ander woord voor karakteriseren. Karakteristieken spelen daarom een rol bij profielen. Als profielen opgesteld worden met resultaten van Big Data-analyses, dan is profileren het voorspellen van de kans dat iets zich voordoet bij de aanwezigheid van bepaalde verbanden en/of patronen die zijn aangetroffen in vergelijkbare situaties uit het verleden. Daarbij wordt niets gezegd over waarom die kans zich voordoet. Belastingadministraties kunnen gebruikmaken van profielen om bijvoorbeeld de kans op een fout in de aangifte te voorspellen. Deze drie technieken (algoritmen, Big Data-analyse en profiling) zijn gebundeld onder de term 'slimme opsporingstechnieken'.

De tweede deelvraag spitste zich toe op het gebruik van slimme opsporingstechnieken door de Nederlandse Belastingdienst. Geconcludeerd is dat de Belastingdienst hier al geruime tijd gebruik van maakt en dat richt zich vooral op risicoselectie door gebruik te maken van een risicomatrix. De risicomatrix combineert de uitkomsten van selectieregels en risicomodellen. Niet-gladde gevallen worden via triaging uitgeworpen. Een uitworp is een advies voor handmatige controle door een inspecteur. Op de website van de Belastingdienst is relatief gemakkelijk informatie te vinden over de inzet van de slimme opsporingstechnieken.

Na deze verkenning is voor de beantwoording van de derde deelvraag het begrip transparantie in relatie tot het gebruik van de slimme opsporingstechnieken onderzocht. Daarbij is aandacht besteed aan het fenomeen *opening up the black box*, wat inhoudt dat de door de slimme opsporingstechniek genomen stappen en de gebruikte data inzichtelijk en te doorgronden dienen te zijn. Vier verschillende vormen van transparantie, welke alle dienen te gelden jegens de programmeur, de inspecteur, de belastingplichtige, de rechter en de wetgever, zijn geïdentificeerd. De eerste vorm is inhoudelijke transparantie welke uiteenvalt in inputtransparantie (welke data worden gebruikt?), outputtransparantie (wat is de uitkomst of de beslissing?) en transparantie van de stappen die doorlopen worden om tot de output te komen. De tweede vorm van transparantie is procedurele transparantie welke inzicht dient te geven in de keuzes en afspraken over (de inzet van) de slimme opsporingstechnieken.

Als derde vorm is transparantie over de wijze waarop fundamentele rechten bij de inzet van slimme opsporingstechnieken worden gewaarborgd, onderkend. Tot slot is als vierde vorm transparantie als voorwaarde voor het afleggen van (democratische) verantwoording erkend.

Deze laatste vorm van transparantie maakt het mogelijk om te controleren of de Nederlandse Belastingdienst zorg draagt voor een rechtsstatelijke inzet van de slimme opsporingstechnieken door zich (onder meer) te committeren aan de in dit onderzoek geformuleerde aanbevelingen. Tevens dient deze vorm van transparantie te zorgen voor een gevoel van gebondenheid aan meer dan slechts geldende wet- en regelgeving. Om hier zorg voor te kunnen dragen dient verantwoording afgelegd te kunnen worden en daarvoor is transparantie een voorwaarde.

Transparantie als voorwaarde voor het (afleggen van) (democratische) verantwoording kan daarnaast bijdragen aan het mitigeren van risico's die kleven aan de inzet van de slimme opsporingstechnieken. Met de beantwoording van de vijfde deelvraag is het belang van transparantie verder inzichtelijk geworden. Om dit belang beter inzichtelijk te maken is gezocht naar belemmeringen en risico's van slimme opsporingstechnieken. Het erkennen hiervan is een goede eerste stap in de richting van een rechtsstatelijke inzet van slimme opsporingstechnieken. Door het (er)kennen van de risico's kunnen zij immers (gerichter) voorkomen worden. Allereerst is transparantie dus vereist voor het kunnen herkennen van de wijze waarop onrechtstatelijkheid van de slimme opsporingstechnieken ontstaat. Ten tweede is transparantie noodzakelijk voor rechtsbescherming in klassieke zin, ofwel voor het kunnen aanvechten van een beslissing. Hiervoor is inzicht in de genomen stappen (die aan de beslissing ten grondslag liggen) vereist. Transparantie is ten derde vereist om een eventuele discriminerende werking van de inzet van slimme opsporingstechnieken te kunnen achterhalen en zelfs te voorkomen. Ten vierde kan transparantie bijdragen aan het opheffen van het *selffulfilling prophecy* effect, het vinden van een gedegen theoretische grondslag van geconstateerde verbanden, het erkennen van foutmarges in de trainingsdata en het actueel en zo veel mogelijk accuraat houden van de gebruikte risicoprofielen.

