Fiscus + Big Data = Big Brother?

Een toetsing van het gebruik van big data door de fiscus aan artikel 8 EVRM

Masterscriptie aan de Faculteit der Rechtsgeleerdheid, Vrije Universiteit Amsterdam
Afstudeerrichting: Internet, Intellectuele Eigendom en ICT
Naam: Maarten Hoyng
Begeleider: Mr. dr. T.H.A. Wisman

Inhoud

Afkortingen

A-G	Advocaat-Generaal
AB	Rechtspraak bestuursrecht
Awb	Algemene wet bestuursrecht
ANPR	Automatic Number Plate Recognition
AWR	Algemene wet inzake rijksbelastingen
BNB	Beslissingen in belastingzaken, Nederlandse Belastingrechtspraak
DD	Delikt en Delikwent
ECLI	European Case Law Identifier
EHRM	Europees Hof voor de Rechten van de Mens
EVRM	Europees Verdrag tot bescherming van de Rechten van de Mens en de fundamentele vrijheden
FED	Fiscaal weekblad FED
GW	Grondwet
HR	Hoge Raad der Nederlanden
HvJ EU	Hof van Justitie van de Europese Unie
Jo	Juncto
NJ	Nederlandse jurisprudentie
Nr.	Nummer
NTFR	Nederlands Tijdschrift voor Fiscaal Recht
p.	Pagina
par.	Paragraaf
Rb.	Rechtbank
Stb.	Staatsblad
TFB	Tijdschrift Formeel Belastingrecht
V-N	Vakstudie Nieuws
WFR	Weekblad Fiscaal Recht
WRR	Wetenschappelijke Raad voor het Regeringsbeleid

1. Inleiding

1.1 Aanleiding

De fiscus is belast met de vaststelling van feiten en omstandigheden die als basis dienen voor de belastingheffing. Om te zorgen dat de heffing naar juistheid geschiedt, is er bij de fiscus de noodzaak om te beschikken over relevante informatie. Bij het uitvoeren van haar taak komt de fiscus op basis van de wet ruime informatievergaringsbevoegdheden toe. Door middel van deze bevoegdheden verkrijgt de fiscus veel (privacygevoelige) gegevens die de basis vormen voor haar *big data*-toepassingen. Digitalisering heeft ertoe geleid dat de reikwijdte van deze bevoegdheden nog breder zijn geworden. Waar de stand van de technologie vroeger een beperking vormde voor het vergaren en verwerken van informatie, speelt deze nu juist een faciliterende rol. Deze ontwikkelingen zijn de fiscus niet onopgemerkt gebleven en de fiscus maakt dan ook op grote schaal gebruik van *big data*-toepassingen zoals: *datamining, profiling* en *nudging*. Deze ruime bevoegdheden die de fiscus tot haar beschikking heeft, hebben ertoe geleid dat de fiscus is uitgegroeid tot de "grootste informatiefabriek" van het land.[1]

De ruime wettelijke informatievergaringsbevoegdheden in combinatie met de digitalisering van de afgelopen jaren kan ertoe leiden dat de bevoegdheden van de fiscus verder reiken dan oorspronkelijk bedoeld was door de wetgever. In dit verband kan men zich afvragen of deze bevoegdheden niet dusdanig worden opgerekt dat er sprake is van een onrechtmatige inbreuk op het recht op privacy dat is neergelegd in artikel 8 Europees Verdrag tot bescherming van de Rechten van de Mens en de fundamentele vrijheden (hierna: EVRM). Des te meer omdat een wettelijke grondslag voor de inzet van *big data*-toepassingen door de fiscus lijkt te ontbreken. Dit volgt onder andere uit de door de Hoge Raad in 2017 gewezen Automatic Number Plate Recognition-arresten (hierna: ANPR), waarbij de vraag centraal stond of er een voldoende wettelijke basis bestond voor het gebruik van de informatie die verzameld is middels de ANPR-camera's. Volgens de Hoge Raad bestond er een onvoldoende specifieke wettelijke basis voor de fiscus om informatie te vergaren, registreren, bewerken en vervolgens te gebruiken. Hierdoor was er volgens de Hoge Raad sprake van een inbreuk op artikel 8 EVRM. Deze zienswijze van de Hoge Raad werd eerder dit jaar eveneens bevestigd door de Rechtbank Den Haag in de Systeem Risico Indicatie-zaak (hierna: SyRi). SyRi is een *big data*-toepassing waarbij overheidsinstellingen (waaronder de fiscus) informatie met elkaar delen teneinde deze informatie aan elkaar te koppelen en te analyseren om belastingfraude op te sporen en te bestrijden. De rechtbank oordeelde in deze zaak dat de wetgeving onvoldoende transparant en controleerbaar was inzake de inzet van SyRi, waardoor deze toepassing in strijd werd geacht met artikel 8 EVRM.
De zeer ruime bevoegdheden van de fiscus in combinatie met digitalisering lijken daarmee op gespannen voet te staan met artikel 8 EVRM. In deze scriptie zal nader onderzoek worden gedaan naar dit spanningsveld. De vraag die bij dit spanningsveld rijst is hoe de wettelijke bevoegdheden rondom het gebruik van *big data* door de fiscus zich verhouden tot het recht op privacy (artikel 8 EVRM).

[1] M. Martijn 'Vergeet de politiestaat. Welkom in de belastingstaat', *De Correspondent* 2014.

1.2 Onderzoeksvraag en deelvragen

Zoals in de vorige paragraaf vermeld, wordt er in deze scriptie inzicht verschaft in de verhouding tussen de bevoegdheden inzake het gebruik van *big data* door de fiscus en artikel 8 EVRM. In dit hoofdstuk zal allereerst de onderzoeksvraag en bijbehorende deelvragen worden besproken, waarna vervolgens de onderzoeksmethode, afbakening en doel van deze scriptie worden behandeld.

De centrale onderzoeksvraag luidt:

'In hoeverre wordt het recht op privacy, dat is verankerd in artikel 8 EVRM, geschonden bij het gebruik van big data door de fiscus?'

De probleemstelling wordt beantwoord aan de hand van de volgende deelvragen:

- Wat wordt er verstaan onder het begrip 'big data'? (hoofdstuk 2)
- Welke wettelijke bevoegdheden heeft de fiscus voor het gebruik van *big data*? (hoofdstuk 2)
- Hoe is het recht op privacy van artikel 8 EVRM vormgegeven? (hoofdstuk 3)
- In hoeverre vormt het gebruik van *big data* door de fiscus een inbreuk op het privacybegrip van artikel 8 EVRM? (hoofdstuk 4)

De opbouw van dit onderzoek ziet er als volgt uit. In hoofdstuk 2 wordt uiteengezet wat onder *big data* wordt verstaan en worden de wettelijke bevoegdheden omtrent het vergaren en gebruik van *big data* door de fiscus uiteengezet. Vervolgens wordt in hoofdstuk 3 het privacybegrip van artikel 8 EVRM uiteengezet, waarna in hoofdstuk 4 getoetst zal worden of het vergaren en gebruik van *big data* door de fiscus een inbreuk oplevert met het recht op privacy. Tenslotte wordt in hoofdstuk 5 de centrale probleemstelling beantwoord in de algehele conclusie.

1.3 Onderzoeksmethode, afbakening en doel

Om inzicht te krijgen in hoeverre het gebruik van *big data* door de fiscus een inbreuk vormt op artikel 8 EVRM, heb ik gekozen voor een rechtswetenschappelijk onderzoek waarbij een jurisprudentie-analyse wordt aangevuld met de resultaten van een literatuuronderzoek.
Het recht op privacy is naast artikel 8 EVRM eveneens neergelegd in de artikelen 7 en 8 Handvest van de grondrechten van de Europese Unie (hierna: Handvest) en artikel 10 Grondwet (hierna: GW). In deze scriptie is gekozen om te toetsen aan artikel 8 EVRM aangezien het Handvest slechts betrekking heeft op gevallen waarin het EU-recht ten uitvoer wordt gelegd. Daarnaast is op grond van artikel 120 GW grondwettelijke toetsing verboden, waardoor eveneens een toetsing aan artikel 10 GW niet voor de hand ligt.
Het doel van het onderzoek is om duidelijk te maken wat de wettelijke bevoegdheden van de fiscus zijn inzake het gebruik van *big data*, wat het recht op privacy behelst en hoe deze zich tot elkaar verhouden.

2. De fiscus en big data

2.1 Inleiding

De fiscus heeft adequate gegevens en inlichtingen nodig om haar taken uit te voeren. De data die de fiscus vergaart vormen de basis voor haar *big data*-toepassingen. Door de toegenomen digitalisering en de huidige techniek is het voor de fiscus eenvoudiger om grote hoeveelheden data te vergaren en te verwerken. Deze ontwikkelingen zorgen ervoor dat de fiscus haar werkzaamheden effectiever en efficiënter uit kan voeren. Zoals de titel van dit hoofdstuk al doet vermoeden, zal ik in dit hoofdstuk ingaan op de mogelijkheden die *big data* bieden voor de fiscus. De vraag die in dit hoofdstuk dan ook centraal staat is: welke wettelijke bevoegdheden de fiscus heeft voor het gebruik van *big data*. Hierbij zal specifiek stilgestaan worden of het huidige wettelijke kader een voldoende wettelijke grondslag biedt voor het gebruik van *big data* door de fiscus. Omdat het gebruik van *big data* door de fiscus geschiedt op grond van de informatievergaringsbevoegdheden die zijn verankerd in de Algemene wet inzake rijksbelastingen (hierna: AWR), zullen deze bevoegdheden eveneens in dit hoofdstuk aan bod komen.

Allereerst zal in §2.2 het begrip '*big data*' uiteen worden gezet, vervolgens zal ik in §2.3 ingaan op de informatievergaringsbevoegdheden van de fiscus. In §2.4 zal vervolgens het gebruik van *big data* door de fiscus worden behandeld, waarbij de *big* data-technieken: *datamining*, *profiling* en *nudging* centraal staan. Ten slotte zal in de laatste paragraaf van het hoofdstuk worden afgesloten met een deelconclusie.

2.2 Big data

Volgens de literatuur kent het begrip '*big data'* geen eenduidige definitie.[2] Zo hanteert het McKinsey Global Institute bijvoorbeeld een definitie van het begrip waarbij de omvang van de verzamelde data als uitgangspunt geldt.[3] Terwijl bij de door Boyd en Crawford gehanteerde definitie juist de rationaliteit en complexiteit van data centraal staat.[4] Het woord 'big' refereert in dat geval aan de grote verscheidenheid van mogelijke gegevenscombinaties.

Aan de hand van de verschillende definities die worden gebruikt voor het begrip *big data,* heeft de Wetenschappelijke Raad voor het Regeringsbeleid (hierna: WRR) drie hoofdkenmerken van *big data* onderscheiden, namelijk: (1) data, (2) analyse en (3) gebruik.[5] Voor dit onderzoek gebruik ik deze drie, door WRR gedefinieerde, hoofdkenmerken om invulling te geven aan het begrip *big data*.

---

[2] Zie o.a.: L. Floridi, 'Big Data and their epistemological challenge', *Philosophy and Technology* 2012/25, p. 435-437., p. 435-437; Ekbia e.a., 'Big Data, bigger dilemmas: A critical review', *Journal of the Association for Information Science and Technology* 2015, p. 1523-1545.

[3] Definitie: "Big Data refers to datasets whose size is beyond the ability of typical database software tools to capture, store, manage and analyze."; 'Big Data: The next frontier for innovation, competition and productivity', *McKinsey Global Institute* 2011, www.mckinsey.com/business-functions/businesstechnology/our-insights/big-data-the-next-frontier-for-innovation, bezocht op 12 december 2020.

[4] Definitie: "Big data is notable not because of its size, but because of its relationality to other data"; Boyd & Crawford 2014, p. 662-679.

[5] *Big Data voor Fraudebestrijding*, WRR, Den Haag: Wetenschappelijke Raad Regeringsbeleid 2016, p. 35.

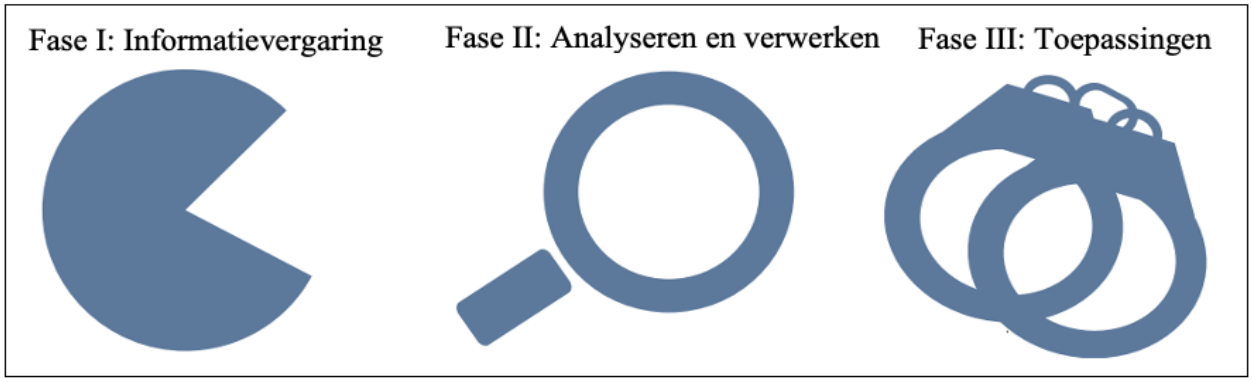
Wat precies onder deze drie hoofdkenmerken wordt verstaan, wordt hieronder schematisch weergegeven:

1. Data	-Omvang van de data: het gaat om grote hoeveelheden gegevens. -Structuur van de data: het kan gaan om gestructureerde of ongestructureerde gegevens of een combinatie van beide. -Variëteit van de data: het gaat om de combinatie van verschillende databronnen.
2. Analyse	-Methode van analyse: de analyse is data-gedreven, er wordt dus gezocht naar patronen in de data zonder vooraf opgestelde hypothesen. -Oriëntatie van de analyse: hoewel big data-analyses ook inzicht kunnen geven in het verleden, zijn het met name de analyses van het heden en de toekomst waar de focus op ligt.
3. Gebruik	-Grensoverschrijdende toepassing: data uit het ene domein kan worden gebruikt voor beslissingen in het andere domein. -Toepasbare kennis: conclusies op geaggregeerd niveau kunnen worden toegepast voor beslissingen op groeps- of individueel niveau.

Dit schema is overgenomen uit WWR, Big Data in een vrije en veilige samenleving, 2016, p.35.[4]

De drie hoofdkenmerken van *big data* kunnen worden beschouwd als fasen in een proces, dat in zijn geheel bestaat uit: het vergaren van informatie (uiteengezet in §2.3), het analyseren en verwerken van deze informatie en tenslotte het gebruik van *big data*-toepassingen (deze laatste twee fases worden uiteengezet in §2.4).

Deze drie fases van het *big data*-proces worden weergegeven in figuur 2.1.



Figuur 2.1. De drie fasen van big data. (Bron: WRR, 'Big Data in een vrije en veilige samenleving', Amsterdam University Press 2016, p. 39)

De fiscus is als momenteel niet (volledig) transparant over de processen rondom fasen II & III van het WRR-model. De fiscus probeert, naar eigen zeggen, op deze manier te verhinderen dat men misbruik kan maken van het opsporingssysteem dan wel dat men zich hiertegen wapent, ook wel '*gaming the system'* genoemd.[6] Door de huidige techniek en digitalisering is er steeds meer informatie over individuen bekend bij de fiscus, echter omgekeerd is de fiscus verre van transparant tegenover individuen over de manier waarop zij *big data*-analyses toepast. Dit wordt

[6] *Big Data voor Fraudebestrijding*, WRR, Den Haag: Wetenschappelijke Raad Regeringsbeleid 2016, p.144; zie ook: 'Waarborgen tegen risico's van data-analyses door de overheid', bijlage bij *Kamerstukken II* 19/20, 26643, 641.

ook wel de transparantieparadox genoemd.[7] Het gebruik van *big data*-analyses gaat volgens deze paradox hand in hand met de toenemende machtsverschuiving tussen individuen en de fiscus. De fiscus krijgt hierdoor vrij spel en kan dus ongebonden haar taken uitvoeren.

Door het ontbreken van een transparant beleid vanuit de fiscus omtrent *big data*-processen is het voor betrokkenen moeilijk, dan wel onmogelijk, om de rechtmatigheid van deze bevoegdheden te toetsen. Immers, deze processen van de fiscus zijn voor de betrokkene onzichtbaar. Een tekenend voorbeeld hiervan zijn de nagenoeg volledige, door de fiscus, zwartgelakte dossiers die betrokkene in de recente toeslagenaffaire onder ogen kregen.[8]

Dat de fiscus over de mogelijkheid beschikt om deze analyse processen rondom *big data* geheim te houden, is mijns inziens verwonderlijk te noemen wanneer men dit vergelijkt met hoe de geheimhouding bij opsporingsdiensten is geregeld. Opsporingsdiensten houden in beginsel ook hun processen geheim echter dienen opsporingsdiensten, in tegenstelling tot de fiscus, zich wel te conformeren aan wettelijke procedures, waaronder bijvoorbeeld de notificatieplicht.[9] De notificatieplicht is een belangrijk vereiste voor de naleving van grondrechten waaronder het recht op privacy omdat het een cruciale en betrouwbare uitvoering afdwingt. Daarnaast is het hierdoor mogelijk om tegen eventuele misstanden vooraf te ageren in plaats van achteraf. Door wettelijke procedures, zoals deze bestaan bij opsporingsdiensten, bestaat er geen kans op een *gaming the system*-situatie, maar bestaat er een gezonde(re) machtsverhouding tussen individuen en de opsporingsdiensten. Het argument van de fiscus dat men vreest voor een *gaming the system*-situatie wanneer zij transparant is over haar processen, lijkt dan ook voort te komen uit eigenbelang en ingegeven vanuit de wens van de fiscus om ongebonden haar taken uit te kunnen blijven voeren.