De zesde deelvraag was gericht op het analyseren van bestaande richtinggevende kaders op het gebied van (transparantie van) het gebruik van algoritmen, Big Data-analyse en profiling voor de Nederlandse Belastingdienst. Meerdere richtinggevende kaders zijn al ontwikkeld, zij het niet specifiek voor de Belastingdienst, maar voor overheidsinstanties in het algemeen. Geanalyseerd zijn het Toetsingskader van de Algemene Rekenkamer, richtlijnen voor het toepassen van algoritmen door overheden en publieksvoorlichting over data-analyses, de Toolbox Ethisch Verantwoord Innoveren en de visie van de Nationale ombudsman. Daarnaast is ook het Algoritmeregister van de stad Amsterdam als good practice geanalyseerd. Voor de beantwoording van de laatste deelvraag is inspiratie ontleend aan deze kaders en good practice.

In dit onderzoek zijn vier aanbevelingen voor een rechtsstatelijke inzet van slimme opsporingstechnieken gedaan. Dat zijn 1) een controlegroep voor controle vooraf, 2) Big Data-analyse en zelflerende algoritmen als laatste middel, 3) verplichte, openbaar toegankelijke documentatie en 4) een gespecialiseerd toezichthoudend orgaan.

De voorgestelde controlegroep voor controle vooraf, als eerste aanbeveling, dient ervoor te zorgen dat de slimme opsporingstechnieken blijk geven van gebondenheid aan fundamentele, rechtsstatelijke beginselen en rechtsnormen die niet per definitie juridisch afdwingbaar zijn. Zij dient dit te doen door gebruik te maken van bias minimaliserende methoden en door rechtsstatelijke risicofactoren te selecteren. Dat wil zeggen risicofactoren die blijk geven van gebondenheid aan fundamentele, rechtsstatelijke beginselen en rechtsnormen die niet per definitie juridisch afdwingbaar zijn. De controlegroep dient zo divers mogelijk te zijn.

Ten tweede wordt aanbevolen om het gebruik van Big Data-analyse en zelflerende algoritmen zo veel mogelijk te beperken, ofwel in te zetten als laatste slimme opsporingstechniek. Reden voor deze aanbeveling is dat deze twee technieken de meeste risico's met zich meedragen.

De derde aanbeveling, een verplichte, openbaar toegankelijke documentatie, draagt bij aan transparantie als voorwaarde voor (democratische) verantwoording en geeft hierdoor de mogelijkheid de toenemende macht van de slimme opsporingstechnieken in te tomen, waardoor tevens de disbalans van de trias hersteld kan worden. Daarnaast kan de documentatie bruikbaar zijn voor de rechterlijke macht bij het bieden van rechtsbescherming achteraf.

De vierde aanbeveling, een gespecialiseerd, toezichthoudend orgaan, kan de rechter voorzien van een toetsing aan de rechtsstatelijkheid van (de inzet van) de slimme opsporingstechnieken. Dit gespecialiseerd, toezichthoudend orgaan dient de Belastingdienst tijdig te informeren over het toetsingsresultaat. Ingeval sprake blijkt te zijn van een gebrekkige rechtsstatelijke inzet van de slimme opsporingstechnieken, kan de Belastingdienst in samenspraak met het gespecialiseerd, toezichthoudend orgaan zorgdragen voor een verbetering van de inzet van slimme opsporingstechnieken.

Een belangrijk onderdeel van deze aanbevelingen vormt het minimaliseren van bias in de slimme opsporingstechnieken. Dit kan bewerkstelligd worden door gebruik te maken van specifieke bias minimaliserende methoden en het erkennen en bediscussiëren van de aanwezigheid van vooroordelen (in de samenleving). Mijns inziens zijn de geformuleerde aanbevelingen relatief gemakkelijk te implementeren. Het naleven van de aanbevelingen vergt enige welwillendheid van de Belastingdienst, hetgeen mijns inziens niet onredelijk is, zeker niet vanuit de rechtsstatelijkheidsgedachte. Ondanks de relatief gemakkelijke implementatie acht ik aanvullend onderzoek voor het nader concretiseren van de aanbevelingen waardevol. Met concretiseren bedoel ik het verder afstemmen van de aanbevelingen op de specifieke slimme opsporingstechnieken die de Nederlandse Belastingdienst gebruikt. Hier lijkt (ook) empirisch onderzoek naar de exacte werkwijze en inzet van de slimme opsporingstechnieken voor nodig. De nu geformuleerde aanbevelingen kunnen wel handvatten bieden voor verder geconcretiseerde aanbevelingen. Met de geformuleerde aanbevelingen wordt enerzijds gepoogd bewustheid van de risico's van slimme opsporingstechnieken te creëren en anderzijds om deze risico's zo veel als mogelijk te beperken.

8.1 Discussie

In dit onderzoek is een suggestie gegeven voor aanbevelingen voor de rechtsstatelijke inzet van slimme opsporingstechnieken door de Nederlandse Belastingdienst. Tijdens de beantwoording van de onderzoeksvraag zijn nog een aantal lacunes gevonden. In deze paragraaf zal hier aandacht aan besteed worden.

Zo dient nader onderzocht te worden of het wenselijk is dat het gespecialiseerde orgaan als bedoeld in par. 7.4 onafhankelijk dient te zijn of onderdeel uit dient te maken van de Nederlandse Belastingdienst.

Een ander, eerder aangehaald punt van aandacht is het nut en de noodzaak van het opleggen van sancties aan belastingadministraties bij overtreding van (wettelijke) kaders. Daarbij dient aandacht besteed te worden aan de leerstukken van onrechtmatig verkregen bewijs en *naming and shaming*.

Verder is het volgende relevant. In dit onderzoek zijn bestaande richtinggevende kaders voor de inzet van slimme opsporingstechnieken voor overheidsorganen geanalyseerd. De Europese Commissie heeft in april 2021 een voorstel gedaan voor het aannemen van een Europese richtlijn met geharmoniseerde regels voor het gebruik van artificiële intelligentie.[1] Dit is het eerste voorstel tot een rechtskader voor de toepassing van artificiële intelligentie in de Europese Unie.[2] Hoewel zelflerende algoritmen dezelfde bouwstenen gebruiken als artificiële intelligentie systemen, is het niet identiek aan elkaar. 'Artificiële intelligentie is de mogelijkheid van een machine om mensachtige vaardigheden te vertonen – zoals redeneren, leren, plannen

1 Europese Commissie 21 april 2021.
2 European Sources Online 21 april 2021.

en creativiteit.'[3] Een zelflerend algoritme heeft als doel om te beginnen wanneer het redelijke prestaties levert en aan de hand van de input van gebruikers zichzelf te verbeteren. Dat verbeteren werkt volgens hetzelfde proces als het trainen van de artificiële intelligentie. Gelet op het feit dat artificiële intelligentie niet identiek is aan slimme opsporingstechnieken, het voorstel tot op heden nog niet is aangenomen en de geringe omvang van dit onderzoek, is gekozen om dit voorstel voor dit onderzoek niet te analyseren. Het kan echter interessant zijn om hier in vervolgonderzoek wel aandacht aan te besteden.

Tevens kan het interessant zijn om de 'General Principles for the use of Artificial Intelligence in the financial sector' van De Nederlandsche Bank nader te analyseren.[4] Gelet op de reikwijdte van dit onderzoek – het gebruik van slimme opsporingstechnieken bij de Nederlandse Belastingdienst – is gekozen om hier in dit onderzoek geen aandacht aan te besteden.

Tot slot is een lastig punt bij transparantie van slimme opsporingstechnieken van de Nederlandse Belastingdienst het vinden van een goede balans tussen openbaarheid van de werking van de slimme opsporingstechnieken en het voorkomen van gaming the system. In de literatuur is nog weinig te vinden over deze afweging. Het is gelet hierop, mijns inziens raadzaam om te onderzoeken in welke mate gaming the system voorkomt in Nederland.

Uit vervolgonderzoek zal moeten blijken in hoeverre transparantie van slimme opsporingstechnieken zal bijdragen aan de mogelijkheden van gaming the system. Indien blijkt dat transparantie de mogelijkheden tot gaming the system (significant) vergroot, zal op een meer beleidsmatig niveau onderzocht moeten worden wat vanuit het publiek belang zwaarder zou moeten wegen: transparantie van de slimme opsporingstechnieken of beperkte transparantie om de mogelijkheden tot gaming the system te beperken.

3 Europees Parlement 4 september 2020 (online, bijgewerkt 29 maart 2021).
4 Van der Burgt 2019.

Geraadpleegde literatuur

Abdul-Aliyeva & Van Eijk januari 2023
T. Abdul-Aliyeva & G. van Eijk, 'Discriminerende risicoprofielen. Waarom er een verbod moet komen op het gebruik van afkomst als selectiecriterium in (geautomatiseerde) risicoprofilering', *Nederlands Juristenblad*, afl. 4, januari 2023, p. 265-296.

Algemene Rekenkamer juni 2019
Algemene Rekenkamer, *Datagedreven selectie van aangiften door de Belastingdienst*, juni 2019, raadpleegbaar via rekenkamer.nl/publicaties/rapporten/2019/06/11/datagedreven-selectie-van-aangiften-door-de-belastingdienst.

Algemene Rekenkamer januari 2021
Algemene Rekenkamer, *Aandacht voor algoritmes*, januari 2021, raadpleegbaar via rekenkamer.nl/publicaties/rapporten/2021/01/26/aandacht-voor-algoritmes.