2.3 Informatievergaring door de fiscus

In deze paragraaf komen de verschillende wettelijke informatievergaringsbevoegdheden van de fiscus aan bod. Omdat het gebruik van *big data* door de fiscus geschiedt op grond van de informatievergaringsbevoegdheden die zijn verankerd in de AWR, zullen deze bevoegdheden in deze paragraaf worden besproken. Het vergaren van informatie vormt de eerste fase in het *big data*-proces. De fiscus heeft binnen de overheid een voortrekkersrol bij de ontwikkeling en het gebruik van *big data*, wat onder andere komt doordat de fiscus de beschikking heeft over een zeer grote dataset van gegevens en inlichtingen die relevant kunnen zijn voor het heffen en innen van belastingen.[10] De fiscus heeft de beschikking over verschillende instrumenten om deze fiscale informatie te vergaren. Allereerst bestaat er de verplichting voor belastingplichtigen om aangifte

[7] Richards, N.M. en H.J. King, 'Three paradoxes of Big Data', Stanford Law Review, September 2013, https://www.stanfordlawreview.org/online/privacy-and-big-data-three-paradoxes-of-big-data/, bezocht op 10 december 2020.

[8] https://www.rtlnieuws.nl/nieuws/nederland/artikel/5169750/belastingdienst-zwarte-lijsten-fraude-toeslagenaffaire; De betrokken hebben gebruik gemaakt van hun inzagerecht (art. 15 AVG). Volgens de fiscus is deze informatie zwartgelakt om zo geen afbreuk te doen aan de rechten en vrijheden van anderen (art.15 lid 4 AVG), maar omdat het voor de betrokkenen ook niet zichtbaar was hoe de processen rondom *big data*-toepassingen door de fiscus zijn vormgegeven, heeft het er alle schijn van dat de fiscus ook deze bewust heeft zwartgelakt.

[9] De notificatieplicht is neergelegd in art. 126 BB SV; De gedachte achter deze notificatieplicht is dat de burger wiens recht op privacy door de overheid is geschonden hiervan op de hoogte dient te worden gesteld.

[10] De Belastingdienst beschikt over gegevens en inlichtingen van ±11 miljoen burgers en ±1,5 miljoen ondernemers die kunnen ingezet ter bestrijding van fraude; WRR-Rapport Big Data 2016, p. 57.

te doen, de zogenoemde hoofdverplichting. Daarnaast heeft de wetgever de fiscus enkele controlebevoegdheden toebedeeld, gezien de belastingplichtige in beginsel een kennisvoorsprong heeft ten opzichte van de inspecteur. Deze controlebevoegdheden zijn neergelegd in de artikelen 47 tot en met 56 AWR en compenseren de ongelijkheid in kennis tussen de belastingplichtige en de inspecteur.[11]

Ten eerste bestaat er op grond van artikel 47 AWR de verplichting voor belastingplichtigen om, wanneer de fiscus daarom vraagt, informatie te verschaffen en toegang te verlenen tot documenten die hij/zij tot zijn beschikking heeft. Daarnaast beschikt de fiscus over de mogelijkheid om informatie op te vragen bij derden (artikel 53 AWR) en bij overheidsinstanties (artikel 55 AWR). Tot slot kan de fiscus informatie vergaren aan de hand van de samenwerkingsafspraken die gemaakt zijn met andere overheidspartijen met bettrekking tot het uitwisselen van fiscaalrechtelijke relevante gegevens.

2.3.1 Gegevensverstrekking door de belastingplichtige

De fiscus maakt bij het analyseproces en de toepassing van *big data* gebruik van interne informatie die is verkregen aan de hand de wettelijke informatievergaringsbevoegdheden van de fiscus.[12] De informatie die verkregen is vanuit de belastingplichtige zelf vormen hierbij de primaire bron. Op grond van artikel 8 AWR kent de belastingplichtige de verplichting om aangifte te doen en daarnaast dient deze op grond van artikel 10a AWR uit eigen beweging onvolledigheden en onjuistheden te melden die van belang kunnen zijn voor de belastingheffing. In geval deze informatieverstrekking door de belastingplichtige voor de fiscus ontoereikend blijkt te zijn en/of de fiscus deze informatie wenst te controleren, heeft de inspecteur de mogelijkheid om nadere informatie bij de belastingplichtige te verzoeken. De verplichting van de belastingplichtige om informatie te verstekken aan de fiscus is neergelegd in artikel 47, eerste lid, AWR en luidt als volgt:

"Ieder is gehouden desgevraagd aan de inspecteur:
a. de gegevens en inlichtingen te verstrekken welke voor de belastingheffing te zijnen aanzien van belang kunnen zijn;
b. de boeken, bescheiden en andere gegevensdragers of de inhoud daarvan — zulks ter keuze van de inspecteur — waarvan de raadpleging van belang kan zijn voor de vaststelling van de feiten welke invloed kunnen uitoefenen op de belastingheffing te zijnen aanzien, voor dit doel beschikbaar te stellen."

De informatieplicht van artikel 47 AWR geldt voor zowel natuurlijke- als rechtspersonen en strekt zich uit over alle gegevens waarover de belastingplichtige beschikt dan wel informatie waarover hij/zij op een eenvoudige wijze over kan beschikken.[13] Deze informatieverplichting kan worden onderscheiden in een actieve- en passieve informatieplicht.[14] Bij de actieve informatieplicht wordt

[11] G.J. Zwenne, *Belastingheffing en informatieverplichtingen*, Den Haag: Sdu 1998, p. 33.
[12] M. Martijn, 'Baas Belastingdienst over Big Data: 'Mijn missie is gedragsverandering', *De Correspondent*, 21 april 2015, https://decorrespondent.nl/2720/baas-belastingdienst-over-big-data-mijn-missie-is-gedragsverandering/83656320-f6e78aaf, bezocht op 15 december 2020.
[13] HR 25 januari 2002, ECLI:NL:HR:2002:AD8475, par. 3.
[14] L.A. de Blieck e.a., *Algemene wet inzake rijksbelastingen*, Deventer: Kluwer 2019, p. 141.

door de informatieplichtige zelf (privacygevoelige) 'gegevens en inlichtingen' verschaft (artikel 47, lid 1, aanhef en onderdeel a, AWR). Een vereiste hierbij is dat de, schriftelijke dan wel mondelinge, vragen van de inspecteur aan de belastingplichtige van feitelijke aard dienen te zijn en ondubbelzinnig en duidelijk moeten zijn geformuleerd.[15] Bij de passieve informatieplicht moeten 'boeken, bescheiden en andere gegevensdragers' voor raadpleging beschikbaar worden gesteld (artikel 47, lid 1, aanhef en onderdeel b, AWR). Volgens de parlementaire geschiedenis moeten deze begrippen ruim worden uitgelegd en kunnen elektronische bestanden hier ook onder worden geschaard.[16] Hierbij kan bijvoorbeeld worden gedacht aan facturen, brieven, notulen, WhatsApp-conversaties, e-mailgesprekken, bankafschriften en creditcardoverzichten.

De verplichting om informatie te verstrekken ziet op alle informatie die 'van belang kan zijn' voor het heffen van belasting. De belastinginspecteur komt met deze 'kan'- bepaling een zeer grote beoordelingsruimte toe om te beslissen welke informatie benodigd is. Uit de praktijk volgt dan ook dat deze voorwaarde een zeer geringe invloed heeft op de inhoud en reikwijdte van de opgevraagde gegevens.[17]

Geconcludeerd kan worden dat de informatieverplichting van artikel 47 AWR een brede reikwijdte kent, welke door digitalisering nog breder is geworden. Zo beschikt de inspecteur bij de uitoefening van zijn bevoegdheid bijvoorbeeld over de mogelijkheid om een integrale kopie te maken van gegevensdragers van de belastingplichtige, een zogenoemde 'forensic image'. Een kenmerk van een *forensic image* is dat er naast de huidige zichtbare informatie tevens een kopie wordt gemaakt van de 'onzichtbare' informatie die door de belastingplichtige ogenschijnlijk is gewist.[18] Daarnaast maakt de huidige technologie het voor de fiscus mogelijk om afgeleide informatie inzichtelijk te maken. Zo kan de fiscus bijvoorbeeld uit een bulk e-mail-, telefoon- en WhatsApp historie de verblijfplaats van de belastingplichtige achterhalen. In de literatuur wordt betoogd dat deze handelingen van de fiscus onrechtmatig zijn omdat deze in strijd zouden zijn met het verbod op een *fishing expeditie* (dit begrip wordt in 2.3.2 nader besproken).[19] Mijns inziens zijn deze handelingen door de fiscus echter niet per definitie onrechtmatig, zolang er in een concrete situatie maar een redelijk evenwicht bestaat tussen de meewerkplicht en het recht op privacy van de belastingplichtige.[20] Dit is dan ook belangenafweging die per situatie kan verschillen.

In geval de inspecteur om gegevens heeft verzocht en de belastingplichtige hieraan onvoldoende gevolg heeft gegeven, beschikt de inspecteur over de mogelijkheid om een informatiebeschikking, in de zin van artikel 52a AWR, af te geven. De informatiebeschikking vormt een waarborg voor de betrokkene tegen bevoegdheidsovertreding vanuit de overheid. Behoudens de situatie waarbij

[15] Dit volgt uit Art. 49 lid 1 AWR; HR 28 oktober 2009, ECLI:NL:HR:2009:BK3815 (concl. A-G Ijzerman).
[16] *Kamerstukken II* 1988-89, 21287, 3, p. 5,21.
[17] G.J. Zwenne, *Belastingheffing en informatieverplichtingen*, Den Haag: Sdu 1998, p. 34.
[18] Deze voor de belastingplichtige 'onzichtbare' informatie kan, mogelijk met behulp van een IT-expert, alsnog door de Belastingdienst worden ingezien waardoor deze toegang heeft tot bijv. verwijderde bestanden en historiek van bestanden. Handeling geschied o.g.v. art. 49 lid 2 AWR; Hof 's-Hertogenbosch 21 maart 2006, LJN:AW4328.
[19] Zie o.a.: G.H. Ulrich & R.W.J. Kerckhoffs, *De informatiebeschikking*, Fed fiscale brochures 2016, p. 43; J.T.M. Megens, 'Art. 47 AWR: taal of digitaal?', *FF* 2001/219-06.
[20] Dit evenwicht kan worden gecreëerd door de betrokkene te voorzien van adequate en effectieve waarborgen tegen misbruik, zoals bijv. de betrokkene aanwezig te laten zijn wanneer de fiscus deze handelingen uitvoert of de kopie te verzegelen gedurende de bezwaarprocedure (EHRM, 14 maart 2013, nr. 24117/08 (*Bernh Larsen Holding*).

de vereiste aangifte niet is gedaan, vindt de omkering en verzwaring van de bewijslast namelijk pas plaats wanneer de informatiebeschikking onherroepelijk is geworden.[21] Door middel van de informatiebeschikking is het mogelijk om van tevoren de proportionaliteit en rechtmatigheid van het informatieverzoek te laten toetsen door een rechter zonder het risico te lopen dat de bewijslast wordt omgekeerd en verzwaard. Uit het evaluatieverslag betreffende de informatiebeschikking volgt dat deze regeling de rechtsbescherming van de betrokkene ten goede komt.[22]

In geval de belastingplichtige niet voldoet aan de in artikel 52a AWR neergelegde verplichtingen, leidt dit tot het opleggen van dwangmiddelen. Zo zal de betrokkene worden geconfronteerd met omkering en verzwaring van de bewijslast (artikel 25, derde lid, AWR en artikel 27e, eerste lid, AWR), daarnaast kan de inspecteur een boete opleggen en/of strafvervolging instellen (artikelen 68 en 69 AWR) en tenslotte kan de inspecteur een civiele procedure aanhangig maken (artikel 52a, vierde lid, AWR).

De verplichting uit artikel 47 AWR kent een zeer ruime reikwijdte welke door digitalisering nog ruimer is geworden. De informatiebeschikking biedt de belastingplichtige hierbij een belangrijke waarborg bij de bescherming van zijn of haar recht op privacy. Op de vraag of de belastingplichtige bij een derdenonderzoek ook over (voldoende) waarborgen beschikt, zal in de volgende paragraaf antwoord worden gegeven.

2.3.2 Derdenonderzoek

Een andere controlebevoegdheid waarover de fiscus beschikking heeft, is het zogenoemde ‘derdenonderzoek’. De fiscus heeft met het derdenonderzoek een machtig middel in handen om grote hoeveelheden informatie te vergaren die kunnen worden gebruikt bij het analyseproces en de toepassing van *big data*. Het doel van het derdenonderzoek is om de Belastingdienst in staat te stellen om gegevens en inlichtingen van de belastingplichtige effectief te controleren door middel van informatie afkomstig van één of meerdere derde(n).[23] De fiscus kan informatie betreffende derden opvragen bij administratieplichtigen op grond van artikel 53 AWR en bij overheidsinstellingen op grond van artikel 55 AWR.

De meerwaarde van de inlichtingen en informatie afkomstig van een derde partij is voornamelijk het gegeven dat deze doorgaans ‘objectiever’ en dus betrouwbaarder zijn dan in geval de belastingplichtige deze zelf zou verstrekken.[24] Volgens Kamerling is deze *contra-informatie* zelfs essentieel voor een goede fiscale informatiepositie van de belastingdienst.[25] De belastingplichtige is namelijk niet in staat om de omvang en aard van de informatie waarover een derde beschikt te beïnvloeden. Naast de repressieve werking kent het derdenonderzoek ook een preventieve werking. Het enkele bestaan van de mogelijkheid dat de belastingdienst de informatie bij derden

[21] *Kamerstukken II* 2008-09, 30645, 14, p. 5.
[22] *Kamerstukken II* 2016-17, 33 772, nr. 2, staatssecretaris van Financiën 30 november 2016 over het Evaluatierapport Wet houdende wijziging van de Algemene wet inzake rijksbelastingen en enige andere wetten ten behoeve van de rechtsbescherming met betrekking tot de administratieplicht en controlehandelingen van de fiscus (Wet-Dezentjé’).
[23] Zie: Fiscale Encyclopedie De Vakstudie Algemeen Deel, Deventer: Wolters Kluwer, art. 53 AWR, aant. 1.4 (Doel en strekking).
[24] M.W.C. Feteris, *Formeel belastingrecht*, Deventer: Wolters Kluwer 2007, p. 199.
[25] R.N.J. Kamerling & E.C.J.M. van der Hel, ‘Derdenonderzoeken in internationaal perspectief’, *WFR* 2013/6544.

kan verifiëren, leidt namelijk tot een vergroting van het fiscale normbesef bij de belastingplichtige. Hierdoor wordt de kans vergroot dat de belastingplichtige bij de aangifte volledige en correcte informatie aan de fiscus overlegt en dat dit tevens tijdig gebeurt.[26]

Artikel 53, eerste lid, onderdeel a, AWR regelt dat de verplichtingen van artikelen 47 tot en met 50 AWR naar analogie van toepassing zijn ten aanzien van de belastingheffing van derden.
Onderdeel b van hetzelfde artikel regelt daarnaast de bevoegdheid van de belastinginspecteur om informatie op te vragen bij administratieplichtigen. Doordat de artikelen 47 tot en met 50 AWR ook van toepassing zijn bij het derdenonderzoek, geldt de actieve en passieve informatieverplichting ook voor derden en inhoudingsplichtigen.

Ook bij het derdenonderzoek dient alle informatie verstrekt te worden die 'van belang kan zijn' voor de belastingheffing. Zoals reeds besproken, in §2.3.1, komt de fiscus met deze 'kan'- bepaling een zeer grote beoordelingsruimte toe om te beslissen welke informatie benodigd is. Het derdenonderzoek kan volgens artikel 53, eerste lid, AWR alleen worden opgelegd aan zogenoemde 'administratieplichtigen', blijkens het tweede lid van deze bepaling behoren tot deze kring van administratieplichtigen: de inhoudingsplichten, resultaatgenieters, lichamen en natuurlijke personen die een zelfstandig beroep dan wel bedrijf uitoefenen. Deze partijen dienen de boeken, bescheiden en andere gegevensdragers ten minste zeven jaar te bewaren.[27] Het toepassingsgebied van het derdenonderzoek is beperkt zich tot het verwerven van gegevens en inlichtingen van 'derden'. Dit begrip kent een ruime reikwijdte, omdat je volgens de rechtspraak al tot de kring van derden behoort in geval er een (indirecte) relatie bestaat tussen de belastingplichtige en de betrokkene.[28]

Bij het stelselmatig verzamelen van informatie dient volgens de wetsgeschiedenis het recht op privacy van de belastingplichtige gerespecteerd te worden.[29] Verder is het volgens de wetgever van belang dat de fiscus 'prudent' dient om te gaan met de bevoegdheid om een derdenonderzoek in te stellen, omdat het veelal privacygevoelige gegevens betreft.[30] Zo dient de inspecteur enige proportionaliteit te betrachten bij het opvragen van inlichtingen, waarbij de te leveren inspanningen vanuit de administratieplichtige in verhouding dient te staan met het fiscale belang.[31]

Het opvragen van gegevens in het kader van een derdenonderzoek kan de fiscus zowel doen op individueel niveau, door het verzoek te richten aan een bij naam genoemde derde, als ook door middel van zogenoemde 'serievragen'. Dit zijn ongerichte informatieverzoeken vanuit de fiscus aan personen en lichamen betreffende één of meerdere derde(n), teneinde contra-informatie te verkrijgen.[32] De bevoegdheid om serievragen te stellen door de fiscus, zorgt ervoor dat deze in staat is om een grote hoeveelheid fiscaal relevante gegevens van belastingplichtigen tegelijkertijd te verkrijgen, wat deze methode tot een effectieve manier van informatievergaring maakt.[33] Het

[26] J. van Blijswijk e.a., 'Beheersverslag Belastingdienst 2004', p. 22.
[27] Dit volgt uit artikel 52, vierde lid, AWR.
[28] Hof Den Haag 30 december 2004, LJN:AS1915, *AB* 2006/301 m.nt. O.J.D.M.L. Jansen.
[29] *Kamerstukken II* 1988-89, 21287, nr. 3, p. 24.
[30] *Kamerstukken II* 1987-88, 19393, nr. 3, p. 7-8.
[31] *Kamerstukken II* 1986-87, 19393, nr. 150b.
[32] Volgens de wetsgeschiedenis kan het gaan om informatie uit het verleden, heden als ook informatie in de nabije toekomst (*Kamerstukken II*, 1985-1986, 19393, nr. 3, p. 6.).
[33] Idem.

gevaar hierbij bestaat dat de fiscus de verzamelde informatie uiteindelijk gebruikt voor andere doeleinden, wat in strijd is met het détournement de pouvoir-beginsel.[34] De belastinginspecteur mag met het instellen van een derdenonderzoek namelijk enkel informatie opvragen ten behoeve van de belastingheffing en deze bevoegdheid dus niet gebruiken voor onderzoek van strafrechtelijke aard.[35]

Bij het stellen van serievragen is het een vereiste dat het controle-element prevaleert bij het verzamelen van gegevens bij de ondervraagde derde.[36] In geval niet aan dit vereiste wordt voldaan, en er dus grote hoeveelheden informatie wordt opgevraagd zonder dat er sprake is van specifieke aanwijzingen van fraude, wordt gesproken van een 'fishing expeditie' oftewel het 'hengelen naar informatie'. Waar het stellen van serievragen rechtmatig is, geldt dit niet voor een fishing expeditie, omdat bij een fishing expeditie onder de noemer van het uitoefenen van controle, louter de focus ligt op het opsporen van delicten.[37] Het probleem is dat bij het stellen van serievragen, niet door de Belastingdienst op voorhand wordt uitgesloten dat deze nadien tevens een fishing expeditie uitvoert.[38] Dit geef de fiscus de mogelijkheid om op grote schaal '*big data*' te vergaren, wat als basis kan dienen voor *big data*-analyse en -toepassingen. Volgens van Houte kan de grens tussen een fishing expeditie en het stellen van serievragen niet eenduidig worden getrokken.[39] Dit valt volgens hem te verklaren doordat de Belastingdienst soms redenen voor een informatievergaring door middel van een derdenonderzoek verzint, teneinde de fishing expeditie te rechtvaardigen. Een voorbeeld hierbij is de SMSParking-zaak waarbij het hof zelf ook lijkt te insinueren dat de fiscus aan opsporing doet. De fiscus vraagt namelijk de parkeergegevens in bulk op, teneinde te voorkomen dat de belastingplichtigen die 'gecontroleerd' worden iets kunnen vermoeden.[40]

Het informatieverzoek uit artikel 53 AWR heeft geen vrijblijvend karakter. De administratieplichtige is dus verplicht om hieraan mee te werken.[41] Tegen het informatieverzoek kan geen bezwaar of beroep worden ingesteld door de administratieplichtige omdat dit verzoek geen, zoals bedoeld in artikel 26 AWR, 'voor bezwaar vatbare beschikking' betreft.[42] Wanneer de administratieplichtige van mening is dat het informatieverzoek onrechtmatig is, kan deze wel een schadevergoeding achteraf claimen op grond van artikel 53, vijfde lid, AWR (de zogenoemde: kostenvergoedingsbeschikking). Dit schadevergoedingsverzoek wordt beoordeeld door de fiscus zelf, wat neerkomt op een 'slager die zijn eigen vlees keurt'. Waar de kostenvergoedingsbeschikking destijds in het leven is geroepen om te dienen als waarborg voor de administratieplichtige, kom ik tot de conclusie dat deze regeling met haar onrechtmatigheidstoetsing achteraf en welke daarnaast uitgevoerd wordt door een niet onafhankelijke partij, geen adequate waarborg betreft.

---

[34] Dit beginsel is neergelegd in art. 3:3 Awb.
[35] M.C.W. Feteris, *'Formeel Belastingrecht'*, Deventer: Kluwer 2007, p.254.
[36] C.P.M. van Houte, 'De Belastingdienst op fishing expedition', *WFR* 2005/1078, p. 1.
[37] Idem.
[38] Dit heeft zich o.a. voorgedaan in de SMSParking-zaak, waarbij door de fiscus parkeer en- en kentekengegevens werd 'gestofzuigd' die eigenlijk vernietigd had moeten worden. Met deze actie heeft de Belastingdienst in 2013 de 'Big Brother Award' gewonnen van Bits of Freedom, zie: https://bba2013.bof.nl/2013/08/dit-zijn-de-winnaars-minister-opstelten-ende-belastingdienst/index.html.
[39] C.P.M. van Houte, De Belastingdienst op fishing expedition, *WFR* 2005/6634, p. 3.
[40] Hof Den Bosch, 19 augustus 2014 m.nt. T.H.A Wisman, *Computerrecht* 2014/182, p. 329.
[41] E. Poelmann, 'Algemene beginselen van behoorlijk bestuur bij informatieverzoeken', *TFO* 2017/152.1, p.156.
[42] Dit volgt uit artikel 26 AWR.

Het niet voldoen aan het derdenonderzoek wordt beschouwd als een belemmering van de controletaak van de belastinginspecteur, waardoor aan de administratieplichtige sancties kunnen worden opgelegd.[43] Wanneer er niet wordt voldaan aan de informatieverplichtingen uit artikel 53, eerste tot en met derde lid, AWR en de administratieplichtige eveneens inhoudingsplichtig is, kan de bewijslast worden omgekeerd en verzwaard.[44] Bovendien is er de mogelijkheid om de administratieplichtige strafrechtelijk te vervolgen omdat deze zich, bij het niet voldoen aan zijn of haar informatieplicht, schuldig maakt aan een strafbaar feit.[45] Ten slotte beschikt de fiscus over de mogelijkheid om doormiddel een procedure bij de voorzieningsrechter informatie af te dwingen op straffe van een dwangsom.[46] Aangezien de rechter geen limiet hoeft te stellen aan de betreffende dwangsom, kan dit bedrag omvangrijk zijn.[47]

Ook kan de fiscus op grond van artikel 55, eerste lid, AWR informatie opvragen aan overheidsinstanties. Hierbij behoort teven tot de mogelijkheid om serievragen te stellen, echter dient hierover eerst wel overleg plaats te vinden op centraal niveau.[48] In geval overheidsinstanties niet mee willen werken aan het informatieverzoek omdat dit strijdig zou zijn met hun geheimhoudingsplicht, kan de betreffende instantie zich beroepen op artikel 55, tweede lid, AWR. Eveneens als artikel 53 AWR bestaat er bij het niet voldoen aan de informatieverplichting van artikel 55 AWR de mogelijkheid voor de fiscus om een boete op te leggen op grond van artikel 68, eerste lid, onderdeel a, AWR.

Al met al kan worden gesteld dat het derdenonderzoek een ruime reikwijdte kent, waarbij de fiscus tevens dwangmiddelen kan inzetten om de gevraagde informatie af te dwingen. De kostenvergoedingsbeschikking vormt hierbij geen adequate waarborg voor de betrokkene.

2.3.3 Gegevensuitwisseling

Bij het vergaren van informatie door de Belastingdienst, heeft de fiscus naast de verschillende controle-instrumenten ook samenwerkingsafspraken gemaakt met overheidspartijen met betrekking tot het onderling uitwisselen van fiscaalrechtelijke relevante gegevens. Deze afspraken zijn vastgelegd in overeenkomsten tussen de betrokken partijen en worden ook wel ‘convenanten’ genoemd. Deze gegevensuitwisselingen tussen overheidsinstanties zorgt ervoor dat de fiscus op eenvoudige wijze toegang heeft tot nog meer *big data*. Bij deze gegevensuitwisseling dient het recht op privacy van de betrokkene in ogenschouw genomen te worden.

Zoals reeds vermeld, beschikt de fiscus over ruime wettelijke instrumenten om (veelal privacygevoelige) informatie over belastingplichtigen te vergaren. De wetgever heeft een geheimhoudingsplicht geïntroduceerd in artikel 67 AWR met het doel om de privacy van de burgers te beschermen en zorg te dragen dat de door de fiscus verzamelde informatie enkel voor

[43] Belangrijk hierbij te vermelden is dat er tegen dit informatieverzoek geen bezwaar kan worden aangetekend door de bevraagde omdat art. 53 AWR niet aan te merken valt als besluit.
[44] Op grond van art. 25, derde lid, aanhef en onderdeel b, AWR jo. art. 27e, aanhef en onderdeel b, AWR.
[45] Op basis van art. 68, tweede lid, sub a, b en c of bij opzet art. 69, eerste en tweede lid, AWR.
[46] Deze civiele procedure is mogelijk op grond van art. 52a lid 4 AWR.
[47] https://www.trouw.nl/nieuws/de-top-van-de-belastingdienst-drukte-de-onrechtmatige-aanpak-stopzetten-kinderopvangtoeslag-erdoor~b96b4867/.
[48] Kamerstukken II, 1985-1986, 19 393, nr. 3, p. 7.

de heffing en invordering van de belasting gebruikt wordt.[49] Op grond van artikel 67, eerste lid, AWR is het voor de fiscus in beginsel niet toegestaan om verzamelende gegevens uit te wisselen met andere partijen. Deze geheimhoudingsplicht is voor de belastingplichtige van groot belang.[50] Voor de belastingplichtige is het namelijk een groot goed dat zijn persoonlijke gegevens enkel mogen worden gebruikt voor belastingdoeleinden en er dus geen misbruik van deze gegevens wordt gemaakt door derden. Verder zal de geheimhoudingsplicht er naar waarschijnlijkheid voor zorgen dat de bereidwilligheid van de belastingplichtigen om informatie te verstrekken toe zal nemen, omdat deze informatie niet wordt ingezet voor andere doeleinden.

In artikel 67, tweede en derde lid, AWR worden enkele uitzonderingen gegeven op de hoofdregel van de geheimhoudingsplicht. Een voorbeeld van een uitzondering waarbij de geheimhoudingsplicht niet geldt, is in het geval van gegevensuitwisseling tussen de fiscus en overheidspartijen inzake de belastingheffing.[51] De informatie die de Belastingdienst heeft vergaard, kan namelijk ook van belang zijn voor andere partijen, en vice versa. Deze uitzondering maakt het voor de fiscus mogelijk om gegevens uit te wisselen met partijen die zijn opgenomen op de lange lijst van artikel 67, tweede lid, onderdeel b, AWR juncto artikel 43c Uitvoeringsregeling AWR. Volgens Blieck is deze lijst zo veelomvattend dat met iedere partij die een rechtmatig belang heeft om kennis te nemen van de fiscale informatie, gegevens kunnen worden uitgewisseld.[52] Uit kamerstukken blijkt dan ook dat de fiscus veelvoudig gegevens uitwisselt met overheidspartijen.[53] De huidige situatie van het aantal koppelingen is helaas niet bekend, maar volgens de kamerstukken zou de fiscus in 2014 de beschikking hebben gehad over ongeveer 100 diverse gegevensbestanden van andere overheidsinstanties.[54] Volgens Snippe kan de fiscus hiermee gerekend worden tot een van de grootste informatieverstrekkers binnen de overheid en de WRR doet hier zelfs nog een schepje boven op door te stellen dat de fiscus "koploper en spil in samenwerkingsverbanden voor data-analyses" is.[55]

Door gegevens aan elkaar te koppelen is er meer data beschikbaar over belastingplichtigen, wat relevant kan zijn voor belastingheffingen. Echter, het nadeel hiervan is dat de kwaliteit van data lastig is te verifiëren. Het risico hierbij kan zijn dat er meer onjuiste veronderstellingen worden gemaakt. Een voorbeeld in praktijk waarbij hiervan sprake was, is een zaak van de Australische Belastingdienst.[56] Deze Belastingdienst besloot haar database te verbinden met de database van een uitkeringsinstantie. Het gevolg hiervan was dat vele duizenden belastingplichtigen ten onrechte een inkomenscorrectie hadden ontvangen. De oorzaak van deze fout was gelegen in het feit dat de systemen dermate waren onderontwikkeld om de data van beide partijen met elkaar te vergelijken. Hierdoor werd er bij bedrijven, die onder verschillende benamingen actief waren, inkomsten dubbel meegerekend. Uit dit voorbeeld volgt dat door het samenvoegen van data,

[49] *Kamerstukken II* 2005-06, 30322, nr. 3 (MvT), p. 12.
[50] L.A. de Blieck e.a., *Algemene wet inzake rijksbelastingen*, Deventer: Kluwer 2019, p. 106.
[51] Op grond van art. 67, lid 2, sub b AWR jo. art. 43c Uitv.reg. AWR 1994.
[52] L.A. de Blieck e.a., *Algemene wet inzake rijksbelastingen*, Deventer: Kluwer 2019, p. 111.
[53] *Kamerstukken II* 2014-15, 26 653, nr. 355; Lijst van convenanten van de Belastingdienst is te raadplegen via: https://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/belastingdienst/intermediairs/toezicht/convenanten/convenanten_met_afnemers_van_informatie/convenanten_met_afnemers_van_informatie_van_de_belastingdienst.
[54] *Kamerstukken II* 2014-15, 26 653, nr. 355.
[55] *Big Data voor Fraudebestrijding*, WRR, Den Haag: Wetenschappelijke Raad Regeringsbeleid 2016, p. 52.
[56] Zie onderzoek ombudsman: www.ombudsman.gov.au/news-and-media/media-releases/media-release-documents/commonwealth-ombudsman/2017/centrelink-complaints.

belastingplichtigen veel kwetsbaarder zijn. Daar komt bij dat in het geval een dataset fouten bevat en er gegevensuitwisseling heeft plaatsgevonden tussen verschillende overheidspartijen, het vrijwel onmogelijk is om de consequenties daarvan weer ongedaan te maken.[57] Het risico bestaat dat de consequenties hiervan uiteindelijk voor rekening van de burger komt doordat deze zelf dient te bewijzen dat er een fout is gemaakt. Een ander nadeel van gegevensuitwisseling is een mogelijke privacyschending, doordat er een verhoogd risico is op een datalek. Bij het uitwisselen van data kan het voorkomen dat deze onvoldoende beschermd is, waardoor data mogelijk in verkeerde handen terecht kan komen, met alle gevolgen van dien zoals bijvoorbeeld identiteitsfraude. Het is dan ook zaak dat de fiscus, als groot databezitter, streeft naar het hoogst mogelijke niveau van gegevensbeveiliging.

Big data maakt dat het steeds eenvoudiger wordt om gegevens van de fiscus te verbinden met gegevens van andere overheidsinstanties. Deze gegevensuitwisselingen tussen instanties dienen te voldoen aan artikel 8 EVRM, waardoor er een wettelijke grondslag en er tevens noodzaak aanwezig moet zijn. Informatie die de fiscus heeft ontvangen van een andere overheidsinstantie waarvoor geen wettelijke grondslag bestaat, is in strijd met het recht op privacy. Als voorwaarde voor de gegevensuitwisseling dient er per uitwisseling een belangenafweging te worden gemaakt. Deze belangenafweging wordt, anders dan bij de eerder besproken informatievergaringsbevoegdheden (art. 47, 53 en 55 AWR), gemaakt door de fiscus zelf in plaats van door de betreffende individuen of bedrijven. Voor een adequate bescherming van het recht op privacy is het mijns inziens beter dat deze belangenafweging door een onafhankelijke partij geschiedt.

[57] *Kamerstukken II* 2017-18, 26643, nr. 557, p. 4.

2.4 Big data-toepassingen van de fiscus

Wanneer de gegevens van individuen en bedrijven door de fiscus zijn verzameld, kan er worden gestart met het proces van analyseren en systematisch verwerken van deze data. De toenemende digitalisering bij de fiscus heeft ertoe geleid dat de hoeveelheid vergaarde data in de afgelopen jaren exponentieel is toegenomen. Deze grote dataset aan gegevens biedt de fiscus de mogelijkheid om hierop *big data*-analyses toe te passen. Hierdoor kunnen mogelijk relevante patronen worden geïdentificeerd, wat vervolgens een basis kan vormen om het gedrag van belastingplichtigen te voorspellen en hier mogelijk zelfs op in te spelen door gedragsbeïnvloeding toe te passen.