Andriessen e.a. maart 2020
I. Andriessen, J. Hoegen Dijkhof, A. van der Torre, E. van den Berg, I. Pulles, J. Iedema & M. de Voogd-Hamelink, *Ervaren discriminatie in Nederland II*, Sociaal Cultureel Planbureau, Den Haag maart 2020.

Arendsen 2008
R. Arendsen, *Geen bericht, goed bericht, Een onderzoek naar de effecten van de introductie van elektronisch berichtenverkeer met de overheid op de administratieve lasten van bedrijven*, proefschrift, Amsterdam: Amsterdam University Press 2008.

Arendsen 2016
R. Arendsen, *Eenvoudig belasting heffen: Tussen droom en daad*, Den Haag: Sdu Uitgevers 2016.

Arndt 1983
A.B. Arndt, 'Al-Khwarizmi', *The Mathematics Teacher JSTOR*, vol. 76, no. 9, 1983, p. 668-670, raadpleegbaar via jstor.org/stable/27963784.

Autoriteit persoonsgegevens
Autoriteit persoonsgegevens, *Data protection impact assessment (DPIA),* raadpleegbaar via autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia.

Belhaj & De Graaf
S. Belhaj & I. de Graaf, 'Kan kunstmatige intelligentie racistisch of seksistisch zijn?', *NOS* 30 mei 2019, raadpleegbaar via nos.nl/artikel/2286930-kan-kunstmatige-intelligentie-racistisch-of-seksistisch-zijn.

Binns & Veale 2021
R. Binns & M. Veale, 'Is that your final decision? Multi-stage profiling, selective effects, and Article 22 of the GDPR', *International Data Privacy Law*, vol. 11, no. 4 2021, p. 319-332.

Blokland & Hondius 2003
T. Blokland & D. Hondius, 'Integratie en racisme. Een verkenning', *Beleid en Maatschappij*, vol. 30 nr. 2 2003.

Bodlaender maart 2017
H.L. Bodlaender, 'Hoe verbonden is je netwerk', *Nieuw archief voor wiskunde* maart 2017, *NAW* 5/18 nr. 1, p. 40-46.

Boon 2020
M. Boon, 'Over nut en nadeel van profileren voor de belastingdienst', *Trouw Letter en Geest* 30 mei 2020.

Bossert 2002
J. Bossert, 'Good Governance: de leidraad voor goed bestuur en management', Overheidsmanagement 2002/9, p. 244-248, raadpleegbaar via primo-institute.com/good-governance-de-leidraad-voor-goed-bestuur-en-management/.

Boyd & Crawford 2012
D. Boyd & K. Crawford, 'Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon', *Information, Communication & Society* 2012, 15, p. 662-679 (online draft versie geraadpleegd op 27 april 2022, via *Research Gate* (p. 2-32)).

Bultheel & Van Barel 1996
A. Bultheel, M. Van Barel & R. Piessens (red.), 'Het Euclidisch algoritme: varianten en toepassingen', *Computerwetenschappen: van vectorruimte tot hyperruimte*, Dept. Computerwetenschappen, K.U. Leuven; Leuven, België 1996, p. 269-294.

Van der Burgt 2019
J. van der Burgt, 'General principles for the use of Artificial Intelligence in the financial sector', *De Nederlandsche Bank Eurosysteem* 2019.

Calders & Žliobaitė, in: *Springer* 2013
T. Calders & I. Žliobaitė, 'Why Unbiased Computational Processes Can Lead to Discriminative Decision Procedures', in: Custers et al. (Eds.), 'Discrimination and Privacy in the Information Society', *Springer* 2013.

Council of Europe 2022
Council of Europe, Bias in algorithms artificial intelligence and discrimination, Vienna 2022.

Custers 2016
B.H.M. Custers, 'Big Data in wetenschappelijk onderzoek', *Justitiële verkenningen* 2016, 1: 8-21 (online, gepubliceerd 26 juli 2018).

Das & Schuilenburg 2018
Das & Schuilenburg, 'Predictive policing: waarom bestrijding van criminaliteit op basis van algoritmen vraagt om aanpassing van het strafprocesrecht', *Strafblad: het nieuwe tijdschrift voor strafrecht*, vol. 2018, no. 4, 33 2018, p. 19-26.

Van Dijck, Snel & Van Golen 2018
G. van Dijck, M. Snel & T. Van Golen, *Methoden van rechtswetenschappelijk onderzoek*, Den Haag: Boom juridisch 2018.

Directorate-General for Justice and Consumers januari 2018
Directorate-General for Justice and Consumers, *De hervorming van de EU-gegevensbeschermingsregels en big data*, European Commission januari 2018, raadpleegbaar via op.europa.eu/en/publication-detail/-/publication/51fc3ba6-e601-11e7-9749-01aa75ed71a1.