Waar de fiscus verschillende wettelijke bevoegdheden kent voor het vergaren van *big data*, bestaan er geen nadere wettelijke grondslagen voor de analyse en toepassing van deze data. In de praktijk blijkt de fiscus de wettelijke bepalingen rondom het vergaren van *big data* tevens te gebruiken om beleid te formuleren voor *big data*-analyses en -toepassingen.

Big data-analyses spelen bij de fiscus een prominente rol. Zo volgt uit de investeringskalender van de fiscus dat er veel gelden zijn geïnvesteerd in systemen om analyses uit voeren en daarnaast zijn er bij de fiscus in de afgelopen jaren de nodige data-analisten in dienst getreden.[58] Uit de vacaturetekst van de functie 'data scientist', volgt dat de fiscus bij het uitvoeren van de data-analyses onder andere gebruik maakt van de volgende drie toepassingen: het op geautomatiseerde wijze opsporen van patronen (*datamining)*, het groeperen van belastingplichtigen waarbij het gedrag van deze personen wordt voorspeld *(profiling)* en tevens het toepassen van gedragsbeïnvloeding op de belastingplichtigen (*nudging*).[59] Deze drie technieken zullen in dit onderzoek achtereenvolgens worden besproken in de subparagrafen 2.4.1 tot en met 2.4.3.

2.4.1 Datamining

Door de toenemende digitalisering beschikt de fiscus over de mogelijkheid om *big data* snel en efficiënt te analyseren, hierbij maakt de fiscus gebruik van *datamining*. Dit betreft een softwarematige techniek waarbij grote hoeveelheden gegevens met elkaar worden verbonden. Daarbij wordt getracht om aan de hand van algoritmes patronen te ontdekken die van toegevoegde waarde kunnen zijn, zonder hierbij een causaal verband aan te tonen.[60] *Datamining* helpt de fiscus om bruikbare informatie te onttrekken uit grote hoeveelheden data, waardoor de fiscus een beter beeld kan krijgen van een specifieke belastingplichtige. Een bijkomend voordeel van het toepassen van *datamining* door de fiscus, is dat deze techniek ook op toekomstige situaties kan worden toegepast. Patronen uit het verleden kunnen in dit geval een basis vormen om het toekomstig gedrag van belastingplichtigen te voorspellen.[61]

Echter, kleeft er volgens van Hout ook een risico aan het gebruik van *datamining*.[62] Bij het gebruik van deze techniek bestaat er namelijk de kans op 'toevallige' correlaties, want in geval er grote hoeveelheden gegevens worden geanalyseerd, kunnen er altijd wel patronen tussen variabelen

[58] Belastingdienst,'Hoofdlijnen aanpak Belastingdienst: Activiteitenkalender', Den Haag: 2015, p. 27.
[59] Zie: https://werken.belastingdienst.nl/starters/data-science/.
[60] M.B.A. van Hout, 'Rechtsbescherming in het tijdperk van big data', *WFR 2017/165,* p. 4-5.
[61] Idem.
[62] Idem.

worden aangetoond. Toevallige correlaties dienen actief te worden opgespoord door de fiscus teneinde te vermijden dat de fiscus onjuiste conclusies trekt, want bij toevallige correlaties hoeft nog geen sprake te zijn van causaliteit.[63] Bij een causaal verband is er sprake van oorzaak en gevolg, terwijl bij een correlatie dit niet het geval hoeft te zijn. Bij een correlatie is sprake van een onderlinge verbondenheid tussen twee componenten.

Zoals reeds besproken in §2.4 kent de fiscus geen specifieke grondslag voor *datamining*. Gezien het privacygevoelige karakter van deze toepassing, betwijfel ik dan ook of *datamining* niet in strijd is met artikel 8 EVRM.

Wanneer de fiscus de patronen in de data heeft blootgelegd, kan deze vervolgens een risicoprofiel van een belastingplichtige schetsen om zo de kans op fraude te voorspellen. Deze handeling wordt behandeld in de volgende paragraaf.

2.4.2 Profiling

De fiscus is, vanwege haar beperkte capaciteit, niet in de mogelijkheid om alle binnengekomen belastingaangiften te controleren. Het is daarom dat de fiscus de *big data*- toepassing: *profiling* inzet als handhavings- en controlemiddel. Aan de hand van *profiling* wordt er een risicoprofiel van de belastingplichtige geschetst waarmee de fiscus de kans op fraude voorspelt. Dit risicoprofiel van de belastingplichtige wordt op geautomatiseerde wijze gebouwd aan de hand van risico-indicatoren die gebaseerd zijn op (privacygevoelige) gegevens en inlichtingen die eerder door de fiscus zijn vergaard.[64]

Een voorbeeld van een risico-indicator aan de hand waarvan de fiscus besluit dat een belastingplichtige in een hoger risicoprofiel valt, is in het geval de belastingplichtige veel aftrekposten heeft opgegeven in zijn of haar aangifte.[65] Een ander voorbeeld van een risico-indicator is de situatie wanneer belastingplichtigen van elkaar scheiden. Uit statistieken van de fiscus volgt namelijk, dat er in het jaar van de echtscheiding een grotere kans is dat belastingplichtigen hun belastingaangifte verkeert invullen.[66] Daarom controleert de fiscus doorgaans vaker en/of strenger op de aangiftes van deze specifieke groep belastingplichtigen.

Volgens de voormalig Directeur van de Belastingdienst, de heer Blokpoel, wordt *profiling* door de fiscus ingezet om aan elke belastingplichtige de behandeling te geven waar hij/zij recht op heeft.[67] Belastingplichtigen met een hoger risicoprofiel worden intensiever gecontroleerd, terwijl

---

[63] Idem.
[64] Algemene Rekenkamer, 'Datagedreven selectie van aangiften door de Belastingdienst', te raadplegen via: https://www.rekenkamer.nl/binaries/rekenkamer/documenten/rapporten/2019/06/11/datagedreven-selectie-van-aangiften-door-de-belastingdienst/Dategedreven+selectie+aangiften+door+Belastingdienst+WR.pdf.
[65] P. Klein, 'Belastingdienst geeft toe: toch sprake van etnisch profileren', Rtlnieuws.nl, 11 mei 2020, https://www.rtlnieuws.nl/nieuws/artikel/5117616/belastingdienst-toeslagen-profileren-nationaliteit, bezocht op 10 december 2020.
[66] Volgens documentatie van de Belastingdienst maken gescheiden stellen gemiddeld 2,5 keer vaker fouten bij het invullen van de inkomstenbelasting dan getrouwde stellen. Zie: https://www.ad.nl/economie/leuker-kan-de-belastingdienst-scheiden-niet-maken~a6b464a5/?referrer=https%3A%2F%2Fwww.google.com%2F.
[67] M. Martijn, 'Baas Belastingdienst over Big Data: 'Mijn missie is gedragsverandering', *De Correspondent*, 21 april 2015, https://decorrespondent.nl/2720/baas-belastingdienst-over-big-data-mijn-missie-is-gedragsverandering/83656320-f6e78aaf, bezocht op 15 december 2020.

belastingplichtigen die juist in een lager risicoprofiel zijn geschaald doorgaans meer met rust worden gelaten door de fiscus. Deze aanpak leidt volgens de heer Blokpoel tot een efficiëntere en effectievere uitvoering van controle- en handhavingscapaciteit binnen het overheidsorgaan.[68]

Volgens de literatuur kleven er echter ook risico's aan het gebruik van *profiling* door de fiscus. Zo geeft van Hout aan dat er een risico bestaat op vooringenomenheid of zelfs discriminatie. Er zou namelijk een oneerlijke behandeling plaats kunnen vinden tussen verschillende belastingplichtigen, omdat de ene belastingplichtige vanwege een vastgesteld risicoprofiel frequenter onderhevig is aan controle dan de andere.[69] Daarnaast bestaat er volgens Custers het risico op een 'tunnelvisie', omdat de fiscus zich met haar controle- en handhavingscapaciteit voornamelijk focust op de groep belastingplichtigen met een hoog risicoprofiel. Hierdoor is het plausibel dat men bij deze groep meer correcties toe zal passen. Dit heeft mogelijkerwijs als bijkomend gevolg dat andere belastingplichtigen die belastingfraude plegen, niet zullen worden opgemerkt door de fiscus.[70]

Recent zijn de hierboven besproken risico's nu werkelijkheid geworden bij de fiscus. Sedert 2019 concludeerde de Algemene Rekenkamer in haar onderzoeksrapport: 'Datagedreven selectie van aangiften door de Belastingdienst' dat: "de wijze waarop door de Belastingdienst met de privacy van burgers wordt omgesprongen bij de onderzochte modellen op orde is". Echter, een jaar later blijkt het tegenovergestelde uit onder andere de 'toeslagenaffaire', waar de fiscus heeft bekend al sinds 2012 gebruik te hebben gemaakt van een discriminerende risico-indicator, namelijk: het hebben van een dubbele nationaliteit van de belastingplichtige.[71] Uit het rapport van de commissie-Donner, die onderzoek deed naar de toeslagenaffaire, volgt dat de fiscus bij haar fraudebeleid "institutionele vooringenomenheid" toepaste. Zo bepaalde de fiscus namelijk op voorhand of een burger kon worden aangemerkt als verdachte waardoor deze feitelijk geen kans had op een eerlijke behandeling.[72] Geconcludeerd kan worden dat er vanuit de fiscus op grote schaal persoonsgegevens zijn misbruikt waardoor verregaande en onjuiste conclusies zijn getrokken.

Dat hierbij geen sprake is van een incident bij de fiscus, blijkt uit de recente onthulling van RTL-nieuws over het bestaan van een, tot voor kort geheime, 'zwarte lijst' die al sinds 2001 door de fiscus wordt gebruikt.[73] Deze zwarte lijst betreft het datasysteem Fraude Signalering Voorziening (hierna: FSV) waarin maar liefst 250.000 belastingplichtigen als (potentiële) fraudeurs zijn geïdentificeerd. Volgens medewerkers van de Belastingdienst werd je al in het FSV-systeem als 'potentieel' fraudeur bestempeld en ook zo behandeld, in geval er slechts sprake was van 'signalen' of 'vermoeden' van fraude.[74] Een saillant detail hierbij is dat, uit onafhankelijk onderzoek van KPGM, is komen vast te staan dat belastingmedewerkers van de afdeling Toeslagen in enkele

[68] Belastingdienst, '14e halfjaarsrapportage 2014', p. 13.
[69] M.B.A. van Hout, 'Rechtsbescherming in het tijdperk van big data', *WFR 2017/165*, p. 4-5.
[70] B. Custers, 'Risicogericht toezicht, profiling en Big Data', *TvT 2014/3.2*, p. 4.
[71] P. Klein, 'Belastingdienst geeft toe: toch sprake van etnisch profileren', Rtlnieuws.nl, 11 mei 2020, https://www.rtlnieuws.nl/nieuws/artikel/5117616/belastingdienst-toeslagen-profileren-nationaliteit, bezocht op 10 december 2020.
[72] *Kamerstukken II* 2019-20, 31066, nr. 546, p. 2; Deze vooringenomenheid van de Belastingdienst is in strijd met artikel 2.4 AWB.
[73] Zie: https://www.rtlnieuws.nl/nieuws/nederland/artikel/5037966/belastingdienst-toeslagenaffaire-ministerie-van-financien; Het FSV-systeem inmiddels volgens de fiscus niet meer in werking omdat het in strijd zou zijn met de AVG-wetgeving, zie: *Kamerstukken II* 2019-20, 31066, nr. 632.
[74] *Kamerstukken II* 2019-20, 31066, nr. 632, p. 4.

gevallen het hokje 'fraude' al aangekruist hadden alvorens het onderzoekstraject was afgerond.[75] Een bijkomend probleem is dat in geval een belastingplichtige eerder onterecht op een zwarte lijst van de fiscus heeft gestaan, deze nog jarenlang daarna onder het vergrootglas van de fiscus ligt en dus extra gecontroleerd zal worden.[76]

Zoals blijkt uit bovenstaande voorbeelden, kan het analyseren van informatie door middel van *profiling* een grote impact hebben op de privacy van de belastingplichtige. Daarbij is het door een gebrek aan transparantie over *big data*-analysemethodes voor de belastingplichtige moeilijk in te schatten wat de exacte impact van *profiling* kan zijn op haar of zijn privéleven. Het is daarom dat de Raad van de Europese Unie en het Europees Parlement van mening is dat er een 'krachtig en coherent kader' dient te bestaan voor het verwerken van persoonsgegevens.[77] Echter, zoals reeds in §2.4 besproken, bestaat er momenteel geen wettelijk kader voor *big data*-toepassingen. De fiscus past *profiling* toe om op een efficiënte manier fraude te bestrijden, waarbij het belang van het recht op privacy voor de betrokkene ondergeschikt lijkt te zijn. Dit blijkt wel uit het feit dat er momenteel geen wettelijke waarborgen bestaan om misbruik en willekeur vanuit de fiscus tegen te gaan.

Nadat de fiscus een risicoprofiel van de belastingplichtige heeft gevormd, volgt de volgende stap in het proces: *nudging*. Deze techniek zal in de volgende paragraaf worden behandeld.

2.4.3 Nudging

Nudging is een techniek waarmee wordt beoogd om het gedrag van personen in positieve zin te veranderen.[78] De fiscus past deze techniek proactief toe om het gedrag van de belastingplichtige op een dusdanige wijze te beïnvloeden dat hij/zij eerder bereid is om volledig, juist en tijdig aangifte te doen.[79] Hierbij geldt het adagium: 'voorkomen is beter dan genezen'.

Dat *nudging* bij de fiscus hoog op de agenda staat, blijkt uit een interview van de heer Blokpoel met De Correspondent waar hij aangeeft: "mijn missie is gedragsverandering". De fiscus heeft zelfs een speciaal Gedragsveranderingsteam opgericht die deze psychologische gedragsmotivatietechniek veelvuldig toepast.[80] Een voorbeeld waar de fiscus *nudging* toepast is bij de vooraf ingevulde belastingaangifte, die grotendeels informatie bevat welke door de fiscus is verkregen door derden. De fiscus past deze *nudge* toe om het invullen van de belastingaangifte voor de burger te vergemakkelijken, wat zal resulteren in een hogere compliance. Omdat de vooraf ingevulde aangifte een standaardoptie is, wordt dit als een sterke *nudge* gezien. Uit onderzoek is

---

[75] *Rapportage verwerking van risicosignalen voor toezicht belastingdienst*, bijlage bij *Kamerstukken II* 2019/20, 31066, nr. 681, p. 39-40.
[76] J. Kleinnijenhuis, 'Belastingdienst hield nóg een omstreden fraudejacht, nu bij aangifte inkomen', Trouw.nl, 7 juli 2020, https://www.trouw.nl/economie/belastingdienst-hield-nog-een-omstreden-fraudejacht-nu-bij-aangifte-inkomen~b08482ef/, bezocht op 6 december 2020.
[77] Verordening (EU) 2016/679, par. 7 en 39.
[78] M.B.A. van Hout, 'Rechtsbescherming in het tijdperk van big data', *WFR 2017/165*, p. 4.
[79] *Beleidsdoorlichting toezicht en opsporing en massale processen Belastingdienst*, bijlage bij *Kamerstukken II* 2017/18, 31935, nr. 44, p. 17.
[80] S. de Jong, 'Denkt u aan uw aangifte? Dank! Liza en Joyce', NRC.nl, 2 maart 2015, https://www.nrc.nl/nieuws/2015/03/10/denkt-u-aan-uw-aangifte-dank-liza-en-joyce-1474025-a399310, bezocht op 12 december 2020.

namelijk gebleken dat individuen doorgaans de standaard instellingen behouden, wat maakt dat veel belastingplichtigen de vooraf ingevulde aangiften zullen accepteren.[81]

Het toepassen van *nudging* sluit naadloos aan bij de gewenste handhavingsstrategie van de fiscus om preventief fouten te voorkomen.[82] *Nudging* in combinatie met *big data* zorgt ervoor dat de fiscus het gedrag van de belastingplichtige effectiever en efficiënter kan beïnvloeden. Het toepassen van gedragsbeïnvloeding kent volgens van Hout echter ook gevaren.[83] Zo zou de scheidslijn tussen *nudging* en manipulatie namelijk flinterdun zijn. Dit komt omdat het de fiscus zelf is die bepaalt welk gedrag 'gewenst' is en tevens de grens trekt wanneer er gedragsbeïnvloeding toegepast mag worden. Volgens van Hout vormt *nudging* dan ook een inbreuk op de autonomie van de burger. Het burgerperspectief dient ten allen tijden centraal te staan bij de vraag of *nudging* geoorloofd is. Ik ben van mening dat de fiscus transparant jegens haar burgers dient te zijn betreffende het gebruik van *nudging* om zo het veronderstelde manipulatieve element van *nudging* te verminderen. Voor de toepassing van *nudging* kent de fiscus geen specifieke wettelijke bevoegdheid, dit terwijl de fiscus zich hierbij bezighoudt met het innerlijk van de belastingplichtigen waarbij een inbreuk op het recht op privacy op de loer ligt.

2.5 Deelconclusie

In dit hoofdstuk stond de vraag centraal welke wettelijke bevoegdheden de fiscus kent voor het gebruik van *big data*. Uit analyse is gebleken dat het begrip '*big data'* geen eenduidige definitie kent, wel zijn drie hoofdkenmerken van *big data* te onderscheiden. Deze kenmerken kunnen worden beschouwd als fasen in een proces, die in zijn geheel bestaat uit: het vergaren van informatie, het analyseren en verwerken van deze informatie en tenslotte het gebruik van *big data*-toepassingen.

De fiscus heeft op basis van de AWR de beschikking over een breed scala aan instrumenten om informatie te vergaren die benodigd is voor het gebruik van *big data*. Zo kan de fiscus gegevens en inlichtingen verkrijgen door middel van de informatieverplichting voor de belastingplichtige en administratieplichtigen, daarnaast is er de mogelijkheid tot gegevensuitwisseling met overheidspartijen. Deze instrumenten kennen een ruime reikwijdte, welke door digitalisering nog breder is geworden. Bij de informatievergaringsverplichting van de belastingplichtige (art. 47 AWR) wordt er een informatiebeschikking afgegeven, waardoor de betrokkene beschikt over voldoende waarborgen ter bescherming van zijn of haar recht op privacy. Dit is anders bij een derdenonderzoek (art. 53 AWR), waarbij de fiscus dwangmiddelen kan inzetten om de gevraagde informatie af te dwingen en de betrokkene hiervoor geen adequate waarborgen toekomt. Daarnaast ontbreekt er ook adequate bescherming voor de betrokkene bij de gegevensuitwisseling tussen overheidsinstanties (art. 67 AWR jo 43c Uitv. Reg AWR) omdat de belangenafweging bij een gegevensuitwisseling niet geschiedt door een onafhankelijke partij.

[81] D. van Hout, 'Gedragsbeïnvloeding in het belastingrecht: are you "nudge"?', *TFR* 2018, nr. 549-550, p. 933.
[82] *Beleidsdoorlichting toezicht en opsporing en massale processen Belastingdienst*, bijlage bij *Kamerstukken II* 2017/18, 31935, nr. 44, p. 17.
[83] M.B.A. van Hout, 'Rechtsbescherming in het tijdperk van big data', *WFR 2017/165,* p. 6.

De toenemende digitalisering bij de fiscus heeft ertoe geleidt dat de hoeveelheid vergaarde data in de afgelopen jaren exponentieel is toegenomen. Deze grote dataset aan gegevens biedt de fiscus de mogelijkheid om hierop *big data*-analyses toe te passen. Waar de fiscus verschillende wettelijke bevoegdheden kent voor het vergaren van *big data*, bestaan er geen nadere wettelijke grondslagen voor de analyse en toepassing van deze data. In de praktijk blijkt de fiscus de wettelijke bepalingen rondom het vergaren van *big data* tevens te gebruiken om beleid te formuleren voor *big data*-analyses en -toepassingen. In dit onderzoek zijn drie *big data*-toepassingen die door de fiscus worden gebruikt aan bod gekomen: *datamining*, *profiling* en *nudging*. Deze toepassingen dragen bij aan een efficiëntere en effectievere uitvoering van controle- en handhavingscapaciteit binnen de fiscus. Echter, kunnen deze toepassingen een grote impact hebben op het recht op privacy van de belastingplichtige. Doordat de fiscus niet transparant is over haar *big data*-analysemethodes, is het voor de belastingplichtige namelijk moeilijk in te schatten wat de exacte impact is van deze toepassingen op zijn of haar privéleven. Ook bestaan er momenteel geen wettelijke waarborgen om misbruik en willekeur vanuit de fiscus tegen te gaan.

Geconcludeerd kan worden dat de burger adequate bescherming nodig heeft om zich te kunnen wapenen tegen de grote en machtige fiscus.
De vraag of het recht op privacy van artikel 8 EVRM deze bescherming biedt wordt besproken in hoofdstuk 4, maar allereest zal in hoofdstuk 3 de regeling van 8 EVRM uiteen worden gezet.

3. Het recht op privacy, artikel 8 EVRM

In hoofdstuk 2 is uiteengezet welke bevoegdheden de fiscus tot zijn beschikking heeft voor het gebruik van *big data*-toepassingen. Bij het uitoefenen van deze bevoegdheden door de fiscus kan er een inbreuk worden gemaakt op het recht op privacy van artikel 8 EVRM. Teneinde te kunnen beoordelen wanneer er sprake is van een inbreuk op artikel 8 EVRM, wordt in dit hoofdstuk achtereenvolgens de reikwijdte (§3.2) en het, in de rechtspraak van de Europees Hof voor de Rechten van de Mens (hierna: EHRM) ontwikkelde, toetsingskader van artikel 8 EVRM (§3.3) besproken. Ten slotte zal in de laatste paragraaf het hoofdstuk worden afgesloten met een deelconclusie.

3.1 Inleiding

Het doel van het EVRM is om een groot aantal rechten en vrijheden van burgers te beschermen tegen inbreuken vanuit de overheid.[84] Het Verdrag omvat enkele mensenrechten, waaronder het recht op privacy dat is neergelegd in artikel 8. Het artikel is tweeledig en luidt als volgt:

"*Lid 1. Een ieder heeft het recht op respect voor zijn privé leven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.*
Lid 2. Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen."[85]

Nederland heeft, als partij bij dit Verdrag, op grond van dit artikel de plicht om het recht op privacy van haar burgers te waarborgen. Lidstaten zijn hierbij vrij om te beslissen hoe deze verplichting tot het recht op privacy in het nationale rechtsstelsel wordt gewaarborgd.[2]

Op grond van artikel 94 GW heeft het recht op privacy rechtstreekse werking in de Nederlandse rechtsorde, waardoor eenieder zich op dit recht kan beroepen. De overheid heeft op grond van het Verdrag zowel een negatieve verplichting: de burger bescherming bieden tegen inmenging van de overheid, als wel een positieve verplichting: actief handelen vanuit de overheid teneinde het recht op privacy van de burger te waarborgen.[86] De fiscus dient, als onderdeel van de overheid, het recht op privacy te respecteren en te waarborgen. In geval de belastingplichtige van mening is dat de fiscus inbreuk maakt op het recht op privacy dan kan deze een klacht indienen bij het Europees Hof voor de Rechten van Mens (hierna: EHRM).

[84] J. Gerards, *EVRM algemene beginselen* , Sdu uitgevers 2011 ,p. 97.
[85] Verg. art. 7 Handvest van de Grondrechten van de Europese Unie, 2000/C 364/01: "Eenieder heeft recht op eerbiediging van zijn privé-leven, zijn familie- en gezinsleven, zijn woning en zijn communicatie.".
[86] F.C.M. Vlemminx, *Het moderne EVRM*, Den Haag: Boom Juridische uitgever 2013, p. 113 e.v..

3.2 Reikwijdte

Het recht op privacy van artikel 8 EVRM waarborgt zoals gezegd het recht op woning, correspondentie, privé-, familie- en gezinsleven. Het EHRM heeft er bewust voor gekozen om dit privacybegrip niet verder te definiëren zodat aan het recht op privacy een ruime reikwijdte toekomt.[87] Dit brengt met zich mee dat de belanghebbende gemakkelijker een beroep kan doen op dit recht. Hierbij dient vermeld te worden dat zowel natuurlijke- als rechtspersonen een beroep kunnen doen op artikel 8 EVRM.[88]

Het recht op privacy is een relatief recht, waardoor het onderworpen kan worden aan beperkingen. Het toetsingskader van de beperkingen is geregeld in het tweede lid van artikel 8, de zogenoemde 'drie-stappentoets'. De uitkomst van deze toets is bepalend voor de vraag of het recht op privacy van de betrokkene mag worden ingeperkt.

Het EHRM heeft in haar rechtspraak de drie-stappentoets nader ingevuld. Hierbij dient vermeld te worden dat het Hof het EVRM dient te interpreteren aan de hand van een *living instrument*-doctrine. Dit betekent dat het Hof het Verdrag dynamisch dient uit te leggen volgens hedendaagse begrippen, waarmee het beoogde doel van artikel 8 EVRM, burgers beschermen tegen inmenging van de overheid, ten alle tijden kan worden gewaarborgd.[89]
De drie-stappentoets van artikel 8 EVRM zal uiteen worden gezet in de volgende paragraaf.

3.3 De drie-stappentoets

Een beperking van het recht op privacy kan worden gerechtvaardigd in geval voldaan wordt aan de cumulatieve drie-stappentoets van artikel 8, tweede lid, EVRM. Allereerst is het een vereiste dat het recht op privacy wordt beperkt. In drie stappen wordt nadien getoetst of de beperking (I) voorzien is bij wet (legaliteitstoets), (II) een legitiem doel nastreeft (legitimiteitstoets) en (III) noodzakelijk wordt geacht in een democratische samenleving (noodzakelijkheidstoets).

De drie-stappentoets, die nader is ingevuld in de rechtspraak van het EHRM, wordt hieronder schematisch weergegeven:

I. Voldoet de beperking aan de legaliteitstoets?
   - Heeft de beperking een wettelijke basis in het nationale recht?
   - Voldoet de grondslag aan het vereiste van voorzienbaarheid?
   - Voldoet de grondslag aan het vereiste van toegankelijkheid?

II. Voldoet de beperking aan de legitimiteitstoets?

III. Voldoet de beperking aan de noodzakelijkheidstoets?
   - Beantwoord de beperking aan de relevantiemaatstaf?
   - Beantwoord de beperking aan de proportionaliteitsmaatstaf?
   - Beantwoord de beperking aan de subsidiariteitsmaatstaf?

Wanneer alle vragen van bovenstaande drieledige toets positief worden beantwoord, dan is er geen inbreuk op het recht op privacy. In de volgende paragrafen zullen respectievelijk de legaliteitstoets, noodzakelijkheidstoets en legitimiteitstoets worden besproken.

---

[87] F.C.M. Vlemminx, *Het moderne EVRM*, Den Haag: Boom Juridische uitgever 2013, p. 91 e.v..
[88] EHRM 16 april 2002, nr. 37971/97, NJ 2003, 452, V-N 2002/47.5 (*Sociétés Colas/France*).
[89] F.C.M. Vlemminx, *Het moderne EVRM*, Den Haag: Boom Juridische uitgever 2013, p. 91 e.v..

3.3.1 Legaliteitstoets

Aan de voorwaarde 'voorzien bij wet', of te wel het legaliteitsbeginsel, wordt voldaan als de beperking een wettelijke grondslag heeft in het nationale recht. Uit de zaak *Sunday Times v. VK* volgt dat het niet relevant is hoe deze wettelijke basis eruitziet, dit kan bijvoorbeeld een wettelijke bepaling, vaste jurisprudentie als ook ongeschreven recht zijn.[90] Hierbij is het wel van belang dat deze rechtsgrondslag daadwerkelijk als doel heeft de betreffende wet te beperken. Een voorbeeld van een zaak waarbij sprake was van een ontoereikende wettelijke grondslag is *P.G. & J.H. t. VK*.[91] Hierbij werd afluisterapparatuur geplaatst op basis van de algemene bevoegdheid van de politie om bewijs te vergaren omdat een wettelijke basis ontbrak. Volgens het Hof was in de casus sprake van een te algemeen geformuleerde bevoegdheidsgrondslag.[8]

Volgens het EHRM stelt het EVRM kwaliteitseisen aan de grondslag die als basis voor de inmenging moet dienen.[92] De grondslag dient te voldoen aan de eisen van voorzienbaarheid en toegankelijkheid, wat inhoudt de betreffende grondslag zodanig geformuleerd moet zijn dat partijen in de mogelijkheid zijn om hierop hun gedrag af te stemmen. Veelal is het gecompliceerd om te beoordelen in welke mate een grondslag het voor een betrokken partij mogelijk maakt om hun gedrag hierop af te stemmen. Voor de wetgever is het namelijk moeilijk om te voorzien in alle mogelijke situaties die zich kunnen voordoen. Om vast te stellen of een grondslag voldoet aan het voorzienbaarheidsvereiste, moeten daarom de aard, inhoud en de context van de bepaling in ogenschouw worden genomen. De grondslag dient daarbij tenminste duidelijkheid te verschaffen over de reikwijdte van de bevoegdheden en dient daarnaast toereikende waarborgen voor de burgers te bevatten om willekeur en misbruik vanuit de overheid tegen te gaan.[93]

Concreet betekent dit dat de betreffende grondslag waaraan de fiscus de bevoegdheid ontleent om *big data* te gebruiken voldoende duidelijkheid dient te verschaffen over welke instanties onder welke condities en omstandigheden beperkende maatregelen mogen uitvoeren. De discretionaire bevoegdheid van de betrokken instellingen en de wijze waarop de partijen deze mogen gebruiken, dienen in de wetgeving voldoende duidelijk te zijn gedefinieerd. Hierbij bestaat er volgens het EHRM een relatie tussen complexiteit van de betreffende technologie en de vereiste mate van nauwkeurigheid van de betreffende juridische grondslag.[94]

Daarnaast kijkt het EHRM bij de beoordeling van de legaliteitstoets naar de kwaliteit van de grondslag en met name of deze betreffende grondslag doeltreffende en adequate waarborgen biedt aan de betrokkene om zich te wapenen tegen mogelijk willekeur en misbruik vanuit de fiscus. Het antwoord op de vraag of er voldoende wettelijke waarborgen bestaan, hangt af van de specifieke situatie waarbij er een inmenging op het recht op privacy is en de daarbij aanwezige wettelijke waarborgen. Volgens het EHRM bestaat er hierbij een verband tussen de ernst van de inmenging op het recht op privacy van de betrokkene en de hoeveelheid en mate van gedetailleerdheid waarmee waarborgen wettelijk zijn vastgelegd.[95]

---

[90] EHRM 26 april 1979, nr. 6538/74 (*Sunday Times v VK),* par. 47.
[91] EHRM 25 september 2001, nr. 44787/98 (*P.G. & J.H. t. VK*).
[92] EHRM 26 april 1979, nr. 6538/74 (*Sunday Times v VK*), par. 49.
[93] EHRM 4 december 2008, nr. 30562/04, *NJ* 2009, 410 (*S. en Marper/Verenigd Koninkrijk*).
[94] EHRM 24 april 1990, nr. 11801/85 (*Kruslin v. France*).
[95] EHRM 2 september 2010, nr. 35623/05 (*Uzun/Duitsland)* par. 66.

Aan het vereiste van toegankelijkheid wordt relatief snel voldaan omdat de grondslag slechts toegankelijk hoeft te zijn voor de personen voor wie deze regels gelden, wat al kan worden bereikt door deze te publiceren op het internet.[96]

In geval een beperking niet aan de legaliteitstoets voldoet, dan wordt het recht op privacy van artikel 8 EVRM geschonden. Het EHRM komt dan vervolgens niet meer toe aan de beoordeling van de beperking aan de legitimiteits- dan wel noodzakelijkheidstoets.[97] Wanneer de beperking wel aan de legaliteitstoets voldoet, zal de beperking vervolgens door het EHRM nog aan de legitimiteits- en noodzakelijkheidstoets worden onderworpen.

3.3.2 Legitimiteitstoets

Naast dat een beperking dient te beantwoorden aan de legaliteitstoets, moet de beperking tevens een legitiem doel nastreven. De limitatief geformuleerde doelcriteria in artikel 8, tweede lid, EVRM zijn: "in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen". Volgens de literatuur zijn deze doelcriteria breed geformuleerd en tevens divers, waardoor al snel aan de legitimiteitstoets wordt voldaan.[98] Uit de rechtspraak van het EHRM volgt dan ook dat de legitimiteitstoets geen grote betekenis toekomt in de beoordeling of er sprake is van inbreuk op het recht op privacy.[99]

De fiscus beroept zich bij de bevoegdheden om *big data*-analyses en -toepassingen uit te voeren, op grond van artikel 47, 53 en 55 AWR, doorgaans op het doelcriteria: 'economisch welzijn van het land'. Uit de rechtspraak volgt dat dit doelcriteria in fiscale zaken vrijwel altijd wordt geaccepteerd.[100] De enkele constatering dat de beperking een legitiem doel nastreeft, is onvoldoende om een beperking op het recht op privacy te rechtvaardigen. Er dient een belangenafweging gemaakt te worden tussen het betreffende legitieme doel en het recht op privacy van de betrokkene. Deze afweging vindt plaats in de noodzakelijkheidstoets.