Doove & Otten 2018
S. Doove & D. Otten, *Verkennend onderzoek naar het gebruik van algoritmen binnen overheidsorganisaties*, Centrum voor Beleidsstatistiek, Den Haag, projectnummer 180288 november 2018, raadpleegbaar via https://www.kennisopenbaarbestuur.nl/documenten/rapporten/2018/11/27/verkennend-onderzoek-naar-het-gebruik-van-algoritmen-binnen-overheidsorganisaties.

Dusarduijn maart 2019
S.M.H. Dusarduijn, 'De smartrobot in de wereld van het fiscale recht: Bedrijfsmiddel of belastingbetaler?, *MBB: Belastingbeschouwingen: Onafhankelijk Maandblad voor Belastingrecht en Belastingpraktijk'*, nr. 3 maart 2019, p. 116-130.

Dusarduijn, in: *Inleiding belastingheffing ondernemingen en particulieren* 2012
S.M.H. Dusarduijn, 'De fiscale geschiedenis van Nederland in vogelvlucht', in: A.C. Rijkers (ed.), *Inleiding belastingheffing ondernemingen en particulieren,* Sdu fiscale & financiële uitgevers, p. 7-19.

Van Eck 2018
M. van Eck, 'Geautomatiseerde ketenbesluiten & rechtsbescherming: Een onderzoek naar de praktijk van geautomatiseerde ketenbesluiten over een financieel belang in relatie tot rechtsbescherming', *Proefschrift, Tilburg: Tilburg Law School*.

Van Eijsden 2007
J.A.R. van Eijsden, 'Fair play als exponent van fiscaal fatsoen', *WFR 2007/6738*, p. 1133–1138.

Engelsman 'De impact van algoritmes'
M. Engelsman, 'De impact van algoritmes', *Faculteit Elektrotechniek, Wiskunde & Informatica, Technische Universiteit Delft*, raadpleegbaar via tudelft.nl/stories/articles/de-impact-van-algoritmes/.

European Sources Online 21 april 2021
European Sources Online, 'Proposal for a Regulation laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts 21'. april 2021, raadpleegbaar via https://www.europeansources.info/record/proposal-for-a-regulation-laying-down-harmonised-rules-on-artificial-intelligence-artificial-intelligence-act-and-amending-certain-union-legislative-acts/

European Commission 7 juni 2022
European Commission, 'Big data', 7 juni 2022, raadpleegbaar via https://digital-strategy.ec.europa.eu/en/policies/big-data.

Europese Commissie 21 april 2021
Europese Commissie, 'Proposal for a Regulation of the European Parliament and of The Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts {SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}', *Directorate-General for Communications Networks, Content and Technology* 21 april 2021, COM(2021)206.

Europees Parlement 4 september 2020 (online, bijgewerkt 29 maart 2021)
Europees Parlement, *Wat is artificiële intelligentie en hoe wordt het gebruikt?* 4 september 2020 (online, bijgewerkt 29 maart 2021), raadpleegbaar via europarl.europa.eu/news/nl/headlines/society/20200827STO85804/wat-is-artificiele-intelligentie-en-hoe-wordt-het-gebruikt.

Favaretto e.a. 2020
M. Favaretto, E. De Clercq, C.O. Schneble & B.S. Elger, 'What is your definition of Big Data? Researchers' understanding of the phenomenon of the decade', *PLoS ONE* 15(2): e0228987 25 februari 2020, doi.org/10.1371/journal.pone.0228987.

Ibz Federale Overheidsdienst Binnenlandse Zaken
Ibz Federale Overheidsdienst Binnenlandse Zaken, 'Historiek', raadpleegbaar via ibz.be/nl/historiek.

Gelissen 9 februari 2021
M. Gelissen, 'Overheid te kort door de bocht met inzet algoritmes', *Computable* 9 februari 2021 raadpleegbaar via computable.nl/artikel/opinie/digital-innovation/7131764/1509029/overheid-te-kort-door-de-bocht-met-inzet-algoritmes.html.

Gemeente Amsterdam
Gemeente Amsterdam, 'Wat is het algoritmeregister?', raadpleegbaar via algoritmeregister.amsterdam.nl/meer-informatie/.

Gerards, in: *Gelijkheid en (andere) Grondrechten* 2004
R.I.H. Gerards, 'Grondrechten en het recht op gelijke behandeling', in: R. Holtmaat (red.), *Gelijkheid en (andere) Grondrechten*, Deventer: Kluwer 2004.

Gribnau 1998
J.L.M. Gribnau *Rechtsbetrekking en rechtsbeginselen in het belastingrecht. Rechtstheoretische beschouwingen over navordering, toezegging en fiscale vaststellingsovereenkomst*, dissertatie, Deventer: Gouda Quint 1998.

Gribnau, in: *Vijf jaar Wet IB 2001* 2006
J.L.M. Gribnau, 'Rechtsbeginselen en evaluatie van belastingwetgeving', in: A.C. Rijkers & H. Vording (red.), *Vijf jaar Wet IB 2001*, Deventer: Kluwer 2006, p. 24-66.

Gribnau, in: *Ondernemend met pensioen* 2015
J.L.M. Gribnau, 'Heeft de Belastingdienst zijn governance op orde?', in: B. Starink & M. Visser (red.) *Ondernemend met pensioen* (Dietvorst-bundel), Deventer: Wolters Kluwer 2015, p.55-70.

Gribnau 2016
J.L.M. Gribnau, 'Fiscale transparantie: de moeilijke weg naar meer vertrouwen', 85 *MBB* 2016/9, p. 370-384.

Gribnau & Jallai 2017
J.L.M. Gribnau & A.G. Jallai, 'Good Tax Governance: A Matter of Moral Responsibility and Transparency', *Nordic Tax Journal* 2017, issue 1, p. 70-88, raadpleegbaar via SSRN: ssrn.com/abstract=3021914.

Govers e.a. 2021
E. Govers, D. Hanse, G. van Beek, J. Mulder & J. van de Wiel, 'Een burger is geen dataset. Ombudsvisie op behoorlijk gebruik van data en algoritmen door de overheid', *Nationale ombudsman* 2021, Rapportnummer: 2021/021.

Haataja, Van de Fliert & Rautio september 2020
M. Haataja, L. van de Fliert & P. Rautio, 'Public AI Registers Realising AI transparency and civic participation in government use of AI', september 2020, algoritmeregister.amsterdam.nl/en/more-information/.

Hacker 2019
P. Hacker, 'Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies Against Algorithmic Discrimination Under EU Law', *55 Common Market Law Review 1143-1186,* 5 mei 2018 (online, bijgewerkt 17 april 2019).

Hacker & Wiedemann 2017
P. Hacker & E. Wiedemann, 'A continuous framework for fairness', *Working Paper* 2017, raadpleegbaar via arxiv.org/abs/1712.07924.

Happé 1996
R.H. Happé, *Drie beginselen van fiscale rechtsbescherming* (Fiscale monografieën, nr. 77), Deventer: Kluwer 1996.

Heij & De Vries 6 december 2020
J. Heij & J. de Vries, 'Maak van onze fiscale rechtsbescherming een erezaak', *Financieel Dagblad*, 6 december 2020.

Hillinga, 'De Bataafse Republiek'
H. Hillinga, 'De Bataafse Republiek', 23 februari 2009, (online, bijgewerkt 14 augustus 2020), raadpleegbaar via nazatendevries.nl/Artikelen%20en%20Colums/Rooms%20Friese%20recht/De%20Bataafse%20Republiek.html.

Hildebrandt 2008
M. Hildebrandt, 'Defining profiling: a new type of knowledge? Profiling the European citizen', *Profiling the European Citizen*, Dordrecht: Springer 2008, p. 17-45.

Hofs 17 juli 2020
Y. Hofs, 'Belastingdienst schuldig aan structurele discriminatie van mensen die toeslagen ontvingen', *de Volkskrant* 17 juli 2020.

Van Hout 29 augustus 2017
M.B.A. van Hout, 'Rechtsbescherming in het tijdperk van big data', *Weekblad fiscaal recht 2017/165,* 29 augustus 2017, p. 1036-1046.

Ishwarappa & Anuradha 2015
K. Ishwarappa & J. Anuradha, 'A Brief Introduction on Big Data 5Vs Characteristics and Hadoop Technology', *Procedia Computer Science* 2015; 48:319-24.

IJzermans 2015
M.G. IJzermans, 'Lessen geleerd: onderwerp, object, en theoretisch kader van rechtswetenschappelijk onderzoek', *Recht en Methode* 2015, 5 (2) p. 1-23.

Khan, Uddin & Gupta 2014
M. A. -u. -d. Khan, M. F. Uddin & N. Gupta, 'Seven V's of Big Data understanding Big Data to extract value', *Proceedings of the 2014 Zone 1 Conference of the American Society for Engineering Education* 2014, p. 1-5, doi: 10.1109/ASEEZone1.2014.6820689.

Kinder, in: *Oxford University Press* 2013
D.R. Kinder, 'Prejudice and Politics', in: 'The Oxford handbook of political psychology', p. 812-850, L. Huddy, D.O. Sears & J.S. Levy (red.), Oxford: *Oxford University Press* 2013.

Kitchen & McArdle 2016
R. Kitchin & G. McArdle, 'What makes Big Data, Big Data? Exploring the ontological characteristics of 26 datasets', *Big Data & Society* 2016; 3(1), p. 1-10, doi: 101177/2053951716631130.