3.3.3 Noodzakelijkheidstoets

Wanneer een beperking van het recht op privacy de toetsen van legaliteit en legitimiteit heeft doorstaan, zal de beperking door het EHRM onderworpen worden aan de noodzakelijkheidstoets. Bij de beoordeling door het EHRM of er voldoende waarborgen bestaan voor de betrokkene om zich te wapenen tegen willekeur en misbruik vanuit de fiscus, komt de overweging van het EHRM of voldaan is aan de legaliteitstoets dikwijls overeen met de beoordeling of een beperking voldoet

[96] J.Gerards, *EVRM algemene beginselen* , Sdu uitgevers 2011 ,p. 120; Dit volgt o.a. uit: EHRM 26 april 1979, nr, 6538/74 (*Sunday Times t. VK*) en EHRM 28 maart 1990, nr. 10890/84 (*Groppera Radio AG e.a. t. Zwitserland*).
[97] J. Vande Lanotte & Y. Haeck, *Handboek EVRM Deel 2 Artikelsgewijze Commentaar*, Intersentia 2004, p. 717.
[98] Zie o.a.: G.T.K. Meussen & C.M. Dijkstra, 'The Law ought to limit every Power it gives: art. 53 AWR versus art. 8 EVRM (recht op privacy)' *WFR 2016/37* en F.M.C. Vlemminx, *Het moderne EVRM*, p. 175.
[99] EHRM 1 juli 2014, nr. 43835/11 (*S.A.S./Frankrijk*), par. 114. Het Hof stelt: "The Court's practice is to be quite succinct when it verifies the existence of a legitimate aim".
[100] Zie o.a.: HR 24 februari 2017, ECLI:NL:HR:2017:310, Hof Den Bosch 19 augustus 2014, ECLI:NL:GHSHE:2014:2803, en EHRM 14 maart 2013, 24117/08 (*Bernh Larsen Holding*).

aan de noodzakelijkheidstoets.[101] De waarborgen dienen namelijk in de wet te zijn verankerd (zie §3.3.1), maar dienen tevens ook adequaat te zijn om willekeur en misbruik door de fiscus te voorkomen. Laatstgenoemde maakt in beginsel deel uit van de noodzakelijkheidstoetsing.

De noodzakelijkheidseis is expliciet terug te vinden in de bewoording van artikel 8, tweede lid, EVRM: "in een democratische samenleving noodzakelijk". Uit de vaste rechtspraak van het EHRM volgt dat een beperking als 'noodzakelijk' dient te worden aangemerkt als er een "dringend maatschappelijk belang" bestaat en de maatregel proportioneel is om deze beoogde doelstelling te bereiken.[102] Bij de beantwoording van de vraag of een beperking 'noodzakelijk is in een democratische samenleving', kent het EHRM de lidstaten een beoordelingsruimte toe, de zogenoemde: *margin of appreciation*. De reikwijdte van deze *margin of appreciation* kan verschillen en hangt onder andere af van het belang van de betrokken partij, de aard van de betreffende verdragsbepaling en de doelstelling en aard van de beperking. De *margin of appreciation* is ruim in geval uit de rechtspraak van de lidstaten blijkt dat er geen consensus bestaat over het gewicht dat aan een concreet belang toekomt, dan wel op welke manier het belang het meest optimaal beschermd kan worden. Een voorbeeld waarbij lidstaten een ruime *margin of appreciation* hebben is bij een maatregel die als doel heeft om de nationale veiligheid te bescherming.[103] Aan de andere kant is de *margin of appreciation* juist kleiner wanneer het betreffende recht van essentieel belang is voor een doeltreffende invulling van de fundamentele rechten van een burger. Met betrekking tot een maatregel die als doel heeft om het economisch welzijn van het land te beschermen (het doelcriteria waar de fiscus zich in het algemeen op beroept) hebben lidstaten doorgaans een kleinere *margin of appreciation*.[104] Het gevolg van deze kleinere *margin of appreciation* is dat de toetsing van het Hof inzake de aangevoerde motivatie van de fiscus voor de beperking van het recht op privacy strenger is.[105]

De proportionaliteitstoets speelt een belangrijke rol bij de beantwoording van de vraag of een beperking 'noodzakelijk is in een democratische samenleving'. Hierbij dient te worden nagegaan of een inmenging proportioneel is aan de beoogde doelstelling. Zoals in de voorgaande paragraaf vermeld, dienen de bevoegdheden van artikel 47, 53 en 55 AWR te voldoen aan een legitiem doel. De resterende vraag is of er een juiste verhouding ('fair balance') bestaat tussen de mate van de beperking op recht op privacy en de beoogde doelstelling. Bij deze beoordeling dient er een belangenafweging te worden gemaakt tussen het belang van de betrokken partij en het maatschappelijke belang, waarbij het subsidiariteitsbeginsel deel van kan gaan uitmaken in deze belangenafweging.

Uit de rechtspraak van het EHRM volgt dat verschillende factoren van belang zijn bij de proportionaliteitstoets, waaronder: de reikwijdte van de inmenging, de aard van de informatie, de status van het individu en tenslotte of er sprake is van adequate waarborgen voor de betrokkene.

[101] Dit was o.a. het geval bij EHRM 4 december 2008, nr. 30562/04, *NJ* 2009, 410 (*S. en Marper/Verenigd Koninkrijk*), waar het EHRM de beoordeling of de waarborgen voldoen aan de legaliteitstoets bespreekt bij de noodzakelijkheidstoetsing.
[102] EHRM 7 december 1976, nr. 6593/72 (*Handyside*), par. 48.
[103] EHRM 26 maart 1987, nr. 9248/81 (*Leander v. Sweden*), par. 59.
[104] EHRM 14 maart 2013, 24117/08 (*Bernh Larsen Holding)*, par. 99.
[105] F.C.M. Vlemminx, *Het moderne EVRM*, Den Haag: Boom Juridische uitgever 2013, p. 191.

3.4 Deelconclusie

In dit hoofdstuk is het juridische kader van dit onderzoek behandeld, waarbij de vraag centraal staat hoe het recht op privacy van artikel 8 EVRM is vormgegeven. Hierbij is eerst ingegaan op de reikwijdte van artikel 8 EVRM en vervolgens is de drie-stappentoets uiteengezet. Het EHRM heeft er bewust voor gekozen om het privacybegrip niet verder te definiëren zodat het recht op privacy een ruime reikwijdte toekomt. Dit brengt met zich mee dat de belanghebbende gemakkelijk een beroep kan doen op dit recht. Bij de beoordeling of een inbreuk van het recht op privacy gerechtvaardigd kan worden, toetst het Hof de beperking aan de volgende drie cumulatieve eisen: de legaliteitstoets, legitimiteitstoets en de noodzakelijkheidtoets.

Uit de rechtspraktijk volgt dat aan de legitimiteitstoets geen grote betekenis toekomt in de beoordeling of er sprake is van inbreuk op het recht op privacy omdat de wettelijke doelcriteria breed en divers zijn geformuleerd. De fiscus beroept zich bij de bevoegdheden om *big data*-analyses en -toepassingen uit te voeren doorgaans op het doelcriteria: 'economisch welzijn van het land'. Uit de rechtspraak volgt dat dit doelcriteria in fiscale zaken vrijwel altijd wordt geaccepteerd. De enkele constatering dat de beperking een legitiem doel nastreeft, is onvoldoende om een beperking op het recht op privacy te rechtvaardigen. Er dient daarom een belangenafweging gemaakt te worden tussen het betreffende legitieme doel en het recht op privacy van de betrokkene.

Daarentegen vervult het legaliteitsvereiste wel een belangrijke rol in deze beoordeling en dan met name de eis van voorzienbaarheid, inhoudende dat de betreffende grondslag zodanig geformuleerd dient te zijn dat partijen in de mogelijkheid zijn om hierop hun gedrag af te stemmen. De grondslag dient daarbij ook duidelijkheid te verschaffen over de reikwijdte van de bevoegdheden en dient daarnaast toereikende waarborgen voor de burgers te bevatten om willekeur en misbruik vanuit de overheid tegen te gaan. Of er voldoende wettelijke waarborgen bestaan, hangt af van de specifieke situatie. Volgens het EHRM bestaat er hierbij een verband tussen de ernst van de inmenging op het recht op privacy van de betrokkene en de hoeveelheid en mate van gedetailleerdheid waarmee waarborgen wettelijk zijn vastgelegd.

In de praktijk komt de grootste betekenis toe aan de noodzakelijkheidstoets. Een beperking is als 'noodzakelijk' aan te merken wanneer er een "dringend maatschappelijk belang" bestaat en de maatregel proportioneel is om deze beoogde doelstelling te bereiken. Bij de beantwoording van de vraag of een beperking 'noodzakelijk is in een democratische samenleving', kennen de lidstaten een *margin of appreciation*. Met betrekking tot een maatregel die als doel heeft om het economisch welzijn van het land te beschermen hebben lidstaten doorgaans een kleine(re) *margin of appreciation*. Het gevolg van deze kleine *margin of appreciation* is dat de toetsing van het Hof inzake de aangevoerde motivatie vanuit de fiscus voor de beperking van het recht op privacy strenger is. Daarnaast speelt bij deze toets de proportionaliteitseis een belangrijke rol, waarbij nagegaan wordt of een inmenging proportioneel is aan de beoogde doelstelling. Hierbij dient er een belangenafweging te worden gemaakt tussen het belang van de betrokken partij en het maatschappelijke belang, waarbij het subsidiariteitsbeginsel deel van kan gaan uitmaken in deze belangenafweging.

4. Het gebruik van big data door de fiscus en de eventuele strijd met artikel 8 EVRM

Nadat in hoofdstuk 2 de wettelijke bevoegdheden van de fiscus voor het gebruik van *big data* is besproken en in hoofdstuk 3 artikel 8 EVRM uiteen is gezet, wordt in dit hoofdstuk ingegaan op de vraag of het gebruik *big data*-toepassingen door de fiscus een rechtmatige inmenging vormt op het recht privacy. Alvorens getoetst kan worden aan de wettelijke vereisten van artikel 8, tweede lid, EVRM, dient allereerst te worden vastgesteld of het gebruik van *big data*-toepassingen door de fiscus op grond de bevoegdheden uit de AWR een inmenging vormt op artikel 8 EVRM (wordt behandeld in §4.1). Wanneer hiervan sprake is, dan dient vervolgens gekeken te worden naar de ernst is van deze inmenging (wordt behandeld in §4.2). Het bepalen van de ernst van de inmenging is relevant voor de beoordeling of de AWR toereikende waarborgen biedt ter bescherming van de privacy van de betrokkene. Het bieden van een adequate bescherming aan de betrokkene is van belang om een inbreuk op het recht op privacy te kunnen rechtvaardigen.

4.1 Reikwijdte artikel 8 EVRM

De fiscus gebruikt de informatievergaringsbevoegdheden van artikel 47 tot en met 56 AWR als grondslag bij het verwerken van (persoons)gegevens. Wil er sprake zijn van een inmenging dan dient er vastgesteld te worden of deze verwerking door de fiscus onder de bescherming valt van artikel 8 EVRM. Allereerst dient te worden bepaald of de bescherming van persoonsgegevens binnen de werkingssfeer van artikel 8 EVRM valt. Uit de rechtspraak van het EHRM volgt dat aan het begrip: 'persoonsgegevens' een ruime interpretatie toekomt, namelijk alle gegevens betreffende een identificeerbaar individu.[106] Daarnaast valt volgens het EHRM het vergaren en opslaan van persoonsgegevens binnen de reikwijdte van artikel 8 EVRM.[107] Omdat de fiscus deze persoonsgegevens verwerkt valt deze handeling onder het toepassingsgebied van artikel 8 EVRM.

4.2 De ernst van de inmenging

Nu vast is komen te staan dat bij het gebruik van *big data*-toepassingen door de fiscus sprake is van een inmenging op artikel 8 EVRM, dient er te worden bepaald wat de mate en de ernst van deze inmenging is. De mate van de inmenging is bepalend bij de vraag of er voldoende waarborgen bestaan om individuen te beschermen tegen overheidsmacht. Des te ernstiger de inmenging, des te steviger de wettelijke waarborgen dienen te zijn.[108]

De ernst van deze inmenging, kan worden bepaald aan de hand van de volgende factoren: de context van de dataverwerking, de aard van de informatie en de uitkomsten van deze verwerking.[109] Bij de context van de dataverwerking kijkt het EHRM onder andere naar de transparantie van de verwerking (of de betrokkene op de hoogte is gesteld van de verwerking), de

[106] EHRM 4 mei 2000, 28341/95 (*Rotaru/Roemenië)*, par. 43.
[107] Idem.
[108] Hoge Raad 4 april 2017, ECLI:NL:2017:584, 4 april 2017, par. 2.8.
[109] EHRM 4 december 2008, nr. 30562/04 (*S. en Marper/VK*), par. 67.

redelijke privacyverwachting van de betrokkene en naar de omvang van de verwerking.[110] Hierbij bestaat er een verband tussen de context van de verwerking en de aard van de informatie. Naarmate er meer privacygevoelige gegevens worden gebruikt, wordt het gewicht van het individuele belang verzwaard.[111] De digitalisering van de afgelopen jaren heeft ervoor gezorgd dat de fiscus op grote schaal privacygevoelige informatie kan vergaren en analyseren. De uitkomsten van deze analyses gebruikt de fiscus vervolgens bij de inzet van *big data*-toepassingen zoals *profiling* en *nudging*. Door gebruik te maken van deze toepassingen wordt het steeds onwaarschijnlijker dat er hierbij geen ernstige inbreuk wordt gemaakt op het recht op privacy.[112]

De fiscus maakt bij haar *big data*-toepassingen gebruik van privacygevoelige informatie die afkomstig is uit een veelvoud van bronnen, hierdoor is het voor de fiscus mogelijk om een volledig risicoprofiel van de belastingplichtige te schetsen. Zoals in hoofdstuk 2 vermeld, is de fiscus niet transparant over deze toepassingen en de daarbij gehanteerde risicomodellen tegenover belastingplichtigen. De belastingplichtige is hierdoor bijvoorbeeld niet op de hoogte met welke bedrijven en/of personen deze gegevens gedeeld worden dan wel voor hoe lang de fiscus deze gegevens archiveert. Dit terwijl, in het geval de belastingplichtige op een geheime 'zwarte lijst' van de fiscus staat waarbij sprake is van een verhoogt risicoprofiel, het een grote impact kan hebben op het recht op privacy van de belastingplichtige.[113] Bovengenoemde aspecten leiden tot de conclusie dat er bij het gebruik van *big data*-toepassingen door de fiscus op grond van de bevoegdheden van de AWR sprake is van een zeer ingrijpende inmenging op het recht op privacy.[114]

Een inmenging op het recht van privacy is slechts toegestaan wanneer voldaan wordt aan de drie-stappentoets. Deze toets zal in de volgende paragraaf worden uitgewerkt.

[110] L. A. Bygrave, 'Data Protection Pursuant to the Right to Privacy in Human Rights Treaties', *International Journal of Law and Information Technology* 1998/6.3, p. 269.
[111] EHRM 13 november 2012, nr. 24029/07 (*MM/VK*), par. 200.
[112] B. Schermer, 'The limits of privacy in automated profiling and data mining', *Computer Law & Security Review* 2011/27.1, p. 50.
[113] Een situatie waarbij dit het geval was is de recente 'toeslagenaffaire'.
[114] Deze conclusie wordt onderschreven door de Rechtbank Den Haag in de recente SyRi-zaak, waarbij onder andere de rechtmatigheid van het koppelen van data en *profiling* door de overheid centraal stond; Rb. Den Haag 5 februari 2020, ECLI:NL:RBDHA:2020:865.

4.3 De uitwerking van de drie-stappentoets in de rechtspraak

Nu ik tot de constatering ben gekomen dat het gebruik van *big data*-toepassingen door de fiscus een inmenging oplevert op artikel 8 EVRM, zal ik in deze paragraaf beoordelen of deze inmenging te rechtvaardigen is. Hierbij dient de inmenging te voldoen aan de cumulatieve drie-stappentoets van artikel 8, tweede lid, EVRM. In de volgende paragrafen zullen respectievelijk de legaliteitstoets (§4.3.1) en de legitimiteits- en noodzakelijkheidstoets (§4.3.2) worden besproken.

4.3.1 Legaliteitstoets

Een beperking voldoet aan de legaliteitstoets ingeval de inmenging een wettelijke basis heeft in het nationale recht, welke voldoet aan de vereisten van toegankelijkheid en voorzienbaarheid. Zoals reeds, in hoofdstuk 2, besproken mag de fiscus op basis van de wettelijke informatievergaringsbevoegdheden (artikel 47 tot en met 56 AWR) alle gegevens en inlichtingen vergaren die 'van belang kan zijn' voor het heffen van belasting. De fiscus komt met deze open norm een vergaande bevoegdheid toe om informatie op een grootschalig wijze te vergaren. Uit de praktijk blijkt dat de fiscus deze wettelijke bepalingen gebruikt om beleid te formuleren voor *big data*-analyses en -toepassingen.

In de ANPR-arresten heeft de Hoge Raad bepaald dat er een voldoende specifieke wettelijke basis vereist is bij elke fase van het *big data*-proces (vergaren, verwerken en gebruik) waarbij het recht op privacy van de betrokkene in het geding is.[115] Op basis van de betreffende bevoegdheden van de AWR voert de fiscus systematische informatieverwerkingen uit aan de hand waarvan de fiscus onder andere profileert en gedragsbeïnvloeding toepast, welke een ingrijpende inmenging vormen op het recht op privacy van de belastingplichtige. Zoals eerder aangegeven is in de AWR niets geregeld over het gebruik van *big data* door de fiscus, wat maakt dat deze bepalingen een onvoldoende specifieke wettelijke basis bieden om zo'n ingrijpende schending van het recht op privacy te rechtvaardigen. Aan het vereiste dat een beperking een wettelijke basis dient te hebben in het nationale recht, wordt hier derhalve niet voldaan.

De bevoegdheden op basis waarvan de fiscus *big data* gebruikt zijn neergelegd in de AWR, waardoor aan het vereiste van toegankelijkheid wordt voldaan. Wil daarnaast ook voldaan zijn aan het voorzienbaarheidsvereiste, dan dienen de betreffende artikelen uit de AWR zodanig te zijn geformuleerd dat partijen in de mogelijkheid zijn om hierop hun gedrag af te stemmen. De grondslag dient tenminste duidelijkheid te verschaffen over de reikwijdte van de bevoegdheden en toereikende waarborgen voor de burgers om willekeur en misbruik vanuit de overheid tegen te gaan. Dat heldere en gedetailleerde wetgeving belangrijk is, volgt verder uit de zaak *Huvig/France* waarbij het Europees Hof aangaf dat er een verband bestaat tussen de geavanceerde technologie en de gedetailleerdheid van de wetgeving.[116] Kortom, des te ingrijpender de inmenging op het recht op privacy, des te nauwkeuriger de wetgeving dient te vermelden voor welke doeleinden informatie mag worden gebruikt. De AWR faalt hierin om drie redenen.[117] Allereerst is in de AWR niet nauwkeurig genoeg beschreven wat voor soort gegevens kunnen worden opgevraagd, waardoor de informatie die de fiscus gebruikt vrijwel onbeperkt is. Daarnaast is in de AWR niet

[115] Hoge Raad 24 februari 2017, ECLI:NL:HR:2017:288, par. 2.3.5.
[116] EHRM 24 april 1990, 11105/84, par. 33. (*Huvig/France*).
[117] Hof 's-Hertogenbosch 19 augustus 2014, ECLI:NL:GHSHE:2014:2803, m.nt. T.H.A. Wisman.

concreet beschreven in welke gevallen de fiscus handelingen kan en mag verrichten, waaronder bijvoorbeeld: het koppelen van informatie, profileren of *nudgen.* Tenslotte zijn er in de AWR geen waarborgen opgenomen om de burger te beschermen tegen willekeur en misbruik vanuit de fiscus.

De fiscus gebruikt de bevoegdheden in de AWR om op grote schaal systematische analyses uit te voeren. Om de burger bescherming te bieden tegen misbruik en willekeur vanuit de fiscus, heeft het Europese Hof in de *Weber & Saravia*-zaak bepaald dat er enkele minimumwaarborgen in de wet dienen te worden opgenomen.[118] Zo moeten er procedures worden opgenomen in de wettelijke grondslag rondom het doorgeven van informatie aan andere partijen en het verwijderen of vernietigen van informatie wanneer deze niet meer benodigd is. Volgens het Hof van Justitie van de Europese Unie is de behoefte aan dergelijke waarborgen des te groter in geval persoonsgegevens op systematische wijze worden verwerkt en de kans daardoor groter is dat deze informatie onrechtmatig wordt ingezien.[119] Zoals bovenstaand vermeld, voorziet de AWR niet in deze minimumwaarborgen waardoor deze wettelijke bepalingen niet voldoen aan de rechtspraak van het EHRM. Dat het ontbreken van (voldoende) wettelijke waarborgen bij het gebruik van *big data* serieuze gevolgen met zich mee kan brengen, is pijnlijk duidelijk geworden in de toeslagenaffaire. Doordat de fiscus niet transparant was jegens burgers over het gebruik van *big data*, zijn ±250.000 belastingplichtigen als (potentiële) fraudeurs bestempeld en behandeld, zonder dat de belastingplichtigen zich hiertegen konden verzetten.[120] Immers, deze belastingplichtigen waren niet op de hoogte dat ze op de 'zwarte lijst' van de fiscus stonden.
Zoals vermeld in §4.2, kennen de bevoegdheden in de AWR een ruime reikwijdte omdat deze bevoegdheden door de fiscus worden gebruikt bij het vergaren en tevens het gebruik van *big data*. Deze bevoegdheden zijn niet omkleed met (voldoende) wettelijke waarborgen, waardoor er vastgesteld kan worden dat niet voldaan wordt aan het voorzienbaarheidsvereiste.

Al met al kan worden geconcludeerd dat de betreffende inmenging niet beantwoordt aan de legaliteitstoets. De inmenging kent namelijk geen wettelijke basis in het nationale recht en tevens wordt er niet voldaan aan het vereiste van voorzienbaarheid omdat de bevoegdheden van de AWR namelijk zeer ruim zijn geformuleerd, terwijl deze grondslagen niet voorzien in minimumwaarborgen. Daarbij is door digitalisering de reikwijdte van de huidige bevoegdheden van de fiscus omtrent het gebruik van *big* data dermate opgerekt, waardoor ik mij afvraag of dit nog te rijmen valt met de aanvankelijke bedoeling van de wetgever.

4.3.2 Legitimiteitstoets en noodzakelijkheidstoets

In deze paragraaf worden de overige twee voorwaarden voor een legitieme inbreuk op het recht op privacy van artikel 8 EVRM behandeld: de legitimiteitstoets en de noodzakelijkheidstoets. Deze toetsen worden gezamenlijk behandeld aangezien de noodzakelijkheid van de maatregel verband houdt met het doel dat deze maatregel dient. Een beperking dient als 'noodzakelijk' te worden aangemerkt als er een "dringend maatschappelijk belang" bestaat en de maatregel proportioneel is om deze beoogde doelstelling te bereiken.

[118] EHRM 29 juni 2016, nr. 54934/00 (*Weber & Saravia/Duitsland)*, par. 101.
[119] EHRM 4 december 2008, 30562/04 (*S en Marper/VK*); EHRM 18 april 2013, 19522/09, par. 25 (*M.K./Frankrijk*).
[120] *Kamerstukken II* 2019-20, 31066, nr. 632, p. 4.

De wetgever heeft de fiscus enkele onderzoeksbevoegdheden (artikelen 47 t/m 56 AWR) toegekend om ervoor te zorgen dat de fiscus tot een correcte belastingheffing kan komen.[121] Het belang van een correcte belastingheffing valt te scharen onder het in het artikel 8, tweede lid, EVRM genoemde doelcriteria: 'economisch welzijn van het land'. Uit analyse van de rechtspraak is gebleken dat de fiscus zich in fiscale zaken doorgaans beroept op dit doelcriteria, waarbij dit beroep doorgaans wordt geaccepteerd.[122] Met betrekking tot een maatregel die als doel heeft om het economisch welzijn van het land te beschermen hebben lidstaten doorgaans een kleine *margin of appreciation*.[123] Het gevolg van deze kleine *margin of appreciation* is dat de toetsing van het Hof inzake de aangevoerde motivatie van de fiscus voor de beperking van het recht op privacy strenger is.[124] De enkele constatering dat de beperking een legitiem doel nastreeft, is onvoldoende om een beperking op het recht op privacy te rechtvaardigen. Er dient een belangenafweging gemaakt te worden tussen het betreffende legitieme doel (correcte belastingheffing) en het recht op privacy van de betrokkene. Deze afweging vindt plaats bij de toetsing van de noodzakelijkheid.

Bij de toetsing van de noodzakelijkheid is relevant of er bij gebruik van *big data* door de fiscus sprake is van een dringend maatschappelijk belang en indien hiervan sprake is, of het gebruik van *big data*-toepassingen op grond van de AWR evenredig is met het beoogde doel: correcte belastingheffing. Zonder de in de AWR neergelegde onderzoeksbevoegdheden van de fiscus en de verplichtingen die daaruit voortvloeien, zou de fiscus afhankelijk zijn van de vrijwillige medewerking van de betrokkenen. Het behoeft geen betoog dat de belastinginkomsten in dergelijke situatie ontoereikend zouden zijn. De behoefte van de betreffende bevoegdheden in de AWR wordt ingegeven door de wens van het kabinet om de in het beginsel aanwezige kennisongelijkheid tussen de fiscus en de burger te compenseren, dit alles in het kader van het maatschappelijk belang: een effectieve belastingheffing.[125]

Het gebruik van *big data* door de fiscus op grond van de AWR voldoet aan de beginselen van proportionaliteit en subsidiariteit in geval er een *fair balance* aanwezig is tussen de doelstellingen van de AWR en de inmenging die betreffende artikelen van de AWR maakt op artikel 8 EVRM. Bij deze belangenafweging zijn de uitkomsten van de SyRi-zaak relevant, waarbij de rechtbank expliciet stil heeft gestaan bij de digitalisering van de afgelopen jaren. Op grond van deze ontwikkeling is de rechtbank de mening toegedaan dat de overheid een 'bijzondere verantwoordelijkheid' heeft bij de inzet van *big data*-technologieën.[126] De toepassing van dergelijke systemen kan er namelijk toe leiden dat de privacy van de belastingplichtige ernstig wordt verstoord, waarbij het voor de belastingplichtige doorgaans onduidelijk is wat de gevolgen voor hem of haar zijn bij toepassing van *big data*-technologieën. Daarom legt de rechtbank de overheid deze bijzondere verantwoordelijkheid op. Deze verantwoordelijkheid van de fiscus ziet op het vinden van een *fair balance* tussen de voordelen die deze technologieën met zich meebrengen en de mate van inbreuk op het recht op privacy. Deze *fair balance* kan worden

[121] *Kamerstukken II* 1986/87, 19393, nr. 150b, p. 2-3.
[122] Zie o.a.: HR 24 februari 2017, ECLI:NL:HR:2017:310, Hof Den Bosch 19 augustus 2014, ECLI:NL:GHSHE:2014:2803, en EHRM 14 maart 2013, 24117/08 (*Bernh Larsen Holding*).
[123] EHRM 14 maart 2013, 24117/08 (*Bernh Larsen Holding)*, par. 99.
[124] F.C.M. Vlemminx, *Het moderne EVRM*, Den Haag: Boom Juridische uitgever 2013, p. 191.
[125] *Kamerstukken II* 1979/80, 16180, nr, 1-2.
[126] Rb. Den Haag 05-02-2020, ECLI:NL:RBDHA:2020:865, par. 6.6.

gecreëerd door middel van waarborgen op te nemen in de wet om misstanden en willekeur van de fiscus te voorkomen. Waar bij de legaliteitstoets al stil is gestaan bij het belang van adequate waarborgen, heeft de rechtbank in de SyRi-uitspraak dit belang eveneens onderstreept voor de noodzakelijkheidstoetsing. Volgens de rechtbank is het namelijk voor betrokkene niet inzichtelijk welke risicomodellen worden gehanteerd bij de toepassing van SyRi, waardoor het voor de betrokkene onmogelijk is om na te gaan wanneer deze als potentieel fraudeur wordt bestempeld. Daarnaast is de rechtbank van mening dat er onvoldoende waarborgen bestaan om het recht op privacy van de betrokkene te kunnen beschermen wanneer deze in relatie worden gezien tot de risicomodellen die bij het SyRi-systeem worden gehanteerd, zo bestaat er vooraf geen noodzakelijkheidstoetsing door een onafhankelijke derde. Dit alles maakt dat de rechtbank het SyRi-systeem buitenproportioneel acht voor het beoogde doel van de overheid om fraude te bestrijden.[127] Het gevolg van de SyRi-uitspraak is dat de overheid dit systeem, in zijn huidige vorm, niet meer mag toepassen en tevens heeft deze uitspraak ook gevolgen voor andere *big data*-toepassingen waarbij door de overheid aan *profiling* en/of *nudging* wordt gedaan. De 'bijzondere verantwoordelijkheid' die de overheid volgens de rechtbank toekomt, maakt dat er bij andere *big data*-toepassingen door de overheid eveneens adequate waarborgen dienen te bestaan, wat bijvoorbeeld kan worden bereikt door voldoende transparantie ten aanzien van de betreffende toepassing en voorafgaande noodzakelijkheidstoetsing door een onafhankelijke derde. Dat deze discussie omtrent adequate waarborgen relevant is, blijkt wel uit de 'toeslagenaffaire'. Kortom, kan uit SyRi-zaak worden opgemaakt dat er voor *big data*-analyse en -toepassingen momenteel onvoldoende adequate waarborgen bestaan. Mijns inziens, wordt er door de SyRi uitspraak paal en perk gesteld aan de *big data*-analyse en -toepassingen van de fiscus.

Vastgesteld kan worden dat bij het gebruik van *big data*-toepassingen door de fiscus niet wordt voldaan aan de noodzakelijkheidstoets. De *big data*-toepassingen waarmee een correcte en effectieve belastingheffing wordt beoogd, dient evenredig te zijn aan de inmenging op het recht op privacy die deze toepassingen met zich meebrengen. De digitalisering van de afgelopen jaren en de veelvoud aan beschikbare data hebben ervoor gezorgd dat de fiscus op een efficiënte(re) manier belasting kan heffen, echter dient er door de fiscus bij *big data*-toepassingen de proportionaliteit niet uit het oog te worden verloren. De fiscus heeft bij inzet van *big data*-toepassingen een bijzondere verantwoordelijkheid om de burger bescherming te bieden tegen misbruik en willekeur, wat kan worden bewerkstelligd door te voorzien in adequate wettelijke waarborgen. Deze waarborgen ontbreken op dit moment. Ik ben dan ook van mening dat het de hoogste tijd is voor nieuwe wetgeving waarin waarborgen en tevens begrenzingen zijn opgenomen.

[127] Rb. Den Haag 05-02-2020, ECLI:NL:RBDHA:2020:865, par. 6.7 e.v..

4.4 Deelconclusie

In dit hoofdstuk is het gebruik van big data door de fiscus getoetst aan het recht op privacy. Centraal stond hierbij de vraag in hoeverre het gebruik van big data door de fiscus een inbreuk vormt op artikel 8 EVRM.

De fiscus maakt bij haar *big data*-toepassingen gebruik van privacygevoelige informatie die afkomstig is uit een veelvoud van bronnen, waardoor het voor de fiscus mogelijk is om een volledig risicoprofiel te schetsen van de belastingplichtige. De fiscus is niet transparant jegens haar burgers betreffende deze toepassingen, waardoor de belastingplichtige niet op de hoogte is met welke bedrijven en/of personen deze gegevens worden gedeeld dan wel voor hoe lang de fiscus deze gegevens archiveert, dit terwijl de impact op de privacy van de belastingplichtige groot kan zijn. Geconcludeerd kan worden dat bij het gebruik van *big data*-toepassingen door de fiscus op grond van de bevoegdheden van de AWR sprake is van een zeer ingrijpende inmenging op het recht op privacy. Deze inmenging is slechts toegestaan in geval deze voorzien is bij wet, een legitiem doel nastreeft en noodzakelijk wordt geacht in een democratische samenleving.

Wil een beperking voldoen aan de legaliteitstoets dan dient de inmenging een wettelijke basis te hebben in het nationale recht, welke voldoet aan de vereisten van toegankelijkheid en voorzienbaarheid. Op basis van de bevoegdheden die zijn neerlegd in de AWR voert de fiscus systematische informatieverwerkingen uit aan de hand waarvan de fiscus onder andere profileert en gedragsbeïnvloeding toepast. Deze toepassingen kunnen een ingrijpende inmenging vormen op het recht op privacy van de belastingplichtige. In de AWR is niets geregeld over het gebruik van *big data* door de fiscus, wat maakt dat deze bepalingen een onvoldoende specifieke wettelijke basis bieden om zo'n ingrijpende schending van het recht op privacy te rechtvaardigen. Aan het vereiste dat een beperking een wettelijke basis dient te hebben in het nationale recht, is derhalve niet voldaan. Wil daarnaast voldaan zijn aan het voorzienbaarheidsvereiste, dan dient de grondslag tenminste duidelijkheid te verschaffen over de reikwijdte van de bevoegdheden en toereikende waarborgen voor de burgers om willekeur en misbruik vanuit de overheid tegen te gaan. De AWR faalt hierin om drie redenen, allereerst is in de AWR niet nauwkeurig genoeg beschreven wat voor soort gegevens kunnen worden opgevraagd, waardoor de informatie die de fiscus gebruikt vrijwel onbeperkt is. Daarnaast is in de AWR niet concreet beschreven in welke gevallen de fiscus handelingen kan en mag verrichten en tenslotte zijn er in deze wettelijke bepalingen geen waarborgen opgenomen om de burger te beschermen tegen willekeur en misbruik vanuit de fiscus. Al met al kan worden geconcludeerd dat de betreffende inmenging niet beantwoordt aan de legaliteitstoets.

Om een inmenging op het recht op privacy te rechtvaardigen dient naast de legaliteitstoets eveneens te worden voldaan aan de legitimiteits- en noodzakelijkheidstoets. De in artikel 8, tweede lid, EVRM genoemde doelcriteria zijn breed geformuleerd en tevens divers, waardoor aan de legitimiteitstoets al snel wordt voldaan. Het doelcriteria: 'economisch welzijn van het land' wordt in fiscale zaken vrijwel altijd geaccepteerd. Echter, de enkele constatering dat de beperking een legitiem doel nastreeft, is onvoldoende om een beperking op het recht op privacy te rechtvaardigen. Er dient een belangenafweging gemaakt te worden tussen het betreffende legitieme doel (correcte belastingheffing) en het recht op privacy van de betrokkene. Deze afweging vindt plaats bij de toetsing van de noodzakelijkheid. Bij de toetsing van de noodzakelijkheid is relevant of er bij

gebruik van *big data* door de fiscus sprake is van een dringend maatschappelijk belang en indien hiervan sprake is, of het gebruik van *big data*-toepassingen op grond van de AWR evenredig is met het beoogde doel: correcte belastingheffing. Bij deze belangenafweging zijn de uitkomsten van de SyRi-zaak relevant, waarbij de rechtbank expliciet stil heeft gestaan bij de digitalisering van de afgelopen jaren en is op grond hiervan de mening toegedaan dat de overheid een 'bijzondere verantwoordelijkheid' heeft bij de inzet van *big data*-technologieën. De toepassing van dergelijke systemen kan er namelijk toe leiden dat de privacy van de belastingplichtige ernstig wordt verstoord, waarbij het voor de belastingplichtige doorgaans onduidelijk is wat de gevolgen voor hem of haar zijn bij de toepassing van deze *big data*-technologieën. Deze bijzondere verantwoordelijkheid van de fiscus ziet op het vinden van een *fair balance* tussen de voordelen die deze technologieën met zich meebrengen en de mate van inbreuk op het recht op privacy, wat kan worden bewerkstelligd door te voorzien in adequate wettelijke waarborgen. Deze *fair balance* kan bijvoorbeeld worden bereikt door voldoende transparant te zijn ten aanzien van de betreffende toepassing en een voorafgaande noodzakelijkheidstoetsing uit te laten voeren door een onafhankelijke derde. Bij het gebruik van *big data* door de fiscus ontbreken momenteel (adequate) waarborgen voor de betrokkene, waardoor niet wordt voldaan aan de noodzakelijkheidstoets. Derhalve dient geconcludeerd te worden dat het gebruik van *big data* door de fiscus op grond van de AWR strijdig is met het recht op privacy van artikel 8 EVRM.