Lauret 16 augustus 2019
J. Lauret, 'Amazon's sexist AI recruiting tool: how did it go so wrong?', *Becoming Human: Artificial Intelligence Magazine* 16 augustus 2019, raadpleegbaar via becominghuman.ai/amazons-sexist-ai-recruiting-tool-how-did-it-go-so-wrong-e3d14816d98e.

Luzón 27 juli 2020
A.F. Luzón, 'Toen zwaarlijvigheid als teken van succes werd gezien', *National Geographic in geschiedenis en cultuur*, 27 juli 2020, raadpleegbaar via nationalgeographic.nl/geschiedenis-en-cultuur/2020/07/toen-zwaarlijvigheid-als-teken-van-succes-werd-gezien.

Lyon 2003
D. Lyon, *Surveillance as social sorting: Privacy, risk and digital discrimination*, New York: Routledge 2003.

Ministerie van Justitie en Veiligheid 1 maart 2021
Ministerie van Justitie en Veiligheid, 'Richtlijnen voor het toepassen van algoritmen door overheden en publieksvoorlichting over data-analyses', raadpleegbaar via rijksoverheid.nl/documenten/richtlijnen/2021/09/24/richtlijnen-voor-het-toepassen-van-algoritmen-door-overheden-en-publieksvoorlichting-over-data-analyses.

De Mauro, Greco & Grimaldi 2016
A. De Mauro, M. Greco & M. Grimaldi, 'A formal definition of Big Data based on its essential features', *Library Review* 2016, vol. 65, no. 3, p. 122-135.

Nicolaï 2016
P. Nicolaï, 'Het formele en het materiële rechtszekerheidsbeginsel', *AB Klassiek* 2016/3.6.

Nijssen & Stevens 19 september 2019
G.M. Nijssen & L.G.M. Stevens, 'Hoe ICT dienstbaar kan zijn aan wetgeving en wetsinterpretatie', *Weekblad fiscaal recht*, 2019/182, 19 september 2019, p. 1104-1114.

NOS 7 december 2021
'Boete voor Belastingdienst van 2,7 miljoen voor discriminatie toeslagenouders', *NOS,* raadpleegbaar via nos.nl/artikel/2408587-boete-voor-belastingdienst-van-2-7-miljoen-voor-discriminatie-toeslagenouders.

Nussbaum 1984
J. L. Nussbaum, 'Apple Computer, Inc. v. Franklin Computer Corporation Puts the Byte Back into Copyright Protection for Computer Programs', *Golden Gate University Law Review* 1984, vol. 14, iss. 2, art. 3, raadpleegbaar via digitalcommons.law.ggu.edu/ggulrev/vol14/iss2/3.

NU.nl/ANP laatste update 26 januari 2022
'Belastingdienst schatte frauderisico regelmatig in op uiterlijk of nationaliteit', *NU.nl/ANP,* raadpleegbaar via nu.nl/economie/6180204/belastingdienst-schatte-frauderisico-regelmatig-in-op-uiterlijk-of-nationaliteit.

Olsthoorn 2016
P. Olsthoorn, *Big Data voor Fraudebestrijding*. *Working Paper 21*, Den Haag: Wetenschappelijke Raad voor het Regeringsbeleid, 2016.

PwC 22 maart 2022
PwC Onderzoek Query's aan de Poort, 22 maart 2022, raadpleegbaar via rijksoverheid.nl/documenten/rapporten/2022/03/16/onderzoek-querys-aan-de-poort.

Raad van State 15 september 2015
Raad van State, *Raad van State: meer rechtsbescherming nodig bij bestuurlijke boete*, Den Haag 15 september 2015, raadpleegbaar via https://www.rechtspraak.nl/Organisatie-en-contact/Organisatie/Raad-van-State/Nieuws/Paginas/Raad-van-State-meer-rechtsbescherming-nodig-bij-bestuurlijke-boete1214-3761.aspx.

De Raedt, Martens & Brughmans juni 2021
S. De Raedt, D. Martens & D. Brughmans, 'Waarom krijg ik fiscale controle? Naar meer transparantie bij de geautomatiseerde besluitvorming door de fiscale overheid', *T.F.R., 2021/12, nr. 604* (online, bijgewerkt 7 oktober 2022).

Richardson, Schultz & Crawford 13 februari 2019
R. Richardson, J.M. Schultz & K. Crawford, 'Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice', *94 N.Y.U. L. REV. ONLINE 192* 13 februari 2019 (online, bijgewerkt 16 juni 2021), online raadpleegbaar via SSRN: ssrn.com/abstract=3333423.

Rekenhof 14 januari 2015
Rekenhof, *Organisatie van de controleacties in de personenbelasting*, 14 januari 2015, raadpleegbaar via https://www.ccrek.be/NL/Publicaties/Fiche.html?id=155ae9f3-7ae0-4bd4-a1f4-3c1797f5ee6e.