5. Conclusie

In de voorgaande hoofdstukken, is aan de hand van rechtswetenschappelijk onderzoek, een studie verricht naar het spanningsveld tussen enerzijds het gebruik van *big data*-toepassingen door de fiscus op grond van de artikelen in de AWR en anderzijds het recht op privacy van artikel 8 EVRM. Allereerst zijn de wettelijke bevoegdheden van de fiscus omtrent het gebruik van *big data* door de fiscus uiteengezet (hoofdstuk 2). Vervolgens is het recht op privacy van artikel 8 EVRM beschreven (hoofdstuk 3), waarna het gebruik van *big data* is getoetst aan artikel 8 EVRM (hoofdstuk 4). In dit laatste hoofdstuk wordt antwoord gegeven op de centrale probleemstelling:

'In hoeverre wordt het recht op privacy, dat is verankerd in artikel 8 EVRM, geschonden bij het gebruik van big data door de fiscus?'

Om deze vraag te kunnen beantwoorden is het allereerst van belang om te weten wat er wordt verstaan onder het begrip *'*big data*'*. Aan de hand van de verschillende definities die worden gebruikt voor het begrip *big data* zijn er drie hoofdkenmerken van *big data* te onderscheiden, welke kunnen worden beschouwd als fasen in een proces, dat in zijn geheel bestaat uit: het vergaren van informatie, het analyseren en verwerken van deze informatie en tenslotte het gebruik van *big data*-toepassingen. Op basis van de AWR kent de fiscus verschillende wettelijke bevoegdheden voor het vergaren van *big data*, echter bestaan er geen nadere wettelijke grondslagen voor de analyse en gebruik van deze data. Uit de praktijk blijkt de fiscus de wettelijke bepalingen rondom het vergaren van *big data* tevens te gebruiken om beleid te formuleren voor *big data*-analyses en -toepassingen, waaronder: *datamining, profiling* en *nudging.*

De fiscus maakt bij haar *big data*-toepassingen gebruik van privacygevoelige informatie die afkomstig is uit een veelvoud van bronnen waardoor het voor de fiscus mogelijk is om een volledig risicoprofiel te schetsen van de belastingplichtige. De fiscus is niet transparant jegens haar burgers over deze toepassingen, waardoor de belastingplichtige niet op de hoogte is met welke bedrijven en/of personen deze gegevens gedeeld worden dan wel voor hoe lang de fiscus deze gegevens archiveert, dit terwijl de impact op de privacy van de belastingplichtige groot kan zijn. Wat maakt dat bij het gebruik van *big data* door de fiscus op grond van de bevoegdheden van de AWR sprake is van een ernstige inmenging op het recht op privacy. Deze inmenging is slechts toegestaan in geval deze zowel voorzien is bij wet, een legitiem doel nastreeft alsook noodzakelijk wordt geacht in een democratische samenleving.

De inmenging voldoet niet aan de legaliteitstoets omdat er enerzijds geen wettelijke basis bestaat in het nationale recht voor het gebruik van *big data* door de fiscus en anderzijds er niet wordt voldaan aan het voorzienbaarheidsvereiste. Dat niet wordt voldaan aan het voorzienbaarheidsvereiste is drieledig, allereerst is in de AWR niet nauwkeurig genoeg beschreven wat voor soort gegevens kunnen worden opgevraagd, waardoor de informatie die de fiscus gebruikt vrijwel onbeperkt is. Daarnaast is in de AWR niet concreet beschreven in welke gevallen de fiscus handelingen kan en mag verrichten en tenslotte voorziet de AWR niet in (adequate) waarborgen om de burger te bescherming tegen willekeur en misbruik vanuit de fiscus.

Daarnaast voldoet de inmenging eveneens niet aan de legitimiteits- en noodzakelijkheidstoets. Hoewel het doelcriteria: ‘economisch welzijn van het land’ in fiscale zaken doorgaans wordt geaccepteerd, is dit onvoldoende om een beperking op het recht op privacy te rechtvaardigen. Er dient namelijk een belangenafweging gemaakt te worden tussen het betreffende legitieme doel (correcte belastingheffing) en het recht op privacy van de betrokkene. Deze afweging vindt plaats bij de toetsing van de noodzakelijkheid, waarbij de vraag relevant is of het gebruik van *big data* door de Fiscus op grond van de AWR evenredig is met het beoogde doel. Uit de SyRi-zaak volgt dat de fiscus een ‘bijzondere verantwoordelijkheid’ toekomt bij de inzet van *big data*-technologieën. De fiscus dient op basis van deze bijzondere verantwoordelijkheid een *fair balance* te bewerkstelligen tussen de voordelen die *big data*-technologieën met zich meebrengen en de mate van inbreuk op het recht op privacy. Bij het gebruik van *big data* door de fiscus wordt niet voldaan aan het *fair balance*-vereiste omdat de AWR geen inzicht verschaft in de gehanteerde risico-indicatoren en -modellen en tevens de AWR ook niet voorziet in (adequate) waarborgen om de betrokkene te beschermen tegen misbruik en willekeur vanuit de fiscus, waardoor niet wordt voldaan aan de noodzakelijkheidstoets. Omdat niet wordt voldaan aan de drie-stappentoets kan worden geconcludeerd dat het gebruik van *big data* door de fiscus strijdig is met artikel 8 EVRM.

.

.

Geraadpleegde literatuur

Boeken

Blieck e.a. 2019
L.A. de Blieck e.a., *Algemene wet inzake rijksbelastingen*, Deventer: Kluwer 2019.

Feteris 2007
M.W.C. Feteris, *Formeel belastingrecht*, Deventer: Wolters Kluwer 2007.

Gerards 2011
J. Gerards, *EVRM algemene beginselen*, Sdu uitgevers 2011.

Kranenborg & Verhey 2018
H.R. Kranenborg & L.F.M. Verhey, *De Algemene Verordening Gegevensbescherming in Europees en Nederlands perspectief*, Deventer: Kluwer 2018.

Okhuizen e.a. 2018
E.C.G. Okhuizen e.a., *Hoofdzaken formeel belastingrecht*, Den Haag: BJu 2018.

Sjobbema 2007
G.H. Sjobbema, *Informatieverplichtingen van banken ten dienste van belastingheffing*, Antwerpen: Maklu 2007.

Ulrich & Kerckhoffs 2016
G.H. Ulrich & R.W.J. Kerckhoffs, *De informatiebeschikking*, Fed fiscale brochures 2016.

Vande Lanotte & Haeck 2004
J. Vande Lanotte & Y. Haeck, *Handboek EVRM Deel 2 Artikelsgewijze Commentaar*, Intersentia 2004.

Vlemminx 2013
F.C.M. Vlemminx, *Het moderne EVRM*, Den Haag: Boom Juridische uitgever 2013.

Zwenne 1998
G.J. Zwenne, *Belastingheffing en informatieverplichtingen*, Den Haag: Sdu 1998.

Artikelen

Booij 2017
J. Booij, 'Privacy en moeilijk controleerbare belastingwetten', *TFB* 2017/1.

Boyd & Crawford 2014
D. Boyd & K. Crawford, 'Critical questions for Big Data. Provocations for a cultural, technological and scholarly phenomenon', *iCS* 2014, p. 662-679.

Burgers & Nuyens 2017
V.A. Burgers & A.M.E. Nuyens, 'Two is company, three is a crowd', *TFO* 2017/152.4.

Bygrave 1998
L.A. Bygrave, Data Protection Pursuant to the Right to Privacy in Human Rights Treaties', *International Journal of Law and Information Technology* 1998/6.3, p. 269.

Custers 2014
B. Custers, 'Risicogericht toezicht, profiling en Big Data', *TvT 2014/3.2*, p. 4.

De Haas 2014
P. de Haas, 'Gegevensvergaring door de fiscus versus het recht op privacy', *V-N* 2014/14.

De Jong 2015
S. de Jong, 'Denkt u aan uw aangifte? Dank! Liza en Joyce', NRC.nl, 2 maart 2015, https://www.nrc.nl/nieuws/2015/03/10/denkt-u-aan-uw-aangifte-dank-liza-en-joyce-1474025-a399310, bezocht op 12 december 2020.

Ekbia 2015
Ekbia e.a., 'Big Data, bigger dilemmas: A critical review', *Journal of the Association for Information Science and Technology* 2015.

Floridi 2012
L. Floridi, 'Big Data and their epistemological challenge', *Philosophy and Technology 2012/25.*

Gribnau 2008
J.L.M. Gribnau, 'Belastingmoraal en compliance. Het belang van legitimiteit van de Belastingdienst', *WFR* 2008/1325, p. 3.

Kamerling & van der Hel 2013
R.N.J. Kamerling & E.C.J.M. van der Hel, 'Derdenonderzoeken in internationaal perspectief', *WFR* 2013/6544.

Kamerling & Klein Sprokkelhorst 2020
R.N.J. Kamerling & A.K.H. Klein Sprokkelhorst, 'Renseignering in het 'big data' tijdperk', *WFR* 2020/199

Klein 2020 I
P. Klein, 'Belastingdienst geeft toe: toch sprake van etnisch profileren', Rtlnieuws.nl, 11 mei 2020, https://www.rtlnieuws.nl/nieuws/artikel/5117616/belastingdienst-toeslagen-profileren-nationaliteit, bezocht op 10 december 2020.

Klein 2020 II
P. Klein 'Tienduizenden burgers hadden jaren last van 'fraudevermoedens' Belastingdienst', Rtlnieuws.nl, 7 juli 2020, https://www.rtlnieuws.nl/nieuws/nederland/artikel/5169750/belastingdienst-zwarte-lijsten-fraude-toeslagenaffaire, bezocht op 6 december 2020.

Kleinnijenhuis 2019
J. Kleinnijenhuis, 'De top van de Belastingdienst drukte de onrechtmatige aanpak stopzetten kinderopvangtoeslag erdoor', Trouw.nl, 18 november 2019, https://www.trouw.nl/nieuws/de-top-van-de-belastingdienst-drukte-de-onrechtmatige-aanpak-stopzetten-kinderopvangtoeslag-erdoor~b96b4867/, bezocht op 6 december 2020.

Kleinnijenhuis 2020
J. Kleinnijenhuis, 'Belastingdienst hield nóg een omstreden fraudejacht, nu bij aangifte inkomen', Trouw.nl, 7 juli 2020, https://www.trouw.nl/economie/belastingdienst-hield-nog-een-omstreden-fraudejacht-nu-bij-aangifte-inkomen~b08482ef/, bezocht op 6 december 2020.

Martijn 2015
M. Martijn, 'Baas Belastingdienst over Big Data: 'Mijn missie is gedragsverandering', *De Correspondent*, 21 april 2015, https://decorrespondent.nl/2720/baas-belastingdienst-over-big-data-mijn-missie-is-gedragsverandering/83656320-f6e78aaf, bezocht op 15 december 2020.

Megens 2001
J.T.M. Megens, 'Art. 47 AWR: taal of digitaal?' *FF* 2001/219-06.

Poelmann 2017
E. Poelmann, 'Algemene beginselen van behoorlijk bestuur bij informatieverzoeken', *TFO* 2017/152.1, p.156.

Richards & Kring 2013
Richards, N.M. en H.J. King, 'Three paradoxes of Big Data', *Stanford Law Review* 2013/41.

Van Eijsden 2016
A. van Eijsden, 'Tax(t) en uitleg', *WFR* 2016/165.

Van Houte 2005
C.P.M. van Houte, 'De Belastingdienst op fishing expedition', *WFR* 2005/1078.

Van Hout 2017
M.B.A. van Hout, 'Rechtsbescherming in het tijdperk van big data', *WFR 2017/165*, p. 4-5.

Visser 2018
A.B. Visser, 'Bela(sti)ngstelling voor privacy', *Geschriften van de Vereniging van Belastingwetenschap* 2018/258, p.7.

Rapporten en adviezen

Beheersverslag Belastingdienst 2004
Beheersverslag Belastingdienst 2004, J. van Blijswijk e.a., Belastingdienst 2014, p. 22.

Hoofdlijnen aanpak Belastingdienst: Activiteitenkalender 2015
Hoofdlijnen aanpak Belastingdienst: Activiteitenkalender, Den Haag: 2015, p. 27.

Rapport datagedreven selectie van aangiften door de Belastingdienst 2019
Datagedreven selectie van aangiften door de Belastingdienst, Algemene Rekenkamer 2019.

Rapport toezicht en opsporing en massale processen Belastingdienst 2017
Beleidsdoorlichting toezicht en opsporing en massale processen Belastingdienst, bijlage bij Kamerstukken II 2017/18, 31935, nr. 44, p. 17.

Rapport verwerking van risicosignalen voor toezicht belastingdienst 2019
Rapportage verwerking van risicosignalen voor toezicht belastingdienst, bijlage bij Kamerstukken II 2019/20, 31066, nr. 681, p. 39-40.

Rapport waarborgen tegen risico's van data-analyses door de overheid 2019
Waarborgen tegen risico's van data-analyses door de overheid, bijlage bij Kamerstukken II 2019/20, 26643, 641.

WRR-Rapport Big Data 2016
Big Data voor Fraudebestrijding, WRR, Den Haag: Wetenschappelijke Raad Regeringsbeleid 2016.

Kamerstukken

Kamerstukken II, 1985-1986, 19393, nr. 3.
Kamerstukken II 1986-1987, 19393, nr. 150b.
Kamerstukken II 1987-1988, 19393, nr. 3.
Kamerstukken II 1988-1989, 21287, nr. 3.
Kamerstukken II 2005-2006, 30322, nr. 3.
Kamerstukken II 2008-2009, 30645, nr. 14.
Kamerstukken II 2014-2015, 26653, nr. 355.
Kamerstukken II 2016-2017, 33772, nr. 2.
Kamerstukken II 2017-2018, 26643, nr. 557.
Kamerstukken II 2019-2020, 31066, nr. 546.

Jurisprudentie

EHRM 7 december 1976, nr. 6593/72 (*Handyside/VK*).
EHRM 25 april 1978, nr. 5856/72 (*Tyrer/VK*).
EHRM 26 april 1979, nr. 6538/74 (*Sunday Times/VK*).
EHRM 28 maart 1990, nr. 10890/84 (*Groppera Radio AG e.a./Zwitserland*).
EHRM 24 april 1990, nr. 11105/84 (*Huvig/France*).
EHRM 24 april 1990, nr. 11801/85 (*Kruslin/France).*
EHRM 23 november 1993, nr. 14032/88 (*A./Frankrijk*).
EHRM 25 september 2001, nr. 44787/98 (*P.G. & J.H./ VK*).
EHRM 16 april 2002, nr. 37971/97 (*Sociétés Colas/France).*
EHRM 8 april 2003, nr. 39339/98 (*M.M./Nederland*)
EHRM 4 december 2008, nr. 27058/05 (*Dogru/France*).
EHRM 4 december 2008, nr. 30562/04 (*S. en Marper/VK*).
EHRM 13 november 2012, nr. 24029/07 (*MM/VK*).
EHRM 14 maart 2013, nr. 24117/08 (*Bernh Larsen Holding*).
EHRM 1 juli 2014, nr. 43835/11 (*S.A.S./Frankrijk*).
HvJ EU 8 april 2014, ECLI:EU:C:2014:238, C-293/12 (*Digital rights Ireland Ltd e.a.*).
HR 25 januari 2002, ECLI:NL:HR:2002:AD8475.
HR 22 september 2006, ECLI:NL:HR:2006:AY8656.
HR 28 oktober 2009, ECLI:NL:HR:2009:BK3815.
HR 24 februari 2017, ECLI:NL:HR:2017:310 (*ANPR*).
Hof Den Haag 30 december 2004, ECLI:NL:GHSGR:2004:AS1915.
Hof Den Bosch 21 maart 2006, ECLI:NL:GHSHE:2006:AW4328.
Hof Amsterdam 2 mei 2013, ECLI:NL:GHAMS:2013:CA0464.
Hof Den Bosch 19 augustus 2014, ECLI:NL:GHSHE:2014:2803 (*SMSParking*).
Hof Den Bosch 18 maart 2016, ECLI:NL:GHSHE:2016:1019.
Rb. Den Haag 5 februari 2020, ECLI:NL:RBDHA:2020:865 (*NJCM C.S./ Staat der Nederlanden*).