Rouvroy 2016
A. Rouvroy, 'Of Data and Men: Fundamental Rights and Liberties in a World of Big Data', *T-PD-BUR(2015)09REV ed.* Strasbourg: Council of Europe, *2016.*

Sainstrain 2003
M. Sainstrain, *TIC. Nouveaux standards transactionnels et fiscalité, Planbureau Working paper*, 15-03 augustus 2003.

Sensoy & DiAngelo 2017
Ö. Sensoy & R. DiAngelo, 'Is everyone really equal?', Multicultural Education, J.A. Banks, Second Edition 2017.

Staats 17 juli 2020
C. Staats, 'Understanding Implicit Bias: What Educators Should Know', *American Educator* 17 juli 2020, raadpleegbaar via facinghistory.org/resource-library/understanding-implicit-bias-what-educators-should-know.

UN Committee on the Elimination of Racial Discrimination 27 december 2020
UN Committee on the Elimination of Racial Discrimination, 'General recommendation No. 36 (2020) on preventing and combating racial profiling by law enforcement officials: Committee on the Elimination of Racial Discrimination', *CERD/C/GC/36*, 102nd sess. 2020: virtual, 17 december 2020.

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

Vranken, in: *Recht en Methode* 2015
J.B.M. Vranken, 'Is de rechtswetenschap gebaat bij een breed strijklicht? Over juridische dogmatiek en methodologie', in: M.G. IJzermans, 'Lessen geleerd: onderwerp, object, en theoretisch kader van rechtswetenschappelijk onderzoek', *Recht en Methode* 2015, 5 (2) p. 1-23.

WRR 2016
Wetenschappelijke Raad voor het Regeringsbeleid, *Big Data in een vrije en veilige samenleving*, Den Haag: Amsterdam University Press, 2016.

Xythali 2018
V. Xythali, *Introduction into gbv core concepts, principles and approaches for non specialized professionals*, Research Centre for Gender Equality (KETHI), raadpleegbaar via

buildingasafetynet.org/wp-content/uploads/2018/11/Diotima-Interagency-Training-Package-Final-Isuu.pdf.

Zweistra & Poort juni 2022
Zweistra & Poort, 'Hoe de trias politica technologische ontwikkeling in haar macht krijgt: het belang van de samenwerking tussen recht, politiek en technologie', *Ars Aequi* juni 2022, p. 457-464.

Zwenne, Steenbruggen & Reker 2016
G. Zwenne, W. Steenbruggen & M. Reker, 'Rechtsbescherming bij het gebruik van big data door toezichthouders: een verkenning', *Tijdschrift voor Toezicht* 2016, (7) 4 doi: 10.5553/TvT/187987052016007004003, p. 29-44.

Steeds vaker worden slimme opsporingstechnieken zoals algoritmen ingezet door overheidsorganen. Ook de Belastingdienst maakt hier veelvuldig gebruik van. Rechtsstatelijkheid, welke kort gezegd grenzen stelt aan de bevoegdheidsuitoefening van de overheid, wordt daarbij lang niet altijd gewaarborgd. Toen recentelijk bleek dat het algoritmeregister van de overheid een half jaar na ingebruikname nog nauwelijks wordt ingevuld, is dit nogmaals duidelijk geworden.

'Een wervelwind aan data, funest voor rechtsstatelijke beginselen?' is een onderzoek naar hoe de rechtsstatelijkheid van (de inzet van) algoritmen, big-data-analyse en profiling door de Nederlandse Belastingdienst gewaarborgd kan worden. Uiteen is gezet wat deze 'slimme opsporingstechnieken' inhouden en hoe de Nederlandse Belastingdienst hier gebruik van (heeft ge)maakt. Daarnaast zijn verschillende vormen van transparantie geduid welke van belang zijn bij (de inzet van) slimme opsporingstechnieken. Uiteindelijk is een viertal aanbevelingen geformuleerd. Hiervoor is inspiratie ontleend aan al bestaande richtinggevende kaders voor de inzet van slimme opsporingstechnieken, welke eveneens worden behandeld in dit onderzoek. De geconstateerde risico's die kleven aan de inzet van slimme opsporingstechnieken vormen de basis van de geformuleerde aanbevelingen. Opvolging van de aanbevelingen zal leiden tot het waarborgen van een rechtsstatelijke inzet van slimme opsporingstechnieken en kan bijdragen aan het bereiken van een meer inclusieve, diverse en gelijkwaardige maatschappij.

Charlotte Kaebisch studeert Fiscaal Recht en International Business Taxation aan Tilburg University. Daarnaast zet zij zich in voor de maatschappij als vrijwilliger bij verschillende organisaties.

Wolters Kluwer